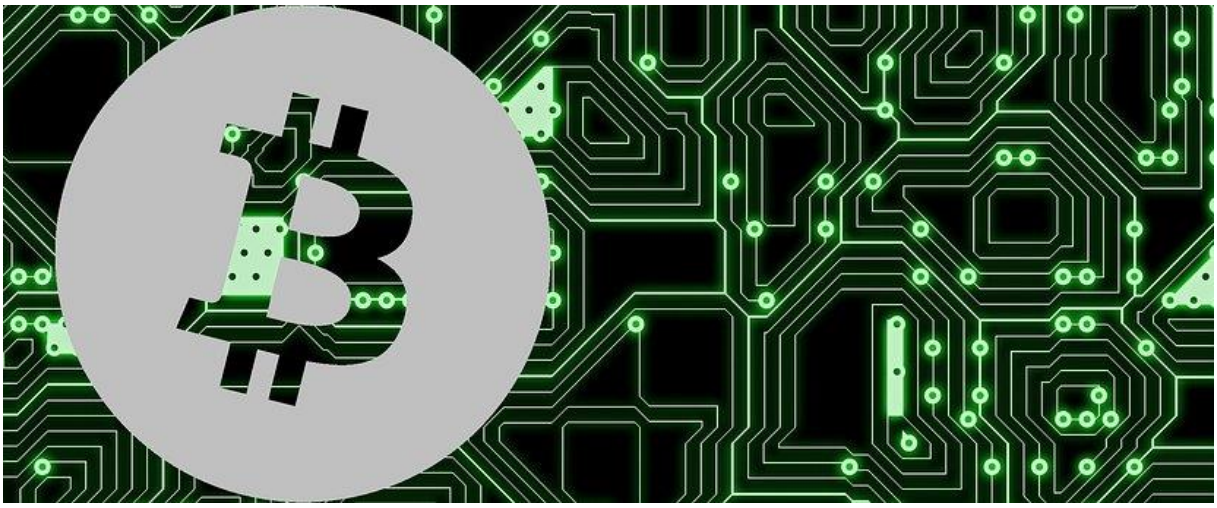


FINTECH – DEFI - KRIPTOESZKÖZÖK GAZDASÁGI ÉS JOGI LEHETŐSÉGEI ÉS KOCKÁZATAI

KONFERENCIAKÖTET – VÁLOGATOTT TANULMÁNYOK

2022

Pécs

2021. november 4. FINTECH – DEFI - KRIPTOESZKÖZÖK GAZDASÁGI ÉS JOGI LEHETŐSÉGEI ÉS KOCKÁZATAI konferencia válogatott tanulmányok

Kiadó:
Pécsi Tudományegyetem Állam- és Jogtudományi Kar

ISBN: 978-963-429-835-9

Tartalom

Antal-Molnár Nikolett: A kriptovalutától a digitális valutáig 4

Breszkovics Botond: Kriptoszabályozás Szingapúrban 14

Bujtár Zsolt: A decentralizált pénzügyek (DeFi) főbb jogi szabályozási kihívásai 26

Csesznik Zoltán: Kripto a jövőbe csomagolva 40

Gáspár Zsolt: Money Laundering and Cryptocurrencies in the Hungarian and EU regulations 49

Gáti Balázs: A mesterséges intelligencia európai uniós szabályozásának egyes adatvédelmi kérdései 59

Nagy Gergely Miklós: A fintech - blockchain informatikai projektek kockázatmenedzsment stratégiájának megalapozása 79

Nagy Zoltán András: Nyomozás a blokkláncban a BTC után 91

Prisznyák Alexandra: „Tradicionális" bankok front/middle/back office területeinek mesterséges intelligencia (AI), gépi tanulás (ML) implementációja 98

Projics Nárcisz: A polgári peres eljárás a digitalizáció világában 114

Tóth Dávid: A közösségi média és a bűnözés összefüggései 130

Antal-Molnár Nikolett*: A kriptovalutától a digitális valutáig

Absztrakt:

Napjainkban az elektronikus eszközök és az internet rohamos fejlődésével, a készpénzes és bankkártyás fizetést kezdik felváltani a mobiltelefonon és az interneten keresztül történő fizetési módok. Ennek megjelenése, és a technológia fejlődése felgyorsította a kriptovaluták elterjedését, és előhívta a digitális valuták iránti igényt. A kriptovaluták – és közülük is a legismertebb a Bitcoin – számos helyen elfogadott fizetőeszközök, de decentralizált rendszere miatt általánosan elfogadott valutaként nem, inkább csak mint kockázatos befektetési forma maradhat fenn. Ezzel szemben a digitális valuta, mely rendelkezne a hagyományos valuta minden tulajdonságával, azt leszámítva, hogy nem megfogható eszköz, lehet a jövőbeni fizetőeszköz. Ezek szintén központi bankok által kibocsátott és ellenőrzött valuták lennének – mint a fiat pénzek –, melynek egy példája a DC/EP (Digital Currency / Electronic Payment). A tanulmány első része, a kriptovaluta és a digitális valuta közötti különbségeket hivatott bemutatni. A második részben fizetőeszközként betöltött szerepüket vizsgálom meg. Végül a digitális valuták előnyeinek megfogalmazásával zárom a tanulmányt.

kulcsszavak: *kriptovaluta, blokklánc, digitális valuta, DC/EP*

I. Bevezetés

Napjainkban egyre nagyobb teret nyernek az elektronikus, és ezen belül is az internet kapcsolatot felhasználó eszközök. Így ezek a mindennapjaink elengedhetetlen részéve kezdenek válni. Gondoljunk csak arra, hogy a kommunikáció számos formája is már gyakran online történik. Egy stabil internetkapcsolattal rendelkező telefonnal szinte bárhonnan tudunk kommunikálni, navigációt használni, online zenét hallgatni és még sokáig sorolhatnánk. A koronavírus hatására még nagyobb teret nyertek az online események, és vásárlásaink során is egyre gyakrabban választjuk az online, akár háztól házig megoldásokat, platformokat. Ennek a növekvő tendenciának is köszönhető, hogy egyre kevesebb készpénzes vásárlás történik. A bankkártyás fizetés egyre elterjedtebbé vált, de napjainkban egyre több helyen találkozhatunk a mobillal történő fizetéssel, amelyhez általában egy folyószámla van csatolva, de manapság már a kriptovaluták is számos helyen elfogadott fizetőeszközök. A legújabb fejlesztés pedig, amely új korszakot hozhat a fizetési rendszerekben nem más, mint a digitális valuta.

* Antal-Molnár Nikolett, PTE-KTK, Pécsi Tudományegyetem Gazdálkodástani Doktori Iskola, PhD hallgató, molnar.nikolett@ktk.pte.hu

Tanulmányomban először a kriptovaluta, majd a digitális valuta fő jellemzőit mutatom be, rávilágítva a kettő közötti különbségekre. Ezután áttekintem, hogy mi ösztönözte a digitális valuták kialakulását, és miért válhat a jövő fizetőeszközévé, majd végezetül a digitális valuták előnyeinek és hátrányainak megfogalmazásával zárom a tanulmányomat.

I. A kriptovaluták és a digitális valuták jellemzői

1. A kriptovaluták jellemzői

Bő egy évtizeddel ezelőtt egy új, eleinte csak pénzügyi innovációnak számító technológiát dolgozott ki a Nakamoto álnéven elhíresült személy (vagy csoport), hogy a banki környezettel szemben egy alternatív fizetési rendszert alakítson ki. A technológia digitális aláírások láncolatán alapul. Ezt nevezzük blokkláncnak, ami alapvetően egy digitális főkönyv, amely az aláírások révén felsorolja az előző tulajdonosokat és a hozzájuk tartozó tranzakciós eseményeket. A blokklánc technológiát eleinte a kriptovaluták fejlesztői használták arra, hogy pénzügyi eszközök cseréjét tegyék lehetővé harmadik fél bevonása nélkül.[1] Napjainkban a Bitcoin a legismertebb kriptovaluta, – amely egyelőre nem terjedt el, mint fizetőeszköz, hanem inkább egy kockázatos befektetési formának tekinthető[2] a piaci ár éles ingadozása miatt – amely blokkláncot használ a tranzakciók végleges rögzítéséhez, időrendben és kódfejtéssel hitelesítve azokat. Így alakulnak ki a blokkok, melyek sokasága alkotja a blokkláncot. Ezeket a blokkláncokat számítógépek *peer-to-peer* hálózata működteti, amelyeken csomópontok találhatóak, és ezen csomópontok mindegyike tárolja a főkönyv teljes másolatát. A rendszer nyílt forráskódú, ezáltal a hálózat mindenki számára hozzáférhető, mindemellett két fél közti tranzakciók lebonyolítására alkalmas harmadik fél bevonása nélkül.[3] Tehát a kriptovaluták rendszerüknél fogva decentralizáltak. Hiszen a kriptovaluák *peer-to-peer* rendszere, mint azt a neve is mutatja, egy olyan hálózatot, és a köztük lévő kapcsolatot jelöl, amelyben minden számítógép szerverként működik, így közvetlen hozzáférést biztosít két fél között egy központi szerver nélkül, míg a digitális valutáknál a bankok jelennének meg harmadik félként. A kriptovaluták tekintetében a tranzakciók és a hozzájuk tartozó adatok egy úgynevezett digitális főkönyvben érhetőek el, blokkokba rendezve. Ezek a blokkok egymáshoz csatlakoznak, amit a

[1] Satoshi Nakamoto: A peer-to-peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, (2021.02.20.)
[2] Bugár Gyöngyi – Somogyvári Márta, 2020: Bitcoin: digitális szemfényvesztés, vagy a jövő valutája? In: Hitelintézeti Szemle. 19. évf. 1. szám., pp. 132-153.
[3] Michael Crawford Urban, 2018: Inside the Black Blocks: A Policymaker's Introduction to Blockchain, Distributed Ledger Technology and the „Internet of Value". Toronto, Mowat Centre for Policy Innovation, pp. 14-19.

peer-to-peer rendszerben lévő csomópontok hitelesítenek és időbélyegzővel látnak el. Ez a hitelesítés igazolja, hogy nem történik kettős költekezés. Az így egymáshoz csatlakozó, hitelesített adatblokkok láncot alkotnak. Ezt nevezzük blokkláncnak. [4]

A blokklánc és az megosztott főkönyvi technológia (DLT) a 21. századi gazdaság alaptechnológiáját képviselik. A DLT technológia a blokkláncot és más hasonló technológiákat is magában foglal. A DLT egy olyan decentralizált hálózat, amelyben az adatok a hálózat tagjai között megosztásra kerülnek, és a hálózat bármely, arra jogosult tagja hozzáférhet ezekhez az adatokhoz, illetve módosíthatja, hitelesítheti azokat. A blokklánc a DLT leggyakrabban előforduló formája, amely plusz kritériumot tartalmaz az osztott főkönyvhöz képest, ami nem más, mint az adatblokkok láncokba rendezése. Ezen felül a blokkláncon az adatok visszamenőleg nem módosíthatóak.[5]

Nakamoto publikációja után számos cikk jelent meg a blokkláncról, így több definíció is létezik, melyek közül párat megemlítek:

- Don és Alex Tapscott szerint a blokklánc egy programozott főkönyv, amely olyan gazdasági tranzakciókat tartalmaz, amelyeken nem lehet változtatni.[6]
- Chen szerint a blokklánc egy osztott főkönyv, ami a tranzakciókat blokkok formájában tárolja, amelyek láncszerűen kapcsolódnak egymáshoz.[7]
- Marr szerint a blokklánc egy decentralizált főkönyv, ami lehetővé teszi a két fél között lezajló tranzakciók időbélyegzését és rögzítését harmadik fél bevonása nélkül.[8]
- Bogart és Rice szerint a blokklánc általában egy osztott főkönyv, azaz blokkok időrendi lánca, ahol minden blokk tartalmazza az érvényes hálózati aktivitás rekordját, az utolsó blokk hozzáadásától számítva.[9]

[4] Satoshi Nakamoto: A peer-to-peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, (2021.02.20.)
[5] Michael Crawford Urban, 2018: Inside the Black Blocks: A Policymaker's Introduction to Blockchain, Distributed Ledger Technology and the „Internet of Value". Toronto, Mowat Centre for Policy Innovation, pp. 6-10.
[6] Don Tapscott – Alex Tapscott, 2016: Blockchain Revolution: How the technology behind bitcoin is changing money, business, and the world. New York, Penguin Random House LLC, p. 7.
[7] Yan Chen, 2018: Blockchain tokens and the potential democratization of enterpreneurship and innovation. In: Business Horizons. 61(4). szám, pp. 567-575.
[8] Bernard Marr: A Very Brief History of Blockchain Technology Everyone Should Read. https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/?sh=63efedc77bc4, (2021.02.20.)
[9] Spencer Bogarat – Kerry Rice, 2015: Blockchain Report: Welcome tot he Internet of Value. https://ripple.com/insights/needham-report-welcome-to-the-internet-of-value/, (2021.02.20.)

- Kakavand és társai szerint a blokklánc egy olyan adatbázis, amely időrendi sorrendben lebonyolított tranzakciókból áll, amiket blokkoknak nevezünk, és ezekben bármely tranzakció ellenőrizhető.[10]

Ezek alapján tehát azt lehet mondani, hogy a blokklánc olyan tranzakciók együtteséből áll, melyek egymás után következnek időrendben, és két fél között zajlanak harmadik fél bevonása nélkül.

Összegezve a blokklánc rendszer egy világméretű, decentralizált számítógépes hálózat, melyben minden, a hálózatba bekapcsolódó számítógép csomópontnak tekinthető. Minden csomópont rendelkezik a blokklánc legfrissebb verziójával és versenyez az utolsó tag megfejtéséért.[11] Bár a kriptovaluták rendszere biztonságosnak tekinthető, a visszaélések és csalások kockázata igen nagy, hiszen nem áll közvetlen ellenőrzés alatt. A kriptovaluták csak elektronikus formában léteznek, online és offline pénztárcákat használnak, valamint kétkulcsos architektúrát alkalmaznak a tranzakciók biztosítására.[12]

Mint említettük, a kriptovaluták is számos helyen elfogadott fizetőeszközök, az előbb említett okok miatt nem valószínű, hogy a jövőben fizetőeszközként funkcionálhatnak. A kriptovaluták térnyerése viszont arra ösztönözte – és ösztönzi mai napig – a tudósokat, hogy jobban megismerjék az alapjául szolgáló blokklánc technológiát, amely új kapukat nyitott meg. A blokklánc technológiát ma már számos helyen alkalmazzák, beleértve a közigazgatást, az egészségügyet, de a tanulmány szempontjából fontos digitális valutát is, melynek fő jellemzőit a következő részben taglalom.

2. A digitális valuták jellemzői

A digitális valuták, a kriptovalutákhoz hasonlóan a blokklánc technológián alapulnak, és adataik digitális főkönyvben találhatóak.[13] A digitális valuta másik hasonlósága a kriptovalutákhoz viszonyítva, hogy csak elektronikus formában létezik. A fiat pénzekhez hasonlóan a digitális valuták kimondottan fizetési célra létrehozott eszközök, melyek a fizikai áruk és szolgáltatások vásárlására is alkalmasak. Ezek, bár blokkláncrendszert alkalmaznak, mégis központi bankok által kibocsátott és ellenőrzött digitális fizetőeszköznek tekinthetőek.

[10] Hossein Kakavand et al., 2017: The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251, (2021.02.20.)
[11] Satoshi Nakamoto: A peer-to-peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, (2021.02.20.)
[12] Jonas Gross – Alexander Bechtel: China's digital currency project: What is DC/EP all about? **Hiba! A hiperhivatkozás érvénytelen.**https://jonasgross.medium.com/chinas-digital-currency-project-what-is-dc-ep-all-about-e3b2f47e49c, (2021. 10. 20.)
[13] Michael A. Peters – Benjamimn Green – Haiyang (Melissa) Yang, 2020: Cryptocurrencies, China's sovereign digital currency (DCEP) and the US dollar system. In: Educational Philosophy and Theory, DOI: 10.1080/00131857.2020.1801146 pp. 5.

Ezáltal megbízható csereeszközt képezhetnek, és ezzel felválthatják a ma használatos valutákat, hiszen a kormány jóváhagyásával stabilabb piaci árral és biztonságosabb értékmegőrzéssel rendelkeznek.[14] Ebből következik az is, hogy a főkönyvet is a kormány vagy a központi bank irányítja, ami szabad kezet nyújt a teljes ellenőrzésben a pénzgazdaság felett, így használatukkal a csalások, a visszaélések és a pénzmosás is nagymértékben visszaszoríthatóvá válik.[15]

A digitális valuták egyik példája a DC/EP, mely a kettős offline fizetési rendszer mintáján alapszik, így helyettesítheti a hagyományos készpénzes fizetési módot, hiszen a fizetés független az internettől. A kínai tesztfázisban az is kiderült, hogy a DC/EP-t egy mobilalkalmazás segítségével lehet használni, melyben nem szükséges bankszámlát kapcsolni a digitális pénztárcához. Ezáltal a DC/EP használata továbbra is névtelen marad, így nem válik ellenőrizhetővé, csak a kínai központi bank számára.[16]

Ebben a részben áttekintettem a digitális valuták fő jellemvonásait, kitérve a kínai központi bank által tesztelésre kibocsátott DC/EP-re, mely a harmadik fejezet alapját képezi. A jelen fejezetet a fent felsorolt jellemzők összegzésével zárom, melyben rámutatok a kriptovaluták és a digitális valuták hasonlóságaira és különbségeire egyaránt.

3. A kriptovaluták és a digitális valuták összehasonlítása

Ebben a részben, a kriptovaluták és a digitális valuták közötti különbségeket és hasonlóságokat vetem össze, melyeket egy táblázatban is összefoglalok.

Az első-, és legfontosabb különbség a két rendszer között az ellenőrzés, harmadik fél által. Hiszen a Bitcoin *peer-to-peer* rendszere, mint azt a neve is mutatja, egy olyan hálózatot, és a köztük lévő kapcsolatot jelöl, amelyben minden számítógép szerverként működik, így közvetlen hozzáférést biztosít két fél között egy központi szerver nélkül, míg a digitális valutáknál a bankok jelennének meg harmadik félként. A kriptovaluták tekintetében a tranzakciók és a hozzájuk tartozó adatok egy úgynevezett digitális főkönyvben érhetőek el, blokkokba rendezve. Ezek egymáshoz csatlakoznak, amit a peer-to-peer rendszerben lévő csomópontok (számítógépek) hitelesítenek és időbélyegzővel látnak el. Az így egymáshoz csatlakozó, hitelesített adatblokkok láncot alkotnak. Ezt nevezzük blokkláncnak. Ezzel szemben, ha a digitális valutákat vesszük figyelembe, melyek szintén a blokklánc rendszeren

[14] XU YU: Analysis on the future of financial market in China - challenges & impact of the issuance of Dcep. http://hdl.handle.net/10362/122786, (2021.10.21.)

[15] Michael A. Peters – Benjamimn Green – Haiyang (Melissa) Yang, 2020: Cryptocurrencies, China's sovereign digital currency (DCEP) and the US dollar system. In: Educational Philosophy and Theory, DOI: 10.1080/00131857.2020.1801146 pp. 2.

[16] XU YU: Analysis on the future of financial market in China - challenges & impact of the issuance of Dcep. http://hdl.handle.net/10362/122786, (2021.10.21.)

alapulnak, és adataik digitális főkönyvben találhatóak, a különbséget az adja, hogy nem a számítógépes csomópontok hitelesítik ezeket, hanem a főkönyvet a kormány vagy az adott bank fogja irányítani, ami szabad kezet nyújt a teljes ellenőrzésben a pénzgazdaság felett. Így egy másik nagy különbség is kirajzolódik. Bár a kriptovaluták rendszere biztonságosnak tekinthető, a visszaélések és csalások kockázata igen nagy, hiszen nem áll közvetlen ellenőrzés alatt. Ezzel szemben a digitális valuták ellenőrzöttségüknél fogva, nagymértékben vissza tudnák szorítani a csalásokat, visszaéléseket és a pénzmosást is.

A kriptovaluták és a digitális valuták legfőbb közös pontja, hogy csak elektronikus formában léteznek. Ezen kívül közös pont még az online és offline pénztárcák használata és a kétkulcsos architektúra alkalmazása a tranzakciók biztosítására. Bár, mint már említettem, a kriptovaluták is számos helyen elfogadott fizetőeszközök, nem valószínű, hogy a jövőben általános fizetőeszközként funkcionálhatnak, inkább megmaradnak kockázatos befektetési eszközöknek. Ezzel szemben a digitális valuták, melyek kimondottan fizetési célra létrehozott eszközök, a jövőben felválthatják a ma használatos valutákat.

A kriptovaluták és a digitális valuták összehasonlítása a fent említett jellemzők alapján

Kriptovaluta	*Digitális valuta*
Decentralizált	Centralizált
Nincs közvetítő/ellenőrző	Ellenőrző a kormány vagy a bank
Blokklánc rendszeren alapszik	Blokklánc szerű rendszert használ
Adatok digitális főkönyvben	Adatok digitális főkönyvben
Csomópontok hitelesítik az adatokat	A kormány vagy a bank hitelesíti az adatokat
Nagy a visszaélések, csalások kockázata	Visszaszorítja a visszaéléseket, csalásokat
Csak elektronikus formában létezik	Csak elektronikus formában létezik
Online és offline pénztárcák használata	Online és offline pénztárcák használata
Kétkulcsos architektúra alkalmazása	Kétkulcsos architektúra alkalmazása
A jövő kockázatos befektetési eszköze	A jövő fizetőeszköze

Saját szerkesztés

II. A digitális valuták létjogosultsága

Ebben a fejezetben a digitális valuták térnyeréséről lesz szó. Mint azt már korábban is említettük a DC/EP ezek egyik példája, így a kínai megvalósítási folyamaton keresztül mutatjuk be a térnyerést.

A digitális valuták kialakulásában a technológia erőteljes fejlődése, a digitalizáció és a kriptovaluták megjelenése is nagymértében közrejátszott. A folyamatosan fejlődő világban a készpénzes fizetéseket a banki tranzakciók váltják fel, melynek alapot ad a technológia fejlődése és ezáltal a digitalizáció térnyerése is. A kriptovaluták blokkláncrendszerét

alkalmazzák a digitális valuták is, melynek bevezetésében Kína élen jár. Kínában a készpénzes fizetéseket a mobiltelefonos fizetési rendszer váltotta fel, és jelenleg a tesztelés ötödik fázisánál tartanak, saját digitális pénznemükre a DC/EP, azaz *Digital Currency / Electronic Payment*-re tekintve.

A kínai központi bankon kívül, más központi bankok is gondolkodnak a digitális valutákra való átállásban. De mi indokolja a digitális valutákra való átállást? Avagy mi történt Kínában, hogy ennyivel előrébb jár, mint a többi ország ezen a téren? 2009-ben a Kereskedelmi Minisztérium Kínában bejelentette, hogy a kriptovaluták nem cserélhetők árukra, vagy szolgáltatásokra[17], majd 2013-ban megtiltotta a pénzintézeteknek, hogy tranzakciókat folytassanak Bitcoin-ban.[18] Ezek után 2017-ben Kína betiltotta a kriptovaluta kereskedelemmel, illetve az ICO-kal (*Initial Coin Offering* – vállalkozás finanszírozás blokklánc hálózaton keresztül) kapcsolatos platformokat, hogy csökkentse a kriptovaluták volatilitása által előidézett pénzügyi kockázatokat. Ennek ellenére a tilalom nem terjedt ki a Bitcoin alaptechnológiájának fejlesztésére, a blokkláncra. Ehelyett a kínai kormány átvette a vezetést a blokklánc technológia fejlesztésének támogatásában. Ugyanezen évben Kína központi bankja kifejezte szándékát 5 éves fejlesztési tervében, miszerint elősegíti a blokklánc technológia kutatását és alkalmazását a pénzügyi szektorban. A támogatás hatására 2017-ben 550 szabadalmi kérelem érkezett a kormányhoz, amely a második helyen álló Egyesült Államok kérelmeinek, majdnem kétszerese. 2019 első félévében 197 blokklánc rendszeren alapuló szolgáltatást hagytak jóvá.[19]

A blokklánc hálózatok kutatása megnyitotta a digitális fizetőeszközök előtt is a kaput, Kínában egy blokklánc-szerű, de nem blokklánc alapú digitális valuta kidolgozása, és tesztelése zajlik.[20] Világszerte a legtöbb átutalás Ázsiában történik, így Indiában, Kínában és a Fülöp-szigeteken. A határon átnyúló utalások költségaránya pedig 7%.[21] Egy 2009-es kutatás szerint a lakossági szolgáltatások igénybevételéhez kapcsolódó tranzakciós költségek a GDP közel 1%-át teszik ki, és ezeknek a terheknek a nagy részét a kiskereskedelem viseli.[22] Ezekből tisztán

[17] Vicenzo Morabito, 2017: Business Innovation Through Blockchain. Bocconi University, Springer, p. 85.
[18] Bashir Masooda – Strickland Beth – Bohr Jeremiah, 2016: What Motivates People to Use Bitcoin? In: International Conference on Social Informatics., pp. 347-367.
[19] Yu Wang – Jing Ren – Caroline Lim – Swee-Won Lo, 2019: A Review of fast-growing Blockchain Hubs in Asia. In: The Journal of the British Blockchain Association 2. évf. 2. szám, pp. 83-98.
[20] Hoffman Samantha et.al.: The flipside of China's central bank digital currency, https://www.aspi.org.au/report/flipside-chinas-central-bank-digital-currency, (2021.04.23.)
[21] Yu Wang – Jing Ren – Caroline Lim – Swee-Won Lo, 2019: A Review of fast-growing Blockchain Hubs in Asia. In: The Journal of the British Blockchain Association 2. évf. 2. szám, pp. 83-98.
[22] Schmiedel Heiko – Kostova Gergana – Ruttenberg Wiebe, 2012: The Social and Private Costs of Reteail Payment Instruments, In: Occasional Paer Series, 137. szám, pp. 25.

látszik, hogy a digitális fizetésekre nagy az igény, és nem utolsó sorban a digitális valuták alkalmazása a tranzakciós költségek visszaesését is eredményezhetné.

Kínában a készpénzes fizetéseket – a bankkártyás fizetésekre való átmenet nélkül – közvetlenül a mobiltelefonos fizetések váltották fel. 2019-ben a lakosság nagy része (86%[23]) az Alibaba Alipay, illetve a Tencent WeChat Pay fizetési rendszerét használta.[24]Ezáltal Kínában az átállás sokkal egyszerűbben megtörténhet, mint azokban az országokban, ahol mai napig a készpénzes és bankkártyás vásárlások preferáltak. 2020 áprilisában a kínai központi bank megkezdte tesztfázisát négy kínai városban (Shenzhen, Suzhou, Chengdu, Xiong'an), így több ezer embernek van lehetősége részt venni a kísérletben úgy, hogy előre meghatározott mennyiségű digitális valutát használnak fel az adott nagyvárosokban. Kína célja, ha sikeres tesztfázist tud maga mögött, hogy a digitális valuta elindítása és használata a 2022-es pekingi olimpiára megtörténjen. Tehát elég sok tényező és hosszú folyamat áll Kína digitális valutájának a bevezetésének a hátterében.[25]

III. A digitális valuták előnyei és hátrányai

Egy új fizetési rendszer van kialakulóban, ha a digitális valuták bevezetésére tekintünk. Ezért elengedhetetlen a bevezetésükhöz és használatukhoz kapcsolódó előnyök és hátrányok megfogalmazása, melyek érveknek is tekinthetőek a bevezetés mellett vagy ellen.

A DC/EP-t digitális jüan-nak is tekinthetjük, mivel értéke megegyezik a fizikai jüan értékével.[26] A digitális jüan egy okostelefon alkalmazással használható, mely közvetítő felet nem igényel, hiszen digitális pénztárcán keresztül terjesztik, nem bankszámlán. Ennek oka, hogy fizikai pénzről nem beszélhetünk, amelyet bankszámlán kellene tárolni, tehát a DC/EP valóban teljes mértékben digitális.[27] Ez az alkalmazás, avagy a kínai központi bank által kiadott digitális pénztárcák, mivel kizárják a közvetítő felet, így az ahhoz kötődő infrastruktúrákat is, ezáltal alacsonyabb tranzakciós költségeket eredményeznek. Másik előnye, hogy nincs szükség kártyás hálózati fizetésre, mert a központi bank és a kibocsátó bankok közvetlenül

[23] Lamb Keith: The future of China's digital currency. https://news.cgtn.com/news/2020-11-11/The-future-of-China-s-digital-currency--VkaX4E1i8g/index.html, (2021.10.21.)
[24] Michael A. Peters – Benjamimn Green – Haiyang (Melissa) Yang, 2020: Cryptocurrencies, China's sovereign digital currency (DCEP) and the US dollar system. In: Educational Philosophy and Theory, DOI: 10.1080/00131857.2020.1801146 pp. 1.
[25] Jonas Gross – Alexander Bechtel: China's digital currency project: What is DC/EP all about? **Hiba! A hiperhivatkozás érvénytelen.**https://jonasgross.medium.com/chinas-digital-currency-project-what-is-dc-ep-all-about-e3b2f47e49c, (2021. 10. 20.)
[26] Michael: China's National Digital Currency DCEP / CBDC overview. https://boxmining.com/dcep/#DCEP_will_operate_on_a_twotiered_system, (2021. 10.20)
[27] Ezquer Evan: DCEP Adoptin: How to use the Digital Yuan. https://www.asiacryptotoday.com/dcep-adoption-how-to-use-the-digital-yuan/, (2021.10.21.)

kapcsolódnak egymáshoz, így ez is a költségek csökkenését jelenti. A mobillal történő fizetési rendszerekhez képest megfogalmazható a digitális jüan azon előnye is, hogy nem igényel internetkapcsolatot, ezáltal könnyebb használatot eredményez, szélesebb körben is alkalmazhatóvá válik, és nem utolsó sorban megelőzi a hálózati meghibásodások, vagy áramkimaradások miatti fennakadásokat.[28] A készpénzhez viszonyítva pedig nem elhanyagolható, főleg a mostani körülmények között, hogy sokkal higiénikusabb megoldást biztosít.

Tehát a digitális valuták egyik legnagyobb előnyeként a megbízhatóságot, azaz az alacsony kockázatú fizetési megoldást említeném. A digitális valuták cseréje abban a pillanatban megtörténik, mikor a két fél között a végső megállapodás megtörténik. A bankkártyás fizetéseknél, elektronikus utalásoknál vagy csekkel történő fizetéskor az ügylet nem teljesül azonnal, csak akkor, amikor azt a bank rögzíti. Másik fontos előny az alacsony költség, és az ehhez kapcsolódó magas hatékonyság. Az alacsony költség a tranzakciós költségek csökkentésére utal, a közvetítők kizárása révén. A hatékonysága pedig a másodpercenkénti tranzakciók (TPS) számában mutatkozik meg. A DC/EP egy kutatás szerint 220 000 tranzakció/másodperc átviteli sebességet képes elérni. Összehasonlításképpen a PayPal 40 000, a Visa hálózatai kb. 1700, az Ethereum 30, a Bitcoin pedig átlagosan 5 TPS átviteli sebességet ér el. Fejlesztések persze folynak, például az Ethereum szoftverfrissítése az év végére, vagy a jövő év elejére várható, amelynek köszönhetően az eddigi 30 TPS 100 000 TPS-re növekedhet, a horizontális skálázás felhasználásával. A harmadik előny, amit még egyszer hangsúlyoznánk a gazdasági bűncselekmények és csalások visszaszorítása. A fiat valutához képest a digitális pénzt nehéz hamisítani. A tranzakciós rekordok titkosítva vannak, és teljes felügyelet alatt állnak. Ez viszont felveti a digitális valuták egyik legnagyobb hátrányát is társadalmi szempontból, méghozzá az adatvédelmi kérdéseket. Elvégre a tranzakciók nem lehetnek teljesen névtelenek, a DC/EP rendelkezik a felhasználók személyes adataival, melyek nyomon követhetőek, és a felhasználástól a tárolásig minden pénzmozgás rögzíthető. Felmerülhet a visszaélés kérdése is a kormányok részéről, elvégre az összes felhasználó pénzügyi információinak birtokában lesznek. Ezek az információk pedig számítógépes bűnözők potenciális célpontja is lehet. A digitális valuták elterjedése nagy kihívást jelenthet még a pénzügyi közvetítőkre, a mobil- és online fizetési platformokra, illetve a bankokra nézve is.[29]

[28] Jonas Gross – Alexander Bechtel: China's digital currency project: What is DC/EP all about? https://jonasgross.medium.com/chinas-digital-currency-project-what-is-dc-ep-all-about-e3b2f47e49c, (2021. 10. 20.)

[29] Kshetri Nir, 2021: The Economics of Central Bank Digital Currency. In: Computer 54. évf. 6. szám. pp. 53-58. DOI: 10.1109/MC.2021.3070091

A felsorolt előnyöket és hátrányokat az alábbi táblázat foglalja össze.

A digitális valuták alkalmazásának előnyei és hátrányai

Előnyök	*Hátrányok*
Alacsonyabb tranzakciós költség	Ellenőrzött/teljes felügyelet
Nem szükséges a kártyás hálózati fizetésre	Adatvédelem hiánya
Nem igényel internetkapcsolatot	Visszaélés lehetősége
Szélesebb körben alkalmazható	Számítógépes bűnözők potenciális célpontja
Higiénikusabb, mint a készpénz	
Megbízható, alacsony kockázatú fizetési mód	
Magas hatékonyság	
Ellenőrzött/teljes felügyelet	

Saját szerkesztés

A táblázatból jól látható, hogy az előnyök igen sokrétűek, míg a hátrányok inkább az adatok és azok védelme köré csoportosulnak. Bár Kínában is még tesztelés alatt áll a digitális valuták használata, így számos előny és hátrány fogalmazódhat még meg, de az már most is tisztán látszik, hogy az adatvédelem egy sarkalatos pontja a digitális valuták használatának.

IV. Összegzés

Összességében a tanulmány megmutatta, hogy mely tényezők akadályozzák a kriptovaluták fizetőeszközzé válását, melyek adnak létjogosultságot a digitális valutáknak és mik azok az előnyök, illetve hátrányok, amelyeket megtapasztalhatunk a digitális valuták fizetőeszközzé válása során. Fontos figyelembe venni, hogy valószínűleg a digitális valuták, mint fizetőeszközök nem a távoli jövőben kerülnek bevezetésre, hiszen a Nemzetközi Fizetések Bankjának felmérése alapján a világ központi bankjainak 80%-a digitális valuták kutatásában vesz részt, míg Kínán kívül, már Svédország, Uruguay és a Bahama-szigeteki központi bank is elindította saját digitális valutáját.[30]

[30] Mian Xia, 2021: In Search of The Perfect Coin: China's Approach towards Cryptocurrency and Its Own Central Bank Digital Currency. In: Banking & Finance Law Review, 36. évf. 3. szám. pp. 419-456.

Breszkovics Botond*: Kriptoszabályozás Szingapúrban

Absztrakt:

Szingapúr kezdetben a brit gyarmatbirodalom részeként, egy stratégiailag meghatározó jelentőségű, kereskedelmi kikötő szerepét töltötte be. Majd az 1965-ös függetlenedését követően, az ázsiai térség egyik kistigriseként gyors gazdasági fejlődési pályára lépett.[1] Napjainkban pedig a városállam amellett, hogy a világ egyik üzleti központja, egyben számos blokklánc vállalkozásnak is otthont ad. Az 2021-ben bekövetkezett nagy kínai kripto kitiltás miatt pedig különösen felértékelődött Szingapúr szerepe az ázsiai régióban, amely a kripto elszívás új dimenzióit nyithatja meg azáltal, hogy a blokklánc vállalkozások tömeges megjelenésével kell számolni. Azonban a városállam vállalkozó központúsága és nyitottsága az innovációra nem mindig volt jellemző. Jelen tanulmány célja röviden bemutatni, hogy egy zérusponthoz közeli vállalkozói kultúrával rendelkező ország, függetlenedését követően milyen külső hatások és belső tényezők által vált meghatározó és népszerű célponttá a kripto-szektor szempontjából.

Kulcsszavak*: kriptovaluta, token, DTP, DTPS, Szingapúr, kriptoban*

I. Szingapúr kedvező intern tényezői

Álláspontom szerint a Szingapúrban jelenleg tapasztalható magas fokú kripto elfogadottság több belső (állami) tényezőre vezethető vissza. A kriptoszektor vonatkozásából ezek közül kiemelném a városállam gazdasági szféráját, az átható adaptív természetet, az innovációra való nyitottságot és az erős vállalkozói kultúrát. Ezen túlmutatóan a kedvező jogi szabályozás valamint a pénzügyi felügyeleti szerv naprakészsége és effektív tevékenysége sem elhanyagolható. Jelen alfejezetben az előzőekben felsorolt belső tényezők bemutatására szorítkozom.

1. KKV-k szerepe és a jogrendszer megszilárdulása Szingapúrban

Napjainkban tényként kezeljük, hogy Szingapúr a világ egyik pénzügyi központja, ahol többek között olyan technológiai óriáscégek is jelen vannak, mint a kínai Tencent Holdings Ltd. A cég délkelet-ázsiai regionális központjának ad otthont a városállam. Megemlíthető a népszerű TikTok alkalmazás mögött álló Byte Dance Ltd. jelenléte[2], vagy az amerikai Twitter Inc. is,

* Breszkovics Botond, PTE ÁJK Doktori iskola, PhD hallgató

[1] Santhi S. Dr, Saravanakumar Ar, 2020: The Economic Development of Singapore, 2020: A Historical Perspective. Aut Aut Research Journal. 11. évf. 7. szám. pp. 441-459.

[2] Reuters.com: Factbox: Global tech giants expanding in Singapore. https://www.reuters.com/article/us-singapore-technology-hiring-factbox-idUSKBN29W0GZ, (2021. 08. 22.)

amely az első ázsiai, csendes-óceáni térségbeli mérnöki központját Szingapúrban fogja létrehozni.[3] A vállalkozások helyzete, különösen a kis-és középvállalkozások (kkv) gazdasági relevanciája és társadalmi elfogadottsága eltérően alakult a gyarmati időszakban és az ország függetlenedését követően.

A gyarmati időszakban (1819-1965) a vállalkozások társadalmi reputációja meglehetősen alacsony szinten állt[4], megítélésük megközelítőleg sem volt pozitív. A gyarmati országban alapvetően nem létezett egy stabil vállalkozói réteg, sem vállalkozói kultúra. Ellenkezőleg, inkább az volt a jellemző, hogy kevés vállalkozás működött és inkább a környező országokból érkeztek azok – a mai szemmel úttörő – vállalkozók, akik létrehozták az első vállalkozásokat. A korai betelepülő vállalkozók célja a letelepedés mellett, a családjuk eltartására alkalmas gazdasági egzisztencia megteremtésé volt. Ebből következően döntően családi vállalkozások jöttek létre, amelyek tevékenységét a betelepülő vállalkozók szociális háttere predesztinált.[5] A korai családi vállalkozások sorsa pedig eltérően alakult, hiszen az évek múlásával vagy végleg befejezték tevékenységüket vagy napjainkra egy adott szektorban, mint például az egészségügy mérvadó piaci szereplőivé váltak. A hosszabb távú sikeres működés részben összefüggésben áll, a vállalkozások állami és társadalmi szintű megítélésében bekövetkezett változással.

Az ország függetlenedését követő első évtizedekben (1985) ugyanis a kkv-k társadalmi megítélése megváltozott, gazdasági relevanciájuk megnövekedett. A globalizáció és a technológia ágazatokon átívelő térnyerése, ahhoz az állami felismeréshez vezetett, hogy hosszú távon a tudásalapú gazdaság kiépítése (*knowledge-based economy*) fogja biztosítani az ország versenyképességének növekedését és megőrzését. A tudásalapú társadalomban pedig a kkv szektorban foglalkoztatott magasan képzett emberi erőforrások dominanciája a jellemző, így nem meglepő, hogy kormányzati célként fogalmazódott meg a kkv szektor megerősítésének elősegítése[6], amely sikeresen abszolválásra került még az évezredforduló előtt. A kkv szektor megszilárdulása, pedig egyike volt azoknak az előfeltételeknek, amelyek megalapozták, az ország napjainkban tapasztalható üzleti- és kripto szférában betöltött kulcsszerepét. További ilyen előfeltételként értékelhető, az országban érvényesülő a kedvező gazdasági jogi és kereskedelmi jogi szabályozás[7], valamint ezzel párhuzamosan a bíróságokkal szemben

[3] Blog.twitter.com: Announcing our first engineering center investment in Asia Pacific: https://blog.twitter.com/en_sea/topics/company/2020/singapore-engineering-center, (2021. 08. 22.)
[4] Lee Boon Chye, Tan Wee Liang 2002: Small and Medium Enterprises in Singapore and the New Economy. Cheltenham, UK. Edward Elgar. 369-374. pp.
[5] Lee Boon Chye, Tan Wee Liang i. m. p. 4.
[6] Lee Boon Chye, Tan Wee Liang i. m. p. 5.
[7] World Bank Group, 2020: Economy Profile of Singapore Doing Business., https://www.doingbusiness.org/content/dam/doingBusiness/country/s/singapore/SGP.pdf, pp. 6-8.

támasztott szigorú követelmény. Ez a gyors ügyintézést szorgalmazza, annak okán, hogy a bírósági rendszer lassúsága nem akadályozhatja az ország jövőbeli fejlődését.[8] Az utóbbi két tényezőnek a relevanciája megkérdőjelezhetetlen, ugyanakkor a kripto szektor vonatkozásában még ennél is jelentősebb a pénzügyi felügyeleti szerv tevékenysége és a pénzügyi szolgáltatásokat érintő jogi szabályozás alakulása.

2. A szingapúri felügyeleti szerv jelentősége a kriptoszektor vonatkozásában

A pénzügyi piacok feletti felügyelet effektív és eredményes ellátása garanciális kérdés a pénzügyi piacok transzparens működésének fenntartásához és megőrzéséhez, és ez nincsen másként a kripto piacok esetében sem. A pénzügyi felügyeleti szerv jelentősége többek mellett abban ragadható meg, hogy a felügyelet végzi a kriptoszolgáltatások, mint például a kriptotőzsdék engedélyezését.

A pénzügyi piac országonként eltérő megközelítéséből eredően, történetileg[9] négy mérvadó pénzügyi felügyeleti megközelítés alakult ki. Ezek a tradicionális (*intitutional, traditional*), a funkcionális (*functional*), az ún. „ikertorony" (*twin peaks*) és az integrált (*integrated, unified*) felügyeleti modellek.[10]

A tradicionális vagy institúcionális megközelítés alapján felépülő felügyeleti rendszer, alapkoncepciója az, hogy a pénzügyi piac három különböző szektorra bontható: 1) bankok, 2) biztosító társaságok, 3) értékpapírok.[11] Ebben a megközelítésben, egy pénzügyi intézmény alaptevékenysége (*core business*) határozta meg annak ágazati besorolását, amely pedig predesztinálta az engedélyezett és ellátható tevékenységek körét.[12] Vagyis mindegyik szektor felett különálló felügyeleti szerv látta el a felügyeleti tevékenységet. Ugyanakkor ez a felügyeleti megközelítés az idő múlásával, a különböző szektorok közötti különbségek összemosódásával elhalt.[13]

---

[8] Phang, Andrew, 2000-2001: "The Singapore Legal System - History, Theory and Practice." Singapore Law Review, 2000-2001. 21. szám. p. 33.

[9] Group of Thirty, 2008: The structure of Financial Supervision Approaches and Challenges in a Global Marketplace. Washington D. C., pp. 13-15 **Hiba! A hiperhivatkozás érvénytelen.**https://group30.org/images/uploads/publications/G30_StructureFinancialSupervision2008.pdf, (2021. 07. 10.)

[10] Kálmán János: A pénzügyi felügyeletek szervezeti megoldásai, különös tekintettel az USA-ra és Kínára. Diskurzus. Batthány Lajos Szakkollégiumi Tudományos Folyóirat 2011/ 2. szám, pp. 38-40.

[11] Samuel J Denton, 2016-2017: The Institutional Structure of Financial Regulation in the UK: The Final Reforms?, p.6.,**Hiba! A hiperhivatkozás érvénytelen.**https://www.academia.edu/38351799/The_Institutional_Structure_of_Financial_Regulation_in_the_UK_The_Final_Reforms, (2021. 10. 11.)

[12] Wymeersch, Eddy, 2007: The structure of financial supervision in Europe: about single, twin peaks and multiple financial supervisors. European Business Organization Law Review, 8. évf. 2. szám, pp. 237-306.

[13] Donato Masciandaro, 2005: Financial Supervision Architectures and the Role of Central Banks. 2005. Transnational Lawyer,18. évf. 2. szám. p. 351.

A funkcionális megközelítés, kvázi a tradicionális megközelítésnek egyik alternatívája, ezért annak tükrében értelmezhető a legegyszerűbben. Amíg a tradicionális megközelítés alapján a különböző pénzügyi szektorokba tartozó pénzügyi intézmények, különböző felügyeleti szervek hatálya alá esnek, addig a funkcionális megközelítésben, az adott pénzügyi intézmény által végzett különböző tevékenységek tartoznak különböző felügyeleti szervek alá. Ennek a megközelítésnek további jellemzője, hogy nem vizsgálja a pénzügyi intézmény jogi státuszát, kifejezetten annak tevékenységére az ellátott funkciókra koncentrál, ezért a több típusú tevékenységet folytató pénzügyi intézmény több felügyeleti szerv felügyelete alá tartozik[14].

Az ún. ikertorony (*twin peaks*) megközelítés, két hatóságot foglal magába, amelyek együttesen felelnek a pénzügyi rendszer[15] megbízhatóságának biztosításáért és a befektetők védelméért.[16] Ebben a felügyelti struktúrában az egyik hatóság a mikro- és makroprudenciális felügyeletért felel[17], a másik pedig a befektetői érdekvédelemmel foglalkozik.[18]

Végül az integrált vagy egységes (*unified*) megközelítés esetében egyetlen hatóság található a pénzügyi piacok felett, amely ellátja azok felügyeletét.[19] Kiegészítésként álljon itt, hogy a bemutatott felügyeleti modellek tiszta formában csak az absztrakció szintjén léteznek. A valóságban egy felügyeleti szervet az adott ország történelmi útja, kultúrája, valamint gazdasági és jogi berendezkedése is alakítani fog. A ténylegesen működő felügyeleti megközelítéstől függetlenül a felügyeleti szerv és a központi bank között olyan kapcsolatnak kell fennállnia, amely figyelemmel van a monetáris stabilitás és a pénzügyi stabilitás közötti lehetséges kapcsolatokra.[20]

A jelen vizsgálódás tárgyát képező Szingapúrban, egyrészt a pénzügyi és a kripto piacok feletti felügyeleti tevékenységet, másrészt az állam központi bankjának a szerepét is betölti a Szingapúri Monetáris Hatóság (Monetary Authority of Singapore, MAS). A MAS több évtizede a fentebb bemutatott felügyeleti megközelítések közül az integrált modell alapján működik.[21] Ebből következően tevékenységének kifejtése során négy területet felügyel, ezek a

[14] Dr. Andy Schmulow, 2015: Approaches to Financial System Regulation: An International Comparative Survey. Working Paper No. 053/2015 / Project No. E018., p. 8.
[15] Szilovics Csaba, 2020: Pénzügyi Jog. Pécs, Inter-Szféra Kft., p. 374.
[16] Michael W. Taylor: The Road from Twin Peaks – and the Way Back. Connecticut Insurance Law Journal. 2009-2010. 16. évf. 1. szám. pp. 90-91.
[17] Michael Taylor, 1999: „Twin Peaks": A regulatory structure for the new century. CSFI. p.15.
[18] Clive Briault, 2002: The Rationale for a Single National Financial Services Regulator. Financial Services Authority Occasional Paper. 16. szám. p. 24.
[19] Dirk Schoenmaker, Nicolas Véron, 2017: A 'twin peaks' vision for Europe. Policy Contributions, 30. szám, p. 3.
[20] Charles Goodhart, Dirk Schoenmaker: Should the Functions of Monetary Policy and Banking Supervision Be Separated? Oxford Economic Papers, 1995. 47. évf. 4. szám, pp. 539- 660.
[21] Michael Taylor, Alex Fleming, 1999: Integrated Financial Supervision Lessons of Scandinavian Experience. A quarterly magazine of the IMF. 36. évf. 4. szám. p. 45.

bankszektor, a tőkepiacok, a biztosítótársaságok és a pénzforgalmi szolgáltatások. Figyelemmel arra, hogy a 2020-ban hatályba lépett pénzforgalmi szolgáltatásokról szóló törvényben meghatározott hét pénzforgalmi szolgáltatás egyikét a digitális fizetési token szolgáltatás képezi, az ilyen szolgáltatásokat nyújtó szervezetek, így például a kripto-tőzsdék a MAS hatálya alatt állnak, jogszerű tevékenységüket csak érvényes engedéllyel végezhetik.

3. 2020-as pénzügyi szolgáltatásokról szóló törvény módosítása

2019. január 14-én a szingapúri parlament elfogadta a pénzforgalmi szolgáltatási törvényt (Payment Services Act 2019, PSA) amely 2020 január 28. napján lépett hatályba. A törvény létrehívása többek között a MAS azon felismerésére vezethető vissza, miszerint a technológiai innováció különösen a fintech megoldások térnyerése átalakítja és megreformálja a pénzügyek és a fizetések világát.[22] Az új fizetési módszerek elterjedésével párhuzamban, viszont az adócsalás[23] és a terrorizmusfinanszírozás új megjelenési formáival is számolni kell.[24] Ezeket a kockázati tényezőket súlyuknak megfelelően mérlegelve a szingapúri keretszabályozás, kockázatközpontú szemléletmódot követ és a hangsúlyt a megelőzésre fekteti, azzal, hogy ahol lehetséges, ott a hatályos szabályozást rendeli alkalmazni. Ennek a törekvésnek a gyakorlati megnyilvánulása többek között az, hogy a pénzügyi szolgáltatások nyújtása érvényes működési engedély meglétéhez kötött, valamint az engedélyt elnyert szervezeteknek a mindenkor hatályos pénzmosás és terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló jogszabályok következetes betartásáról gondoskodniuk kell.[25]

A továbbiakban a PSA által bevezetett új jogi terminológiák, így a digitális fizetési token szolgáltatások, a digitális fizetési tokenek kibontására szorítkoznék, kiegészülve az ilyen szolgáltatásokat nyújtó szervezetek bemutatásával.

A PSA jogszabály összesen hét önálló nevesített pénzforgalmi szolgáltatással operál[26], amely közül az egyik a digitális fizetési token szolgáltatás, amely szolgáltatásnak tárgyát a

[22] Ong Ye Kung: "Payment Services Bill" – Second Reading Speech, https://www.mas.gov.sg/news/speeches/2019/payment-services-bill (2021. 10. 17.)

[23] Szívós Alexander, 2021: A kriptoeszközök és az adózás In: Bujtár, Zsolt; Szívós, Alexander Roland; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics, Botond (szerk.) Kriptoeszközök világa a jog és gazdaság szemszögéből Konferenciakötet - Válogatott tanulmányok Pécs, Magyarország. Pécsi Tudományegyetem, Állam- és Jogtudományi Kar., pp. 12-23.

[24] Tóth Dávid, 2020: A pénz- és bélyegforgalom biztonsága elleni deliktumok büntetőjogi és kriminológiai aspektusai. Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar., p. 211.

[25] Monetary Authority of Singapore, 2019: Consultation paper. Consultation on the Payment Services Act 2019: Scope of Emoney and Digital Payment Tokens. P016-2019 december, p. 12.

[26] PSA 1. sz. melléklet 1. a)-g). https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220, (2021. 11. 02.)

digitális fizetési tokenek képezik. A jogszabály további nóvuma, hogy ex lege meghatározza a digitális fizetési token fogalmát, ezzel új és önálló eszközkategóriát teremt, elhatárolva a digitális fizetési tokeneket az elektronikus pénztől (e-money).[27] [28] De a jogi fogalomalkotás szintén megakadályozhatja a jogbizonytalanság kialakulását.

A digitális fizetési tokenek, önálló jogi kategóriát képeznek, a gyakorlatban de facto különbséget tehetünk, a utility, security[29] és a payment tokenek között.[30] Más megközelítések a payment tokenek helyett a currency token kategóriával operálnak.[31] A utility tokenek, alapvetően a tulajdonosnak biztosítanak hozzáférést egy létező vagy jövőbeli szolgáltatáshoz vagy termékhez. Lényeges viszont, hogy a tulajdonost nem illetik meg azok a jogok és nem terhelik azok a kötelezettségek, amelyek egy értékpapír esetén.[32] Ezzel szemben a security tokenek tulajdonosi pozíciót jelölnek és nyereségrészesedést biztosítanak adott kripto megoldás vonatkozásában, így amennyiben nincs speciális szabályozás az értékpapírra vonatkozó szabályok nyernek alkalmazást esetükben.[33] [34] A payment tokennek, mint például a Bitcoin (BTC), körébe azok a kriptoeszközök tartoznak, amelyek funkciója a felek közötti fizetési műveletek lebonyolítása.[35] A felsorolás ugyan nem tartalmazza a presale tokenek kategóriáját, egy gondolat erejéig azonban érdemes megemlíteni. A presale tokenek meghatározó jelentősége döntően az elsődleges nyilvános érmekibocsátások (ICO) aranykorában volt

[27] Monetary Authority of Singapore, 2019: Consultation paper. Consultation on the Payment Services Act 2019: Scope of Emoney and Digital Payment Tokens. P016-2019 december, p. 9.
[28] Szilovics Csaba: A kriptovaluták pénzfunkciójáról és gazdasági, társadalmi jelentőségéről In: Bujtár, Zsolt; Szívós, Alexander Roland; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics, Botond (szerk.) Kriptoeszközök világa a jog és gazdaság szemszögéből, 2021 : Konferenciakötet - Válogatott tanulmányok Pécs, Magyarország : Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, pp. 24-33.
[29] A security, equity vagy investment token elnevezések egymás szinonimái.
[30] A felsorolás példálózó jellegű.
[31] Michael Jünemann, Johannes Wirtz: ICO: Regulation of Types of Token in Germany. https://www.twobirds.com/en/news/articles/2018/germany/ico-arten-und-regulierung-von-tokens, (2021. 10. 29.)
[32] A gyakorlatban például *utility tokenek* bocsátanak ki innovatív technológiai megoldások fejlesztői csapatának, a marketingeseknek illetve más közreműködő személyeknek, akik így adott kriptovaluta platform szolgáltatásaihoz kedvezményesen hozzáférnek.
[33] The Authority of audit, accounting, property, property valuation and insolvency management under the Ministry of Finance of the Republic of Lithuania (AVNT): Accounting Guidelines on Cryptocurrency and Tokens. http://www.avnt.lt/assets/Veiklos-sritys/Apskaita/VAS/Euras-ir-kriptovaliuta/2018-06-07-Cryptocurrencies-accounting-guidance.pdf, (2021. 10. 29.)
[34] The Swiss Financial Market Supervisory Authority (FINMA), **Hiba! A hiperhivatkozás érvénytelen.**https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/, (2021. 11. 02.)
[35] Di Angelo Monika, Salzer Gernot: Tokens, Types, and Standards: Identification and Utilization in Ethereum. 2020. Conference: The 2nd IEEE International Conference on Decentralized Applications and Infrastructures. p. 2.

érzékelhető.[36] A presale tokenek jellemzően a pre-ICO folyamán kerültek kibocsátásra és elővásárlási jogot biztosítottak a később kibocsátásra kerülő kripto eszközök jegyzésére.[37]

A tokenek közötti különbségtétel, nem csak elméleti síkon, de a gyakorlatban is relevanciával bír, hiszen nem minden token kategória tartozik a jogi szabályozás alá. Így Szingapúrban a hatályos jogi szabályozás a security és a payment tokenek kategóriáját lefedi, viszont a utility tokenek kívül esnek a jogalkotás látókörén. A security tokenek 2017 óta az értékpapír törvény hatálya alá tartoznak[38], amennyiben annak törvényi feltételei fennállnak.[39],[40] A payment tokenek vonatkozásában a PSA törvény rendelkezései lesznek relevánsak. A jogszabály alapján digitális fizetési token bármely olyan digitális értékmegjelenítő eszköz, amely egységet képez, nem denominált fiat pénzben vagy nem kötődik azokhoz, továbbá nyilvánosan (köz által) elfogadott fizetési eszköz és elektronikusan tárolható, átruházható és kereskedhető, valamint a MAS által esetlegesen meghatározott további előírásoknak megfelel. A digitális fizetési tokenekkel szemben támasztott törvényi feltételek konjunktívak, így valamelyik hiánya esetén, az eszköz nem minősül digitális fizetési tokennek.

A kriptotőzsdék a szingapúri tőkepiaci szabályozás értelmében szabályozott piactereknek minősülnek[41], amelyek gyakorlatilag online interaktív felületeket jelentenek. Ezeknek az online felületeknek és a kapcsolódó szolgáltatásoknak – szervezettől független – közös jellemzője, hogy interneten keresztül vagy natív okostelefon applikációkon keresztül érhetők el és használhatók. A tradicionális értéktőzsdék-és árutőzsdék jellemzője, hogy az eladókat és a vevőket egy helyre tömöríti (konszolidált piactér), ebből következően a szereplők könnyen beléphetnek és kiléphetnek (eladási-vételi) a pozíciókba, amely likviditást biztosít a piacnak. A kriptotőzsdék a kriptovaluták kereskedését teszik könnyen elérhetővé. A kriptotőzsdéket működésük alapján jelenleg két csoportba sorolhatjuk, így különbséget tehetünk a DEX (decentralized exchanges)[42] és a CEX (centralized exchanges) között.[43]

---

[36] Breszkovics Botond: Az elsődleges nyilvános érmekibocsátás előtti jogi teendők Európában. In: Bujtár Zsolt; Szívós Alexander Roland; Gáspár Zsolt; Szilovics Csaba; Breszkovics Botond (szerk.) Kriptoeszközök világa a jog és gazdaság szemszögéből, 2021 : Konferenciakötet - Válogatott tanulmányok. Pécs, Magyarország: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, pp. 136-158.

[37] Dan Seitz: What Is a Token Presale and How Does It Work, https://www.bitcoinmarketjournal.com/token-presale/, (2021. 10. 29.)

[38] Bujtár Zsolt, 2021: Az értékpapírosítás. Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, p. 243.

[39] Monetary Authority of Singapore: MAS clarifies regulatory position on the offer of digital tokens in Singapore. Elérhető: https://www.mas.gov.sg/news/media-releases/2017/mas-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-singapore, (2021. 10. 29.)

[40] Securities and Futures Act (Cap. 289). https://sso.agc.gov.sg/Act/SFA2001?ProvIds=P1II-#top, (2021. 10. 29.)

[41] Securities and Futures Ac (Cap. 289) Második rész., https://sso.agc.gov.sg/Act/SFA2001?ProvIds=P1II-#top (2021. 10. 29.)

[42] Angelo Aspris, Sean Foley, Jiri Svec, Leqi Wang, 2021: Decentralized exchanges: The "wild west" of cryptocurrency trading. International Review of Financial Analysis, 77 évf. C. szám, 1-10. pp.

[43] A Binance például a CEX tőzsdetípusba tartozik.

A CEX sok hasonlóságot mutat a klasszikus tőzsdékkel, hiszen ez esetben is egy olyan tőzsdei/kereskedési felületről van szó, amely egyrészt megbízható közvetítőként funkcionál a tranzakciók lebonyolítása során, másrészt pedig a befizetett fiatpénzek és/vagy kriptovaluták vonatkozásban őrzési szolgáltatást (custodial service) nyújt. Ez utóbbi tulajdonsága miatt a CEX felületeken a regisztrált felhasználók nem rendelkeznek saját privát kulccsal a pénztárcájukhoz, amelyben a kriptovalutáikat tartják, mert azokat a kriptotőzsde elkülönített pénztárcában „őrzi[44]". A CEX kereskedési felületek további jellemzője, hogy nagy hangsúlyt fektetnek a jogi megfelelőség biztosítására. Így szigorú ügyfélazonosítást végeznek (KYC) valamint a mindenkori pénzmosás- és terrorizmusfinanszírozás elleni küzdelemmel kapcsolatos jogszabályok betartásával működnek/fejtik ki tevékenységüket. Ezzel szemben a DEX kereskedési felületeken nincs KYC azonosítás, valamint a felhasználók személyes adatainak tárolására sem kerül sor. Eltérés van abban is, hogy a DEX felületén nincs megbízható közvetítő személy, a tranzakciók közvetlenül a felek között (P2P) mennek végbe transzparens módon. A felhasználók a DEX kereskedési felületet lényegében csak a tranzakciók végrehajtásához használják, a kriptovalutákat pedig saját pénztárcájukban tárolják. A különböző működésű kriptotőzsdék előnyeinek és hátrányainak ismertetésétől jelen tanulmányban eltekintenék.

Megjelenési idejük szerint a centralizált kriptotőzsdék (CEX) korábban jelentek meg mint a decentralizált kriptotőzsdék (DEX). Ez utóbbi DEX kereskedési felületek, mint például az UNISWAP megszületése, főleg válaszadásnak tekinthető a CEX kereskedési felületeken felmerült problémák orvoslására, mint például a kibertámadások.[45][46] Véleményem szerint, ezen túlmutatóan a DEX-ek terjedése mögött a decentralizált pénzügyi szolgáltatásokat (DeFi) érintő általános hype is megjelölhető, viszont a DEX-en a megfelelő likviditás biztosítása még a jövő feladata, amely a hibrid felületek megjelenésének is teret engedhet.

A kriptotőzsdék működésétől és népszerűségüktől függetlenül, Szingapúrban egységesen a MAS felügyelete alatt állnak, tekintettel arra, hogy ezeken a felületeken pénzforgalmi szolgáltatásokat nyújtanak. A hatályos jogi szabályozás alapján pedig minden olyan szervezetnek, amely bármilyen típusú pénzforgalmi szolgáltatást nyújt, főszabály szerint engedélyre[47] van szüksége, kivéve, ha ez alól egyébként mentességet élvez. A PSA

[44] Ezért a kriptotőzsdék esetében ún. hot- vagy custodial-wallettben tárolják a kriptovalutákat. Viszont nagyobb összegek huzamos ideig tartó tárolása kockázatos lehet az ilyen felületeken, ezért célszerűbb azokat ún. cold- vagy non-custodial walletben tárolni.

[45] Joe Tidy: The real victims of mass crypto-hacks that keep happening, https://www.bbc.com/news/technology-58331959, (2021. 11. 06.)

[46] Tóth Dávid, Gáspár, Zsolt, 2020: Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés területén. Büntetőjogi Szemle 2020. 2. évf. pp. 140-150.

[47] A benyújtott engedély elbírálása a MAS feladata.

hatálybalépését követően, azonban lehetősége nyílott a szervezeteknek, hogy előzetes jóváhagyás birtokában megkezdjék a tevékenységüket. Ennek a kivételszabálynak az alkalmazási feltétele az volt, hogy az érintett szervezeteknek a törvény hatálybalépését megelőzően, már szabályozott tevékenységet kellett folytatniuk, és a türelmi időn belül határozott kérelmet kellett benyújtaniuk, amely arra irányult, hogy mentesüljenek az engedélyezési eljárás alól. Ez a türelmi időszak a digitális fizetési szolgáltatók esetében 2020 januárjától július hónapjáig tartott. A MAS statisztikai adatai alapján, pedig a PSA hatálybalépését követően 480 engedély iránti kérelem érkezett, ebből 170 digitális fizetési token szolgáltatótól, mint például a Coinbase vagy a Kraken. A beérkezett kérelmekből 2021 július hónapjáig 30 kérelmet visszavontak, 2 pedig elutasítottak, míg a többi az utolsó fázisba került.[48] Ide kapcsolódóan három szervezetet emelnék ki a gyakorlatból, amelyek pozitív elbírálásban részesültek és elnyerték a MAS digitális fizetési token szolgáltatás nyújtásra irányuló engedélyét. Az első a szingapúri székhelyű fintech cég, a Fomo Pay, a második az ausztrál Independent Reserve[49] elnevezésű kriptovaluta tőzsde, végül a harmadik a szintén szingapúri DBS Bank Ltd. multinacionális banki és pénzügyi szolgáltató vállalat alá tartozó DBS Vickers.[50] A pozitív elbírálásban részesített szervezetek mellett azonban elutasító döntések is születtek. Példaként említhető a Bitcoin Exchange Pte Ltd. szervezet, amely digitális fizetési token szolgáltatást nyújt, azonban nem tudott a kedvezményes szabályozási lehetőséggel élni.[51] Ez a tendencia álláspontom szerint a MAS szigorú felügyeleti szemlélet módját tükrözi, amely a jogszerű működés és a transzparens piaci működés megőrzését szolgálja.

II. Külső hatások

1. Kína és a kripto-szektort sújtó intézkedések

Kína szkepticizmusa a kriptovalutákkal szemben nem újkeletű jelenség, figyelemmel arra, hogy az elmúlt közel egy évtizeden belül többször határozottan fellépett a kripto szektor ellen, különböző szigorításokkal bevezetésével.

---

[48] Chua Kheng Wee Louis, 2021: Reply to Parliamentary Question on Digital Payment Token Service Provider Applicants. https://www.mas.gov.sg/news/parliamentary-replies/2021/reply-to-parliamentary-question-on-digital-payment-token-service-provider-applicants, (2021. 10. 30)

[49] Ethan Wu: Singapore grants its first-ever crypto exchange license as the industry remains wary of China. **Hiba! A hiperhivatkozás érvénytelen.**https://markets.businessinsider.com/news/currencies/singapore-crypto-china-hong-kong-exchange-binance-2021-08, (2021. 10. 17.)

[50] DBS.com: DBS Vickers receives regulatory approval under Payment Services Act to provide digital payment token services. https://www.dbs.com/newsroom/DBS_Vickers_receives_regulatory_approval_under_Payment_Services_Act_to_provide_digital_payment_token_services, (2021. 10. 29.)

[51] Entities that are no longer exempt pursuant to the Payment Services (Exemption for Specified Period) Regulations 2019 ("Exemption Regulations"). https://www.mas.gov.sg/regulation/payments/entities-that-are-no-longer-exempt-pursuant-to-the-ps-esp-r, (2021. 10. 30.)

Kronológiai sorrendben haladva Kína legelső kripto-szektort érintő korlátozó intézkedése 2013-ra datálható. Ebben az évben az ország megtiltotta a pénzintézeteknek, a BTC-vel folytatott tranzakciók lebonyolítását. A döntés mögöttes oka az volt, hogy a Bitcoin, nem rendelkezik jogi státusszal és nem használható fizetőeszközként, valamint annak decentralizált jellege is aggályos.[52] Ugyanakkor lényeges, hogy a döntést követően a magánszemélyek továbbra is szabadon kereskedhettek BTC-vel, a kapcsolódó kockázatok tudomásul vételével. Ezt követően 2017-ben a Kínai Jegybank (People's Bank of China, PBOC) megtiltotta az elsődleges nyilvános érmekibocsátásokat (ICO) az országban, az alternatív forrásbevonási módban rejlő potenciális veszélyek miatt.[53] A 2017-es Kínai ICO tiltással kapcsolatban azonban érdemes megemlíteni, hogy ekkor a Szingapúri MAS is hasonló álláspontot helyezkedett el, hiszen egy augusztus hónapban kiadott állásfoglalásában kifejezésre juttatta, hogy „az ICO-k rövid időn belüli nagy tőkebevonási képessége a terrorizmus finanszírozás és a pénzmosás melegágya lehet".[54] Ezen túlmutatóan még ebben az évben, további, a belföldi (illetőségű) székhelyű kripto-tőzsdék tevékenységét korlátozó intézkedések léptek érvénybe. Ennek következtében a kereskedési felületeken tiltásra került 1) a kriptovaluták és fiat pénzek átváltása; 2) kriptovaluta kereskedés (vétel-eladás); valamint 3) a kriptovalutákhoz vagy virtuális valutákhoz kapcsolódó kereskedelmi ügynöki szolgáltatások nyújtása.[55] Ez utóbbi korlátozó intézkedés elrendelése mögött döntően az állt, hogy a befektetők a nemzeti fizetőeszköz a kínai jüan (CNY) ellen kezdtek el kereskedni a BTC javára. A korlátozásnak mind a kriptovaluták piacára, mind a kripto-tőzsdék működésére káros hatása volt. A kriptovaluta árfolyamok esni kezdtek, így például a BTC 30%-ot, de a történeti adatok[56] alapján tudhatjuk, hogy még abban az év decemberében a BTC új történelmi rekordot döntött, amikor elérte a 20.000 USD-t. Így álláspontom szerint ennek a szigorításnak, káros következményei nem a kriptovaluték piacát érintették meghatározó mértékben, sokkal inkább annak a káros gyakorlatnak nyitottak teret, hogy elkezdődött az offshore kripto-tőzsdék megjelenése.

[52] Lauren Gloudeman, 2014: Bitcoin's Uncertain Future in China. USCC Economic Issue Brief. 4. évf. p. 6.

[53] Tai Zhong: 中国人民银行 中央网信办 工业和信息化部 工商总局 银监会 证监会 保监会关于防范代币发行融资风险的公告.: http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html, (2021. 10. 31.)

[54] MAS: MAS clarifies regulatory position on the offer of digital tokens in singapore. https://www.mas.gov.sg/news/media-releases/2017/mas-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-singapore, (2021. 11. 01.)

[55] Greg Pilarowski, Lu Yue: China Bans Initial Coin Offerings and Cryptocurrency Trading Platforms. China Regulation Watch., p. 3.

[56] Statista: Bitcoin price index. **Hiba! A hiperhivatkozás érvénytelen.**https://www.statista.com/statistics/326707/bitcoin-price-index/, (2022. 01. 05.)

Példaként említhető az azonnali és a derivatív kereskedést egyaránt lehetővé tevő Huobi és OKEx kripto-tőzsdék, amelyek a Seychelle-szigeteken vannak bejegyezve.

Majd 4 év távlatából vizsgálva 2021 május hónapjában eszközölt szigorú fellépést a kriptovaluták ellen, az a 2017-es évi intézkedések kiterjesztésének tekinthető. A szigorítások a kriptovalutákal kapcsolatos pénzügyi és fizetési szolgáltatásokat érintették. Ezen túlmutatóan a kínai klímacélok szem előtt tartásával, valamint a környezetvédelmi és fenntartható gazdaságot tartó törekvések fényében a bányász tevékenység kitiltása is megkezdődött. Belső-Mongólia autonóm régió, egy kampányt indított a kriptovaluta-bányászat felszámolására, a szén-dioxid-kibocsátás csökkentése érdekében. Ennek okán létrehozott egy platformot, amelyen a lakosok bejelenthetik az illegális „bányász" tevékenységet.[57]

A kínai központi bank alá tartozó három szövetség, a Kínai Internet Pénzügyi Szövetség, a Kínai Bankszövetség és a Kínai Fizetési és Elszámolási Szövetség közös közleményében figyelmeztetést adott ki, amelyben megtiltotta a pénzintézeteknek és a pénzügyi vállalatoknak, hogy közvetlenül vagy közvetve kriptovaluta-szolgáltatásokat nyújtsanak az ügyfeleiknek.[58] Az új tilalom olyan szolgáltatásokra is kiterjed, amelyekről korábban nem esett szó. Például egyértelművé tette, hogy az intézmények nem fogadhatnak el virtuális valutákat, és nem használhatják azokat fizetési és elszámolási eszközként. Az intézmények nem végezhetnek kriptovaluták és jüan vagy külföldi valuták közötti csereügyleteket sem.

Végül 2021. szeptember 24. napján a Kínai Jegybank (People's Bank of China) közleményt tett közzé, amelyben bejelentette, hogy megtilt minden kriptovalutával kapcsolatos műveletet. A közlemény szerint minden kriptovalutával folytatott művelet "tiltott pénzügyi tevékenységnek" minősül, amely büntetőjogi felelősségre vonást is eredményezhet. A tiltás kiterjedt jellegét és teljeskörűségre való törekvését tükrözi, hogy szemben a 2017-ben érvénybe lépett szigorításokkal, amelyek a belföldi kripto-tőzsdéket célozták, jelenleg a tengeren túli, offshore[59] kripto-tőzsdék által kínai állampolgároknak nyújtott szolgáltatások is illegális tevékenységnek minősülnek.[60]

---

[57] Inner Mongolia Development and Reform Comission: **关于**设立虚拟货币"**挖**矿"**企**业举报平台的公**告** http://fgw.nmg.gov.cn/xxgk/zxzx/tzgg/202105/t20210518_1502529.html, (2021. 10. 31.)

[58] The People's Bank of China: **中国互**联网金融协会 **中国**银行业协会 **中国支付清算**协会关于防范虚拟货币交易炒作风险的公**告**. https://mp.weixin.qq.com/s/ZcIWk3hcQNp-vnp08nHyQg, (2021. 10. 31.)

[59] Bánfai Edina, Bujtár Zsolt, Ferencz, Barnabás, 2017: Lehetőségek és veszélyek az offshore-jelenségben. Polgári szemle: gazdasági és társadalmi folyóirat 2017. 13 évf. 1-3. szám, pp. 321-335.

[60] The People's Bank of China: **关于**进一步防范和处置虚拟货币交易炒作风险的通知. http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4348521/index.html, (2021. 11. 01.)

Az elmúlt években alkalmazott tilalmak álláspontom szerint jól tükrözik, hogy azok alapvetően mindig a kripto szektorban aktuálisan uralkodó trendek visszaszorítására, mérséklésére irányultak. Véleményem szerint, ezeknek a korlátozó intézkedéseknek a hátterében, alapvetően az a konzervatív szabályozási megközelítés áll, amely az ország gazdasági védelmét, a befektetői érdekvédelmet, valamint a fejlesztés alatt álló digitális jegybankpénz a digitális jüan (e-CNY)[61] bevezetésének védelmét helyezi előtérbe.

III. Záró gondolatok

Véleményem szerint, annak okán, hogy Szingapúr az ezredforduló előtt felismerte a kkv szektor és a tudás alapú gazdaság relevanciáját, a városállam predesztinálta saját gazdasági útját, amely napjaink egyik meghatározó üzleti és pénzügyi központjává emelte. A városállam technológiai innovációra való nyitottsága és nagy adaptációs képessége, kiegészülve a kedvező jogszabályi környezettel, együttesen elősegíthetik, hogy az elkövetkező években egy meghatározó kripto-központtá emelkedjen. Ezen túlmutatóan Szingapúrnak a kripto-tőzsdék új és kiemelt célpontjává válását elősegítő külső hatásként értékeltem a Kínában az elmúlt évtizedben folyamatosan megjelenő és a kriptoszektort sújtó tilalmakat, amelyek lokálisan a kripto erőviszonyok térségbeli átrendeződését eredményezték. Ugyanakkor a kínai tiltásoknak olyan következményei is keletkeztek, amelyek túlmutatnak a régió határain és a bányászati kapacitás erőviszonyainak megváltozásában, az alternatív bányászati megoldások keresésében jelölhetők meg. A kínai tiltás a bányászok exodusát eredményezte az országból, aminek következményeként nagy mennyiségű használt videókártya jelent meg az online piactereken. Kriptovaluta bányászati szempontból új területek és országok[62] kerültek célkeresztbe, így például preferált térséggé válhatnak az Egyesült Államok kriptobarát szabályozást követő szövetségi államai[63], élre törve a bányászati erőkapacitás vonatkozásában.[64]

[61] Bujtár Zsolt, 2020: Central bank-issued digital currencies: - ready, steady, go? In: Szilovics, Csaba; Bujtár, Zsolt; Ferencz, Barnabás; Breszkovics, Botond; Szívós, Alexander Roland (szerk.) Gazdaság és pénzügyek a 21. században II. - konferenciakötet = business and economy in the 21st century II. – conference proceedings. Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, pp. 113-123.

[62] Lásd például: Gáspár Zsolt, 2022: Az el salvadori Bitcoin-törvény gazdasági és jogi aspektusai. In: Bujtár, Zsolt; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics, Botond; Ázsoth, Szilvia; Szívós, Alexander Roland (szerk.) Fenntartható növekedés (ESG) jogi és gazdasági aspektusai. Pécs, Pécsi Tudományegyetem Állam-és Jogtudományi Kar, pp. 39-51.

[63] Breszkovics Botond: Wyoming: Liberal crypto regulation. In: Csiszár Beáta, Hankó Csilla, Kajos Luca Fanni, Mező Emerencia (szerk.) IX. Interdiszciplináris Doktorandusz Konferencia. Tanulmánykötet. Pécs, Pécsi Tudományegyetem Doktorandusz Önkormányzat, 2020., pp. 100-109.

[64] Cambridge bitcoin electricity consumption index: https://cbeci.org/index, (2021. 11. 25.)

Bujtár Zsolt*: A decentralizált pénzügyek (DeFi) főbb jogi szabályozási kihívásai

Absztrakt:

A kriptoeszközök több mint 10 éves története nemcsak több mint tizenötezer kriptoeszköz létrejöttét, de egy önálló ökoszisztémát is, a decentralizált pénzügyek (Decentralized Finance - DeFi) kialakulását is eredményezte. A jelen tanulmány azt vizsgálja, hogy ez az új pénzügyi rendszer (DeFi) és annak egyes jellemzői milyen kockázatokat hordoznak magukban és azok miként kezelhetők a jog eszközrendszerével. A tanulmány először meghatározza a DeFi jellemzőit és részeit, majd ezt követően beazonosítja a DeFi legfontosabb makroszintű kockázatait és végül vizsgálja a kockázatok kezelésének lehetséges módjait.

Kulcsszavak: *DeFi, makroprudenciális kockázatok, kriptoeszközök, stabil kriptopénz*

I. A decentralizált pénzügyek (Decentralizált Pénzügyek – DeFi) rendszere

A DeFi a blokklánc technológiára alapozott pénzügyi szolgáltatások olyan autonóm módon, előre programozott pénzügyi szolgáltatások összessége, mely tárgya meghatározó mértékben kriptoeszköz és melynek meghatározó közvetítő eszköze a stabil kriptopénz.[1] A DeFi jellemző szolgáltatásai a hagyományos pénzügyi rendszer univerzális banki szolgáltatásaihoz hasonlítanak azáltal, hogy ahhoz hasonlóan fizetési szolgáltatásokat úgy mint hitelezési tevékenységet, biztosítási tevékenységet, vagyonkezelési és értékpapír kereskedési és befektetési szolgáltatásokat foglal magában. Az egyedi szolgáltatások tényleges tartalma jelentősen módosítja a DeFi-ről alkotott képet. Ezek a szolgáltatások már egy új, jelentős kihívások előtt álló globális pénzügyi rendszert jelenítenek meg a jogalkotó és jogalkalmazó számára egyaránt, különösen, a pénzügyi rendszer biztonságos működtetése[2] és stabilitásának fenntartása szempontjából.

* Dr. Bujtár Zsolt, PhD, PTE ÁJK Pénzügyi Jogi és Gazdasági Jogi tanszék, adjunktus, bujtar.zsolt@ajk.pte.hu

[1] BIS International banking and financial market developments Quarterly Review december, 2021, p. 21.

[2] Szilovics Csaba, 2003: A magyar államháztartás pénzügyi rendszere In: [s n,] (szerk.) Adójog alapjai. Illetékjog. A magyar államháztartás pénzügyi rendszere Pécs, PTE Állam- és Jogtudományi Kar. pp. 65-67. és Szilovics Csaba, 1997: Az államháztartás pénzügyi jogi rendszere Pécs, Magyarország: Janus Pannonius Tudományegyetem, p. 62.

A DeFi a fenti kockázatok tekintetében meghatározó szolgáltatásai között magában foglalja a stabil kriptopénzeket (stablecoin), a kripto tőzsdéket (melyek inkább kripto kereskedési platformoknak tekinthetők), és a hozzájuk kapcsolódó vagyonkezelési szolgáltatásokat, illetve a hitelezést, az erre a digitalizált tőkepiaci szegmensre jellemző magas tőkeáttétellel, és az autonóm programozott működésből eredő nemteljesítés kockázatát csökkentő biztosításokat.

1. A DeFi felépítése – a meghatározó szolgáltatások köre

Az osztott főkönyvi technológia (Distributed Ledger Technology - DLT) alkalmazása a Defi – és általában a kriptoeszközök - esetében, lehetővé teszi az adatok decentralizált és egyidejű rögzítését és azok archiválását további felhasználás céljából. Ez a számítógépes hálózat, akár nyílt, akár zárt formában előre rögzített feltételek teljesítésével bővíthető, illetve a jogosultságok különböző szintjeivel korlátozható. Így lehetségessé válik a zártkörű működés is decentralizált módon, jelentős adatbiztonsággal, mely tény különösen fontos érzékeny adatokat kezelő iparágak a pénzügyi szolgáltatók, egészségügy vagy akár az élelmiszerbiztonság területein. A titkosítással tovább növelhető az adtabiztonság a nyílt hálózatok esetében is. A kriptoeszközök éppen ezt a magas szintű biztonságot biztosítják nyílt hálózat formájában a titkosítással: matematikai formulák, azaz algoritmusok segítségével létrehozott blokkok zárt láncolatával. Ezek az önálló adatblokkok képezik a blokklánc alapját, melyek úgy alkalmasak a biztonságos működésre, hogy az egyszer már több jóváhagyó által validált (érvényesnek nyilvánított) blokk a későbbiekben nem módosítható adattartalommal rendelkezik. A Bitcoin alkalmazta a kripto eszközök között elsőként ezt technológiát a decentralizált főkönyvi rendszerben működő közvetítő nélküli (peer-to-peer) elektronikus pénz létrehozásával. A Bitcoin alapdokumentumát (white paper) 2009-ben Satoshi Nakamoto néven közismert, bár konkrét személyazonossága tekintve azóta sem ismert személy hozta létre.[3]

A második generációs kriptoeszközök között az Ethereum és annak ERC20 kódja valósította meg a blokklánc technológia alkalmazás következő szintjét: az előre programozott szerződéseket (smart contracts), melyek lehetővé teszik, hogy további emberi beavatkozások nélkül valósuljanak meg pénzügyi tranzakciók.[4] Az okosszerződések alapvető pénzügyi műveletek (primary) programozott lebonyolítását teszik lehetővé. Ezen programozott eljárások jelentős előnye az élőmunka költségeinek és az emberi hibák lehetőségének az érdemi

[3] https://bitcoin.org/bitcoin.pdf, (2021.12.22.)
[4] Glavanits Judit, 2021: A blokklánc technológia közbeszerzési alkalmazási lehetőségei., In Bujtár, Zsolt (szerk.) ; Szívós, Alexander Roland (szerk.) ; Gáspár, Zsolt (szerk.) ; Szilovics, Csaba (szerk.) ; Breszkovics, Botond (szerk.) Kriptoeszközök világa a jog és gazdaság szemszögéből: Konferenciakötet - Válogatott tanulmányok p. 91

csökkentése. Ugyanakkor ez programozottság teszi sebezhetővé is a DeFi-t, azáltal, hogy ha az okosszerződés algoritmusa kijátszhatóvá válik például a kereslet, illetve a kínálat programozott, félrevezető megjelenítésével, tehát nem valós piaci igények generálásával. Ez a tőkepiac esetében tiltott magatartás a piaci manipuláció fogalomkörébe sorolható.[5] A DeFi esetében a szabályozás hiányában valós kockázatot jelent ez a manipulációs lehetőség egészen a szabályozás hatálya alá történő bevonásig.[6]

Az okosszerződések két új működési forma megjelenését is eredményezték: a decentralizált applikációk (Decentralized Applications - DAPP) és a decentralizált szervezetek (Decentralized Autonomous Organizations - DAO) személyében.[7] Mindkét megoldás az okosszerződések előre programozottságával él, és a létrehozótól látszólag független működést tesz lehetővé. Azáltal, hogy a működésük alapja az okosszerződések kapcsolt hálózata, sebezhetőségük is e jellemzőjükből fakad. Bármely személy, aki ismeri a nyílt forráskódú rendszer működését visszaélhet azzal.

A kriptoeszközök és a DeFi jelentős technológiai kihívása a skálázhatóság, hiszen a megnövekedett igényekre a DAPP vagy DAO[8] automatikusan az előre definiált mennyiségű tranzakciók, illetve az előre definiált kapacitások mértékéig tud reagálni. A DeFi további lényeges jellemzője éppen ez, a mindkét fenti megoldásra jellemző irányítási modell. A DAPP, illetve DAO esetében is az irányítás akár az okosszerződések, akár a DAO mint önálló jogalany[9] esetében az egyes irányítási jogokkal rendelkező kriptoeszköz tulajdonosok kezében összpontosul.[10]

A kripto ökoszisztémában az egyre inkább jellemző *proof of stake* működés (a logikai művelet alapú energiaigényes *proof of stake* működés helyett ebben az esetben a kriptoeszköz tulajdoni aránya alapján történik a tranzakciók jóváhagyása) keretében nem az egyes

[5] Az Európai Parlament és a Tanács 596/2014/EU Rendelete (2014. április 16.) a piaci visszaélésekről (piaci visszaélésekről szóló rendelet 15-16. cikk

[6] Szívós Alexander, 2020: A pénzügyi kultúra https://arsboni.hu/a-penzugyi-kultura/, (2020.10.01.) és Szívós, Alexander Az adórendszer és a pénzügyi kultúra összefüggései In: Szilovics, Csaba; Bujtár, Zsolt; Ferencz, Barnabás; Breszkovics, Botond; Szívós, Alexander Roland Gazdaság és Pénzügyek A 21. Században II. - Konferenciakötet = Business And Economy In The 21st Century II. – Conference Proceedings Pécs, Magyarország : Pécsi Tudományegyetem, Állam- és Jogtudományi Kar 207 p., pp. 54-56. és Szilovics Csaba, 2003: A magyar államháztartás pénzügyi rendszere In: Adójog alapjai. Illetékjog. A magyar államháztartás pénzügyi rendszere Pécs, Magyarország: PTE Állam- és Jogtudományi Kar, pp. 59-62.

[7] Glavanits Judit - Király Péter Bálint, 2018: A blockchain-technológia alkalmazásának jogi előkérdései: a fogalmi keretek pontosításának szükségessége Jog Állam Politika: Jog- és Politikatudományi Folyóirat, 3 pp. 180

[8] https://ethereum.org/en/dao/ (2021.11.01.)

[9] Már 2021 év közepétől lehetőség van az Egyesült Államokban, Wyoming államban korlátolt felelősségű társaságként történő bejegyzésre is a DAO-k esetében Aramonte Sirio – Huang Wenqian - Schrimpf Andreas – DeFi risks and the decentralisation illusion, 2021: The DeFi ecosystem An overview in. BIS International banking and financial market developments Quarterly Review, december, 2021, p. 27.

[10] A két lehetséges forma a token és a share alapú. Mindkettő esetében nyitott a csatlakozás lehetősége. https://ethereum.org/en/dao/, (2021.11.01.)

okosszerződések módosításával, hanem azok cseréjével, illetve a közöttük fennálló logikai kapcsolatok módosításával érhető el az adott DeFi szolgáltatás módosítása. Ez a tény mindjárt meg is kérdőjelezi a teljes függetlenség és automatizáltság tényét. Ezt a jelenséget nevezik Aramonte és társai decentralizációs illúziónak.[11] Nyilvánvaló ugyanis, hogy nem lehet útjára indítva magára hagyni a DAO működését[12], hiszen az rosszindulatú beavatkozás, illetve túlterheltség esetében leállna és nem tudna tovább működni. Ezért a decentralizált működést fenntartással és meghatározott korlátozással kell kezelni.[13] A működés ezen formája egyben egy lehetséges releváns beavatkozási pontot is jelenthet a jogi szabályozás területén.

A DeFi főbb összetevőit tekintve még fontos az adatforrásokra (*oracle*) kitérni.[14] Az adatforrások olyan releváns külső adatbázisok, melyek input adatokat szolgáltatnak az egyes pénzügyi szolgáltatások működtetéséhez és melyek jellemzően nem érhetők el a blokkláncon, hanem az egyes szabályozott tőzsdéken. Különösen igaz ez a származtatott pénzügyi eszközök esetében, amikor a mögöttes termék árfolyamát követi a származtatott pénzügyi eszköz árfolyama. Ezekkel az adatforrásokkal, annak manipulálása esetén jelentős károkat szenvedhetnek el az érintett személyek, ahogy az a LIBOR esetében is történt.[15]

II. A decentralizált pénzügyi rendszer (Decentralized Finance) kockázatainak részletes elemzése

A decentralizált pénzügyi rendszer önmaga is tartalmaz egy jogalkotói kihívást, mely már önmagában is egy jelentős kockázat lehet: ez pedig a DeFi globális jellegéből fakadóan a szabályozási arbitrázs. A DeFi a modern fiatpénz rendszer alternatívájaként decentralizáltan, központi felügyelet által nem ellenőrzötten működik. Ez utóbbi elkülönülés gyorsan a növekedés korlátjává válhat intézményi befektetők hiányában. Az intézményi befektetők ugyanis csak a jog eszközeivel szabályozott és védett intézményi struktúrákban történő befektetéseket részesítik előnyben tömegesen. Ez mára az intézményi befektetői iparág jelentős szereplői részéről is megfogalmazásra került. Nem meglepő ezért, hogy a DeFi szolgáltatásokat

[11] Aramonte et al, i.m. pp. 27-28.
[12] Valójában nem is kerül sor automatikus működésre, hanem csak az adott műveletek vagy azok csoportja automatikus. A beavatkozás, azaz a változás azonban egy rendkívül lapos szervezetben történik, ahol csak tagok/tulajdonosok döntenek és döntésüket az okos szerződés alapján végre is hajtják legfőbb szerv és ügyvezetés nélkül, tehát az ügynök megbízó jogviszony hiányában és ez utóbbi költségei nélkül. Halász Vendel (2016): A „társaság érdeke": a vállalati vezetők tevékenységére irányadó szabályokról Európában és Amerikában, Magyar Jog 63. évf. 12. szám, pp. 698-699.
[13] Aramonte et al. i.m. p. 28.
[14] Wharton University of Pennsylvania: DeFi Beyond the Hype The Emerging World of Decentralized Finance Produced by the Wharton Blockchain and Digital Asset Project, in collaboration with the World Economic Forum May 2021 p. 3.
[15] David Hou - David Skeie, 2014: LIBOR: Origins, Economics, Crisis, Scandal, and Reform, Federal Reserve Bank of New York Staff Reports Staff Report No. 667, March, 2014

is platformján elérhetővé tevő Binance 10 pontos memoranduma[16] jelentős mértékben támogatja a tőkepiaci szabályozást és a felügyeleti szervekkel történő aktív együttműködést. A jól felismert önérdek alapja a Binance nyilatkozat esetében az, hogy a befektetők bizalma akkor építhető fel és tartható fenn, ha a befektetővédelem meghatározott szintje biztosítható és a tisztességtelen piaci magatartások kiszűrhetők és szankcionálhatók. A szabályozási arbitrázs valószínűleg a DeFi-re is hatáskörrel bíró pénz- és tőkepiaci szabályozás létrejötte esetén sem fog eltűnni, hiszen a szabályozási arbitrázs újabb és újabb lehetőséget teremt a profit növelésére, akár az egyes országok, akár az egyes piaci szereplők eltérő szabályozása miatt. A szabályozás hatályán kívüli lét a DeFi esetében még évekig fennállhat, elsősorban a DeFi komplexitása és globális jellege miatt. A legfontosabb szabályozandó terület a stabil kriptopénzek, mely megvalósulhat akár egy új, erre a pénzügyi eszközre kialakított szabályozással, de akár a DeFI a meglévő szabályokba történő integrálásával is.[17]

A tőkeáttételes pénzügyi eszközök már egy mini tőzsdekrach vagy egy a kriptoeszközökre korlátozott válság esetén is jelentős kockázatot jelentenek különösen, ha jelentős részük hitelből finanszírozott. Pontosan ez utóbbi valósult meg a kriptoeszközök esetében. A DeFi részeként működő stabil kriptopénzek és a DeFi tőzsdék esetében a tőkeáttétel a nem decentralizált tőkepiaci tevékenységek akár 50-125-szörös tőkeáttételénél alacsonyabb, de még így is jelentős kockázattal bír a maga 10-25-szörös tőkeáttételével.[18]

Mind a hitelezés, mind a tőkeáttétel esetében további kockázat a hitelpozíció automatikus lezárása, a fedezet megfelelő szint alá csökkenésekor. Ez a zárás az okosszerződés által előre rögzített szinten valósul meg, automatikusan. Ez egy fontos biztonsági megoldás normál piaci helyzetben. Piaci összeomlás esetében azonban még ez a megoldás sem képes a rendszerszintű kockázatok jelentős növekedése nélkül minden egyes egyedi beavatkozást ily módon kezelni. Az Egyesült Államok 2021. december 14-i Szenátusi bizottsági meghallgatása során Hillary J. Allen professzor[19] a 2008-as subprime válságot egy feltételezett kriptoeszközök okosszerződései által meghatározott DeFi pénzügyi rendszerében vizsgálta. Azt állapította meg, hogy ha Goldman Sachs az AIG-val[20] kötött hitelfedezeti csereügyletekre követelt fedezeteire

[16] Marc Vojno, 2021: Binance calls for global regulatory frameworks for crypto markets: Releases 10 Fundamental Rights https://www.zdnet.com/article/binance-calls-for-global-regulatory-frameworks-for-crypto-markets-releases-10-fundamental-rights/, (2021.11.19.)

[17] Breszkovics Botond, 2020: Kriptoszabályozás: Colorado, Kalifornia és New York In: Koncz, István; Szova, Ilona (szerk.) Tizenhét éve az európai szintű tudományos megújulás és a fiatal kutatók szolgálatában Budapest, Magyarország: Professzorok az Európai Magyarországért Egyesület pp. 49-55.

[18] Aramonte et al. i.m., p. 30.

[19] Hearing on "Stablecoins: How Do They Work, How Are They Used, and What Are Their Risks?" Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, Tuesday, december 14, 2021, pp 14-15.

[20] AIG – American Insurance Group a 2007-2009-es Nagy pénzügyi válságban az értékpapírosításokra fedezetet biztosító hitelfedezeti csereügyletek kötelezetti oldalán állva jelentős kitettséget halmozott fel, tette mindezt

hiába vállalt volna a kriptoeszközök esetében garanciát az Egyesült Államok kormánya, azok a hitelfedezeti csereügyletek az okosszerződések alapján óriási veszteség mellett mindenképpen lezárásra kerültek volna. A probléma lehetséges megoldása az okosszerződések esetében egy olyan klauzula beépítése lehetne, mely a pozíció zárást állami beavatkozás esetében késleltetné. Ennek megvalósítása a gyakorlatban azért lehet érdekes, hiszen feltételezi egy előre nem ismert (*black swan*)[21] esemény megvalósulását és arra az állam mentőöv dobását is. Ez az erkölcsi kockázat jelentős növekedését eredményezheti, hiszen, ha minden szerződés részévé válik ez a függő feltétel, akkor a piac részéről erős nyomás alakulhat ki a jegybank felé az utolsó menedék hitelező szerepben való fellépésre minden egyes esetben. Ez az a kockázat, amit szükséges lenne elkerülni, hiszen jól láthatóvá vált a FED put[22] hatása a subprime válság kialakulásában, amikor a nagy pénzügyi holdingok a TBTF elv[23] mentén bátran vállalták a jelentős tőkeáttételt, bízva abban, hogy a méretük miatt a FED mindenképpen megmenti őket. Tévedtek. Az utolsó menedék hitelező szerep[24] esetében éppen a morális kockázat kiküszöbölése miatt szükséges a szelektív alkalmazás. Az értékpapírosítás a 2007-2009-es subprime válságban, toxikus jellegét érdemben korlátozó jogi eszköz használatát érdemes fontolóra venni ezért ebben az esetben is. Ekkor az irányító részesedéssel bíró személyek helytállását érdemes mérlegelni. A felelősség egyértelmű telepítésének a kérdését is felveti.[25] Amennyiben a DAO vagy a DAPP korlátolt felelősségének áttörése megvalósul, akkor érdemes a felelősségvállalás technikai feltételeit is rögzíteni. Az állami szerepvállalás helyett egy befektetői helytállás megvalósítása is reális alternatíva lehet, akár a pénzügyi eszközök befagyasztása, akár a visszaváltás korlátozása révén,

tartalék képzése nélkül, annak ellenére, hogy üzleti biztosítóként a helytállási kötelezettségeire tartalékot kellett volna képeznie.

[21] A black swan (fekete hattyú) elméletet Nassim Nicholas Taleb pénzügy professzor, korábbi tőzsdei kereskedő a 2007–2009-es pénzügyi válságot követően dolgozta ki. Az elmélete szerint a fekete hattyú események nem kiszámítható gyakorisággal és váratlanul jelennek meg. Annak ellenére, hogy nem előre jelezhetőek a hatásuk katasztrofális méretű.

[22] A Fed put az Egyesült Államok jegybankjának a védőhálójára utal, mely megvédi a piaci szereplőket a pénzügyi eszközök jelentős leértékelődésétől azáltal, hogy a FED vevőként megjelenik ezeken a piaci szegmenseken. Kecskés András – Halász Vendel – Bujtár Zsolt, 2019: Tőzsdeuniverzum HVG-Orac Lap- és Könyvkiadó Kft. Budapest, pp. 59-65.

[23] A Too big to fail (TBGF) a túl nagy ahhoz, hogy megbukjon elméletre alapozva túlzott kockázatot vállalnak a pénzügyi szolgáltatók, abban bízva, hogy az adott állam mindenképpen mentőövet nyújt nekik, mert anélkül az egész pénzügyi rendszer összeomlana.

[24] Az utolsó menedék hitelező szerep (Lender of Last Resort) a jegybank azon szerepe, melyet a likviditási válságba jutott pénzügyi szereplő esetében alkalmazhat, megfelelő mérlegelés alapján.

[25] Nochta Tibor – Papp Tekla, 2019: Üzleti kockázat a szerződéses jogviszonyokban pp. 29-32. és Bold Uurna – Ferencz Barnabás – Kecskés András, 2019: Limiting „limited liability" Economics and Working Capital 4. évf. 3-4. szám, pp. 30-31 és Halász Vendel, 2021: Vállalatfelvásárlás, Budapest, Magyarország: Menedzser Praxis Kiadó, pp. 20-25.

hasonlóan a nyíltvégű nyilvános ingatlanalapok forgalmazásának a felfüggesztéséhez.[26] Ez a visszaváltás korlátozása már átvezet a stabil kriptopénzek kérdésköréhez.

A stabil kriptopénzek a kriptoeszközök árfolyamingadozásának a problémájának megoldására jöttek létre. Azáltal, hogy alacsonyabb árfolyamingadozású eszközökhöz (deviza, illetve devizakosár, nemesfém) kötik az adott kriptoeszköz értékét, biztosítják a jelentős árfolyamingadozási probléma kezelését. Ezen túl a stabil kriptopénzek az átjárót biztosítják a fiatpénzek és a kriptoeszközök között és egyfajta likviditási puffer szerepet töltenek be a kriptoökoszisztémában hasonlóan a pénzpiaci alapokhoz a pénz- és tőkepiacok esetében. A fenti két utóbbi funkció úgy valósulhat meg, hogy kripoteszközbe történő befektetés vagy az adott kriptoeszköz fedezetként történő felhasználásig a kriptoeszköz tulajdonosa átmenetileg stabil vagy (annak vélt - lásd Terra stabil kriptopénz összeomlása 2022 májusában)[27] kriptopénzben tartja az átváltott fiatpénzét. Ezzel azonnal átválthatóvá válik bármely más kriptoeszközre az adott stabil kriptopénz, sőt két kriptoeszköz befektetés közötti időtartamra is az értékálló stabil kriptopénz lehet a megfelelő megoldás. Ez utóbbi esetben nem keletkezik adófizetési kötelezettség, mert a kriptoeszköz tulajdonos nem lép ki a kripto ökoszisztémából.

A fenti előnyök hatására a centralizált (gazdasági társaságok és trustok által működtetett) stabil kriptopénzek és a DeFi rendszerében működtetett decentralizált stabil kriptopénzek jelentős növekedésnek indultak az elmúlt néhány évben. A működésbeli különbség két módon határozható meg: a gazdasági szervezeti az előbbi, és az okosszerződés által meghatározott működés az utóbbi. A stabil kriptopénzek működése három fő területre osztható.[28] A stabil kriptoeszközök irányítási modelljének elemei, az egyes stabil kriptopénz érmék kibocsátásának, visszaváltásának és a stabil kriptopénz értékének megőrzésére vonatkozó területek és azok szabályozása. A decentralizált kriptopénzek esetében az irányítási modell okosszerződések által előre meghatározott. Azért, hogy a biztonságos működés fenntartható legyen megfelelő fedezet szükséges. A fedezetek esetében a problémát azok kényszer értékesítése jelenti, hiszen ezzel egyrészt védi a stabil kriptopénz értékét annak működtetője tehát szükség van a kényszer értékesítésre. Éppen ez a védelem okozhatja viszont az bankpánikszerű helyzet kialakulását a kripto stabilpénz iránt bizalom elvesztésekor. Ez az egyre jelentősebb mértékű

[26] A 2007-2009-es subprime válságot követően a magyar ingatlanpiacon a nyílt végű nyilvános ingatlan alapok befektetési jegyeinek a visszaváltását 180 napos időszakra felfüggesztette az akkori magyar tőkepiaci felügyelet, a Pénzügyi Szervezetek Állami Felügyelete. Lásd Szűcs József: Az ingatlanalapok jogi szabályozása és gazdasági helyzete Hitelintézeti Szemle 2009 9.évf. 6. szám, pp. 528-555.

[27] Lásd https://edition.cnn.com/2022/05/17/investing/luna-terra-losses-crypto-traders (2022.05.20.)

[28] Financial Stability Board, 2020: Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements Final Report and High-Level Recommendations 13 October, 2020, pp. 10-11.

kényszerlikvidálások miatt alakulhat éppen ki, amit viszont az okosszerződések előre rögzített fedezettség mellett valósítanak meg.

A stabil kriptopénzek értékének megőrzéséhez a másik megoldás különböző algoritmusok működtetése. Ez a módszer azonban még nem élt át jelentős válságokat, hiszen a kriptoeszközök éppen a 2007-2009-es subprime válságra[29] történő reakcióként jöttek létre. Így az algoritmusok az alacsony bekövetkezési valószínűségi eseményekkel (*tail risk*)[30] nem vagy nem megfelelő módon kalkulálnak és így azok bekövetkezésekor akár pénzügyi rendszer szintű kockázatot is eredményezhetnek.

A fenti két kockázat megfelelő kezeléséhez szükséges a stabil kriptopénzek működéséhez visszatérni. A stabil kriptopénzek esetében látható leginkább az a nyilvánvaló tény, hogy a likviditási transzformáció jelentős kockázatot hordoz magában az egyedi stabil kriptopénzek esetében is.[31] Azáltal, hogy az alacsony állampapír hozamok miatt magasabb kockázatú eszközökbe így kereskedelmi kötvényekbe fekteti a stabil kriptoeszköz működtetője jelentősen növeli a stabil kriptoeszközök likviditási kockázatát. Bár a kereskedelmi kötvények piaca likvid, a kereskedelmi kötvények megújítási kockázata jelentős.[32] Az első pénzpiaci alap 2008-as bukását éppen az eszközalapú fedezett kereskedelmi kötvények, mint árnyékbanki szereplők megújításának az elmaradása okozta.[33] Éppen azért, mert pénzpiaci likviditás beszűkülése miatt az addig közkedvelt kereskedelmi kötvények iránt jelentősen lecsökkent a pénzügyi befektetők érdeklődése, mert saját likviditásuk biztosítása érdekében kizárólag állampapírokba illetve készpénzbe csoportosították át likvid eszközállományukat.[34] Tették mindezt akár úgy is, hogy ezzel jelentős hozamtöbbletről mondtak le, azért, hogy a folyamatos likviditásuk biztosítható legyen vagy a pénzpiaci alapok és a pénzintézetek esetében a folyamatos ügyfélpénzkivonásokra megfelelő fedezetet képezhessenek.

---

[29] Lentner Csaba – Zéman Zoltán, 2016: Handling Crisis – Role in the Economy, Moderni Veda, 2016 no 3. pp. 45-58. és Szilovics Csaba, 2000: A liberalizáció lépései a devizabelföldi természetes személyek devizabirtoklása terén JURA, 6. évf., 1-2 szám, pp. 115-120., és Zéman Zoltán – Kalmár Péter - Lentner Csaba, 2018: Evolution of Post-Crisis Bank Regulations and Controlling Tools: A Systematic Review from A Historical Aspect Banks And Bank Systems, 13. évf. 2. szám, pp 138-140.

[30] A tail risk elmélet az események nem normál eloszlását is feltételezi. Az elmélet ezért a normál eloszlás két szélső – a 99,7%-os és a 0,03%-os valószínűséggel megvalósuló – értékének a bekövetkezésével is számol. Amiért ez az elmélet különösen izgalmas, az az a tény, hogy Harry Markovitz modern portfólióelmélete és a Black-Scholes-féle opciós árazási modell is a 99,97%-os valószínűséggel megvalósuló eseményeken alapulnak. Még napjainkig is a Black-Scholes-féle árazási modell alapján történik az opciók árazása. A tail risk események bekövetkezésével éppen ezért fontos számolni, különösen előre programozott eszközök esetében.

[31] Aramonte et.al. i.m, pp. 29-30.

[32] Bujtár Zsolt, 2016: Az eszközalapú kereskedelmi kötvény Egyesült Államokbeli tündöklésének és bukásának okai Jura 22. évf. 2. szám, p. 215.

[33] Bujtár Zsolt, 2016: Az eszközalapú kereskedelmi kötvény Egyesült Államokbeli tündöklésének és bukásának okai Jura 22. évf. 2. szám, p. 219.

[34] Kecskés András, 2017: A kereskedelmi kötvények és a pénzpiaci alapok szabályozási összefüggései JURA 23. 1. szám, pp. 82-92, p. 87.

A DeFi szolgáltatásokat és különösen a stabil kriptopénzeket tekintve, ahogy azt az IMF 2021 szeptemberi tanulmánya[35] alapján is megállapítja, ezek a szolgáltatások jelentős irányítási és működési kockázatok mellett, kiberbiztonsági[36] és globális szabályozási és felügyeleti kockázatokat is jelentenek a pénzügyi rendszer számára. Ezek a kockázatok és a stabil kriptopénz mélyebb vizsgálata azonban már egy önálló tanulmány részét képezhetik.

III. A DeFi makroszintű kockázatai és azok kezelésének lehetséges módjai

1. A DeFi makroszintű kockázatai

A makrogazdasági kockázatok körébe a DeFi esetében egyaránt a kriptoizáció (dollarizációhoz hasonlóan),[37] a tőkemozgások korlátozása és monetáris transzmisszió hatékonyságának a csökkenése, valamint a banki közvetítőrendszer meggyengülése sorolható.[38] A kockázatok növekedésével a pénzügyi rendszer DeFi-n kívüli részeire is átterjedhet a DeFi likviditási válsága. Ez a hatás eredményeképpen nemcsak DeFi-n belül, de a jelenleg szabályozott pénzügyi rendszer szereplői esetében is likviditási válságot eredményezhet.

A kriptoizáció, egy a dollarizációhoz hasonló folyamat elnevezése, melynek során a nemzeti valuta pénzfunkciói háttérbe szorulnak és különösen annak a fizetési eszközként történő használata jelentősen csökken.[39] Ahogy az történik azokban az országokban, ahol az US dollár akár hivatalos pénznemként, akár a nemzeti valuta jelentős leértékelődése miatt először csak megtakarítási eszköz funkcióban majd, egy párhuzamos pénzként már fizetési eszközként is

[35] International Monetary Fund. Monetary and Capital Markets Department: The Crypto Ecosystem And Financial Stability Challenges p. 44., https://www.elibrary.imf.org/view/books/082/465808-9781513595603-en/ch002.xml, (2022.04.21.)

[36] Gáspár Zsolt, 2021: Crytocurrencies & Cybercrimes: The criminal aspects of crypto assets. In: Bujtár, Zsolt; Szívós, Alexander Roland; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics, Botond (szerk.) Kriptoeszközök világa a jog és gazdaság szemszögéből : Konferenciakötet - Válogatott tanulmányok. Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, pp. 99-105. és
Gáspár Zsolt, 2021: A pénzmosás Európai Uniós és hazai szabályozásának kérdései a kriptovaluták tekintetében. In: Szilovics, Csaba; Bujtár, Zsolt; Ferencz, Barnabás; Szívós, Alexander Roland; Breszkovics, Botond; Gáspár, Zsolt (szerk.) Gazdasági kihívások a XXI. században : Konferenciakötet. Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Pénzügyi Jogi és Gazdasági Jogi Tanszék, pp. 78-88.
Mezei Kitti, 2020 A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre Állam- és Jogtudomány 61: 4, pp. 65-81. és
Mezei Kitti, 2019: A kriptovaluták kihívásai a büntető anyagi és eljárási jogban PRO FUTURO - A jövő nemzedékek joga 9, 1., p 88.

[37] International Monetary Fund. Monetary and Capital Markets DepartmentGlobal Financial Stability Report, October 2021: COVID-19, Crypto, and Climate: Navigating Challenging Transitions 2021. október 21., p. 49.

[38] International Monetary Fund. Monetary and Capital Markets DepartmentGlobal Financial Stability Report, October 2021: COVID-19, Crypto, and Climate: Navigating Challenging Transitions 2021. október 21., p. 49.

[39] Gáspár Zsolt, 2022:Az el salvadori Bitcoin-törvény gazdasági és jogi aspektusai In: Bujtár, Zsolt; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics, Botond; Ázsoth, Szilvia; Szívós, Alexander Roland (szerk.) Fenntartható növekedés (ESG) jogi és gazdasági aspektusai Pécs, Magyarország : Pécsi Tudományegyetem Állam-és Jogtudományi Kar pp. 39-51.

funkcionál. Erre jó példaként szolgál Venezuela és Kuba pénzügyi rendszere napjainkban. A kriptoeszközök fizetési eszközként történő széles körű elterjedése miatt így nemcsak a nemzeti valuta szerepe csökken, de a monetáris politika hatékonysága is gyengül. A monetáris politika a monetáris transzmisszión keresztül valósul meg, amely a pénzügyi közvetítőrendszer igénybevételével, az egyes pénzügyi eszközök piacain keresztül közvetíti a monetáris politika céljait. E transzmisszió keretében a kamatpolitika és az eszközvásárlások, valamint a repo és fordított repo ügyletek jegybanki indíttatású tranzakciói így már kevéssé érhetik el a céljukat, ha az egyes jogalanyok kriptoeszközökben tartják megtakarításaikat és likvid eszközeik egyre jelentősebb részét. Erre különösen jó példa El Salvador, ahol 2021 szeptemberében a Bitcoin is hivatalos pénznemként került bevezetésre. A tőkemozgások korlátozása lehet egy megoldás, de csak rövid távon és megfelelő kiszámítható gazdaságpolitika és jelentős devizatartalék mellett. A rosszul rögzített kötött árfolyam ugyanis jelentős devizatartalék felhasználást eredményezhet, ami a nemzeti valuta leértékelését eredményezheti, ami aztán ismét a kriptoizációt erősítheti. A kriptoizáció során a pénzügyi közvetítő rendszer a nemzeti valuta háttérbe szorulásával is egyre kisebb szerepet kap, legalábbis annak szabályozott szereplői. Ez azért lehet veszélyes makrogazdasági szempontból, mert így a közvetítő rendszer gyengülésével tovább csökken a monetáris transzmisszió hatékonysága és a pénzügyi rendszer fiatvalutái iránti bizalom. Ez a két tény önmagában ismét gyengíti a monetáris politika hitelességét és ennek közvetlen hatásaként a monetáris politika hatékonyságát is.

Végül szerződéses partnerkockázatra (counterparty risk) érdemes külön figyelmet fordítani. Ez a kockázat alapvetően mikroszintű, de a széles körű partner nemteljesítés a pénzügyi szerződések, illetve értékpapírügyletek esetében már makrogazdasági kockázatot hordoz magában. A 2007-2009-es pénzügyi válság során az értékpapírosítás szintetikus formája a hitelfedezeti csereügyletek létrehozását és széles körű elterjedését eredményezte. A hitelfedezeti cserügyletek a szintetikus értékpapírosítás részeként és egyfajta garanciális elemként egyaránt jelentős pénzügyi veszteséget okoztak az adófizetőknek, amikor az Egyesült Államok kormányának kellett a legnagyobb hitelfedezeti csereügylet kötelezett AIG veszteségeit feltőkésítéssel pótolni. A veszteséget éppen a központi szerződő fél[40] alkalmazásának a hiánya eredményezte. A szerződéses partnerkockázat csökkentésére, a központi szerződő fél a hitelfedezeti csereügyletek körére történő kiterjesztésével a CFTC[41]

[40] A központi szerződő fél noválja az elszámolási rendszerébe tartozó ügyleteket. Ennek során a teljesítési kockázatokat jelentősen képes csökkenteni. Ehhez többszintű pénzügyi tartalék- és garanciarendszert működtet az egyes pénz és tőkepiaci ügyletek és szereplők kockázati profiljai alapján súlyozva a tartalékok szintjét.
[41] A Commodity Futures Trading Commission (CFTC) 1974-ben jött létre az Egyesült Államok határidős és opciós piacainak és különösen a határidős tőzsdéinek a felügyeletét látja el.

elnöke, Brooksley Born már 1998-ban javaslatot tett. Ez a javaslat éppen a hivatalban lévő FED elnök, Alan Greenspan és a pénzügyminiszter, Robert Rubin ellenkezése miatt nem vált a szabályozás részévé. Ennek következtében nem volt 2008 őszére megfelelő nyilvántartás a hitelfedezeti csereügyletek kitettségeiből eredő kötelezettségek nagyságára és megoszlására. Ez a tény az érintett piaci szereplők iránti bizalom megrendüléséhez vezetett és a likviditási válság kialakulásában jelentős szerepet játszott. Ez a központi szerződő fél hiányzik a DeFi és a kriptoeszköz elszámolások esetében is, ami nemteljesítés vagy nem megfelelő fedezettség esetleg programozási hiba esetén hasonló bizalomvesztést eredményezhet. A megoldás ebben az esetben nem biztos, hogy egy központi szerződő fél beiktatása, hanem a szerződéses partnerkockázathoz hasonló működési kockázatok csökkentése érdekében a blokklánc technológia adta biztonság teljes körű kihasználása lehet. A nemteljesítés kockázata a DeFi esetében is bizalomvesztést okozhat, amelynek kialakulását egy működőképes pénzügyi rendszernek meg kell tudni előzni.

2. A DeFI makroszintű kockázatok kezelésének lehetséges módjai és rendszere

A fenti kockázatok kezelésére mind a Nemzetközi Valutaalap (IMF)[42] mind a Nemzetközi Fizetések Bankja (BIS)[43] széles körű ajánlásokat tett közzé. Ezek a megoldások mellett szükséges a hasonló pénzügyi eszközök válságok kezelésekor alkalmazott jogi szabályozási megoldásait is tanulmányozni, hogy egy komplex gondolkodás keretében kialakulhasson egy olyan szabályozás, mely a piaci integritás fenntartása mellett biztosítja a fogyasztók és a befektetők érdekeinek a védelmét és ugyanakkor képes a technológia fejlődés ezen új színtereinek bővülését is támogatni.

A DeFi kockázatai speciálisak a tekintetben, hogy egy központi irányítástól az államhatalomtól függetlenként definiálják magukat és a blokklánc technológiára épülnek[44], melyben szintén a decentralizált kontroll a jellemző. Ezt erősíti az egyetlen jogszuverenitáshoz sem kötődő globális jelleg, mely a DeFi szolgáltatások igénybevételét bármely állam vagy

[42] International Monetary Fund. Monetary and Capital Markets Department: The Crypto Ecosystem And Financial Stability Challenges, https://www.elibrary.imf.org/view/books/082/465808-9781513595603-en/ch002.xml, (2022.04.21.)

[43] BIS International banking and financial market developments Quarterly Review December, 2021

[44] Szuchy Róbert, 2020: A Blockchain technológia alkalmazása a kötelmi jogban In. Csitei, Béla - Dr. Certicky, Mário: Az önvezető járművek és a kontraktuális felelősség. Jogértelmezési nehézségek a személyszállítási szolgáltatási és a bérleti szerződések körében Miskolc, Magyarország: Magánjogot Oktatók Egyesülete, pp. 75-83. és Szuchy Róbert, 2018: Az új technológiák hatása az energiajogra In. Homicskó, Árpád. Technológiai kihívások az egyes jogterületeken Budapest, Magyarország: Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, pp. 203-216.

államok közössége területén elérhetővé teszi.[45] Ezért a kockázatok kezelése is globális szinten lehet hatékony és az egyes államok korlátozásai vagy tiltásai a szabályozási arbitrázst erősítik azáltal, hogy olyan országok felé terelik át a kriptoeszközökkel kapcsolatos gazdasági tevékenységeket, melyek kevésbé szigorú esetleg támogató ösztönző szabályozást valósítanak meg.

A szabályozás tekintetében érdemes Dirk A. Zetzsche, Ross P. Buckley, Janos N. Barberis, és Douglas W. Arner professzorok által a Fintech cégek szabályozására vonatkozó négy lépcsős kategorizálását alkalmazni.[46] Azért lehet ez releváns eszköztár, mert a DeFi szolgáltatásai is új technológiai megállapodáson alapulnak (osztott főkönyvi technológia) és pénzügyi szolgáltatásokat nyújtanak. A DeFi, és azon belül is a stabil kriptopénzek, valamint a hitelezés és a tőkeáttétel használata miatt kockázatok kezelésére azok decentralizált jellege miatt szükséges a szabályozás szélesebb körű megközelítése és szabályozás alá bevonandó tevékenységek újszerű jellege miatt az új technológiákhoz hasonló szabályozás mérlegelése is.

A fenti, Fintech tevékenységekre vonatkozó szabályozás szerint[47] ez a modell négylépcsős megközelítést alkalmaz a tesztelést a kísérleti környezetben, a *regulatory sandbox,* mint fejlett tesztelési környezetét, a korlátozott engedély kiadását és a teljes körű engedélyezést. E modellt érdemes annyiban módosítani, hogy az első kategória esetén a jogalkotó nem tesz semmit a változások hatására, a második esetben (összevonva az első két kategóriát a fenti példából) teret ad a kísérletezésnek, akár strukturált formában is (*regulatory sandbox*),[48] a harmadik lehetőség során óvatos engedékenységgel él (egyedi engedélyek), és a negyedik kategóriában pedig teljes engedély kiadására vagy akár egy teljesen új keretek közötti jogszabályi környezet kialakítására is sor kerülhet.

Az első esetben lehetséges egy szigorú elutasítás, ahogy az Kína, India esetében történt több alkalommal a kriptoeszközök forgalmazása és előbbi esetében a bányászata tekintetében is. A

[45] Breszkovics Botond, 2020: Kriptoszabályozás Wyomingban Szerk. Szilovics, Csaba; Bujtár, Zsolt; Ferencz, Barnabás; Breszkovics, Botond; Szívós, Alexander Roland Business and Economy in the 21st Century II. – Conference Proceedings Pécs, Magyarország: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar p. 107. és Breszkovics Botond, 2021: Az elsődleges nyilvános érmekibocsátás előtti jogi teendők Európában. In: Bujtár Zsolt; Szívós Alexander Roland; Gáspár Zsolt; Szilovics Csaba; Breszkovics Botond (szerk.) Kriptoeszközök világa a jog és gazdaság szemszögéből, 2021. Konferenciakötet - Válogatott tanulmányok. Pécs. Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, pp. 136-158.

[46] Dirk A. Zetzsche, Ross P. Buckley, Janos N. Barberis, and Douglas W. Arner: Regulating a Revolution, 2017: From Regulatory Sandboxes to Smart Regulation, 23 FORDHAM J. CORP. & FIN. L. 31

[47] Dirk A. Zetzsche, Ross P. Buckley, Janos N. Barberis, and Douglas W. Arner 2017: Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation, 23 FORDHAM J. CORP. & FIN. L. 31, p. 99.

[48] A regulatory sandbox olyan meghatározott időre vonatkozó a felügyelet által létrehozott kísérleti terep, ahol az ügyfelekkel élesben tesztelhetik a Fintech cégek a szolgáltatásaikat. Ezzel a szolgáltatások minősége jelentősen javulhat, a hibák azonosíthatók, a felügyelet pedig megismerkedik az új technológiával és azok létrehozóival kialakítva egy bizalmi kapcsolatot a további együttműködés alapjaként.

szigorú jogalkalmazói magatartás másik megvalósulási formája az adott vonatkozó – jelen esetben a tőkepiaci jog – jogszabályi kereteinek szigorú betartása. Az Egyesült Államok esetében a Ripple VS SEC per során az Egyesült Államok tőkepiaci felügyelete a SEC a Ripple, mint kriptoeszköz kibocsátóját perelte be azért, mert véleménye szerint a Howey teszt[49] szerint a Ripple értékpapírnak minősül, és ebben az esetben kötelező a tőkepiaci felügyelet engedélye a kibocsátáshoz[50], amit a kibocsátó elmulasztott megszerezni, mert szerinte a Ripple nem értékpapír.

A második esetben a szabad kísérletezés eddig éppen a szabályozatlanság miatt megvalósult, de a strukturált kísérletezés alapformája a regulatory sandbox a kriptoeszközök globális jellege miatt nehezen lenne értelmezhető. Helyette globális együttműködés keretében a Nemzetközi Fizetések Bankja (BIS) innovációs központot (Innovation Hub) hozott létre a BIS és a különböző pénzintézetek bevonásával az új technológiai eszközökkel történő kísérletezése. Az innovációs központ úttörő kísérleteket végez digitális jegybankpénz határon átnyúló[51] és a nagykereskedelmi jegybankpénzt (wholesale CBDC) osztott főkönyvi technológiai platformon történő működtetésére[52] egyaránt. Az egyedi engedélyek a stabil kriptopénzek szabályozása esetében lehet működőképes modell, azáltál, hogy a stabil kriptopénzek csak forrásgyűjtésre jöttek létre és hitelezési funkciót még nem valósítanak meg. A speciális banki licenszre vonatkozó javaslatot az alábbiakban részletesen tárgyalja a szerző.

A teljesen új komplex szabályozói megközelítésre a példát pedig az Európai Unió előkészületben lévő szabályozása nyújtja. Az Európai Unió a Tőkepiaci Unió kiépítésének keretein belül tesz kísérletet a digitális innováció egyidejű támogatására és a fogyasztóvédelem, valamint a piaci integritás szempontjainak összehangolására a kriptoeszközök piacaira

[49] A Howey-teszt során a SEC az 1933-es Értékpapírtörvény (Securities Act of 1933) és az 1934-es Tőzsdetörvény (Securities Exchange Act of 1934) alapján dönti el, hogy az adott befektetési szerződés (investment contracts) tartalmilag értékpapírnak minősülnek-e, amennyiben igen, akkor a két törvény szerinti regisztrációs és közzétételi tevékenységnek is eleget kell tennie a kibocsátónak Lásd Bujtár Zsolt, 2018: A kriptovaluták európai és máltai szabályozásának összehasonlítása: A máltai sólyom szárnyalása Európai Jog: Az Európai Jogakadémia folyóirata 18. évf. 5.szám, pp. 6-16.

[50] Halász, Vendel, 2016: A „társaság érdeke": a vállalati vezetők tevékenységére irányadó szabályokról Európában és Amerikában, Magyar Jog 63. évf. 12. szám, pp. 698-699.

[51] A határon átnyúló fizetések (cross border payment) rendszerét a Kínai Jegybank vezetésével az Egyesült Arab Emirátusok jegybankjának, a BIS Innovációs központjának, a Hong Kong Monetáris Hatóság és Thai Jegybank bevonásával a jelenleg lassú nemzetközi utalások felgyorsítását egy multidevizás jegybankpénz tesztelésével oldaná meg, megteremtve a digitális jegybankpénz határon átnyúló formáját. https://icsin.org/blogs/2021/08/23/chinas-cbdc-cross-border-prospects-and-challenges/, (2022.04.01.)

[52] A Helvétia Projekt célja, hogy bemutassa a működési, szabályozási és jogi kereteit a jegybanki elszámolási rendszeren működtetett kísérleti, DLT alapú jegybankpénznek. A projektben a Svájci Jegybank a SIX DLT elszámolóház üzemeltető pénzügyi szolgáltató és a Goldman Sachs, az USB, a Citibank, a Hypotekharbank Lenzburg vesz részt. https://cryptonews.com/news/bis-claims-cbdc-interoperability-victory-while-us-congressman-bids-block-digital-usd.htm? (2022.02.01.)

vonatkozó rendelet tervezet törvényhozási folyamatba történő integrálásával.[53] A MICA rendelet (Markets in Crypto Assets) a teljes kriptoökoszisztéma szabályozására tesz kísérletet. A rendelet tervezet a szolgáltatások és a szolgáltatók meglévő és újonnan létrejövő elemeire kiterjedő hatállyal kívánja az egységes európai szabályozást megteremteni. A hagyományos piaci eszközök a MIFID II hatálya alatt maradnának, a kriptoeszközök jelentős részét a MICA rendelet hatálya alá integrálná a jogalkotó, mégpedig azokat, melyek nem veszélyeztetik a piac integritását, a pénzügyi stabilitást és a monetáris politikai kockázatokat sem növelik. Teszi ezt, úgy, hogy azokat a kockázatot hordozó vagy a szigorú szabályozásnak megfelelni nem képes már létező eszközök európai uniós piacon történő forgalmazását meg is tiltaná, ez különösen igaz a stabil kriptopénzek a rendeletben történő tervezett szabályozására.[54]

IV. Konklúzió

A DeFi, mint független, decentralizált pénzügyi rendszer globális kihívások elé állítja a tőkepiac szereplőit és azok felügyeleti szerveit. A szerző tanulmányában azt vizsgálta, hogy miként és milyen építőelemekből épül fel a DeFi, az egyes elemek, illetve azok összessége milyen új vagy már ismert kockázatokat hordozhatnak magukban. Megállapítható, hogy a DeFi globális és decentralizált jellege makrogazdasági kockázatokat hordoz magában és globális, valamint decentralizált jellege újszerű megközelítést igényel a jogalkotó részéről. Ehhez egy, a szerző a Fintech szabályozásnál használt módosított négyes skálájú rendszerben vizsgálta a lehetséges szabályozói magatartásokat. Az eddigi lehetséges szabályozói reakciókat áttekintve a szerző a saját kutatásai alapján azokat két lehetséges megoldási javaslattal bővítette. A repo ügyletek és a pénzpiaci alapok 2007-2009-es subprime válságban betöltött jelentős negatív szerepük és kockázataik miatti újraszabályozásuk módját is mérlegelendőnek tartja a szerző a DeFi és különösen a stabil kriptopénzek kockázatainak kezelése során. A szabályozásra jól láthatóan számos megoldási javaslat született, az idő azonban sürget, hiszen már 2022 év elején is 100 Mrd USD nagyságrendű pénzek áramlottak a meghatározó stabil kriptopénzekbe, így azok értéke hamarosan átlépheti a beavatkozás szükségességének kritikus szintjét.

[53] https://www.portfolio.hu/bank/20220118/uj-rendeletekkel-menne-neki-az-eu-a-kriptopiacnak-mutatjuk-a-mestertervet-521645, (2022.01.18.)

[54] Proposal for a Regulation Of The European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 pp. 5-6., https://data.consilium.europa.eu/doc/document/ST-11053-2020-INIT/en/pdf, (2022.04.21.)

Csesznik Zoltán*: Kripto a jövőbe csomagolva

Absztrakt:

Rengeteg információt találhatunk az alternatív devizákról, a felépítésükről, tulajdonságaikról, működésükről, kereskedésükről. A kriptopiac egy rendkívül fontos aspektusáról ugyanakkor nagyon kevés szó esik. Ez nem más, mint a kriptodevizák határidős szerződései, melyeken keresztül a pénzügyi világ elfogadta és validálta ezek közül a devizák közül a legnagyobbakat. A bitcoin és az ethereum határidős piacokra való bevezetésével azokat szürkezónából átemelte a szabályozott kereskedés medrébe, mely így már bármely entitás számára legálisan elérhető és kereskedhető.

A modern pénzügyi világ mind a mai napig egyik legfontosabb eszközei a határidős szerződések (un. *futures contracts*). Ezek a szerződések rögzítik valamely áru vagy akár értékpapír vételét vagy eladását egy előre meghatározott áron. A szerződések minden részlete standardizált, mely lehetővé teszi, hogy ezekkel a papírokkal az úgynevezett határidős piacokon kereskedni lehessen, kereskedelmük tőzsdén történik.[1] 2017 decemberében a bitcoin határidős szerződések bevezetésével bárki számára megnyílt az út, hogy úgy kereskedjen kriptodevizákkal, hogy ténylegesen nincs a tulajdonában, ugyanakkor élvezze a világ legnagyobb határidős tőzsdéje által biztosított standardizált szerződések minden előnyét és biztonságát.

Kulcsszavak: *határidős szerződések, CME, bitcoin, BRR, tőzsde, BRTI, arany*

I. Bevezetés

A cím alapján biztosak lehetünk abban, hogy a következő néhány oldalon a kriptodevizákról és a kriptopiacról olvashatunk. Ez a téma napjainkban annyira népszerű, hogy ha felnyitunk egy random pénzügyi folyóiratot biztosak lehetünk benne, hogy legalább egy cikket találunk róla. Nem véletlen, hogy jelen konferenciakiadvány is e téma köré épül. Rengeteg információt találhatunk az alternatív devizákról, a felépítésükről, tulajdonságaikról, működésükről, kereskedésükről. A kriptopiac egy rendkívül fontos aspektusáról ugyanakkor nagyon kevés szó esik. Ez nem más, mint a kriptodevizák határidős szerződései, melyeken keresztül a pénzügyi világ elfogadta és validálta ezek közül a devizák közül a legnagyobbakat.

* Csesznik Zoltán Magyar Agrár- és Élettudományi Egyetem Gazdaság- és Regionális Tudományok Doktori Iskola, Phd hallgató, csezsnik.zoltan@mate.hu

[1] John C. Hull, 2017: Fundamentals of Futures and Options Markets. Canada, Pearson Education Limited, pp. 17-18.

Bár rengetegen szállnak be a kriptokereskedésbe, sokkal kevesebben tudják, hogy ezen pénzügyi eszközök a világ legtöbb országban legfeljebb a megtűrt kategóriában vannak.[2] Az Európai Unió minden tagállamában bitcoinnal kereskedni, bányászni és azzal fizetni legálisnak számít. Ugyanis jelen állás szerint az EU mindeddig nem hozott egyetlen jogszabályt sem a bitcoin, mint deviza definiálására vonatkozóan[3]. Ugyanakkor például a magyar adótörvények egészen 2022-ig büntetéssel sújtották a kriptopiacokon képződött nyereséget, hiszen a jogalkotó nem tekintette szabályozott tőkepiacon keletkezett jövedelemnek, így az éves adóbevallásnál a személyi jövedelemadón kívül meg kellett fizetni értékhatár nélküli a szociális hozzájárulási adót is, mely további ~20% adóbefizetést jelent.

A Nemzeti Adó és Vámhivatal minden bizonnyal tisztában van ezen piacok népszerűségével, a meghirdetett amnesztia több tízezer embert érinthet hazánkban, akik az elmúlt években elmulasztották, vagy akár nem is voltak tisztában azzal, hogy e tevékenységből származó jövedelmük szintén adóköteles.

A bitcoin és az ethereum határidős piacokra való bevezetésével azokat a szürkezónából átemelte a szabályozott kereskedés medrébe, mely így már bármely entitás számára legálisan elérhető és kereskedhető. A továbbiakban megnézzük mi is a kriptodeviza, hol kereskednek vele, mi a jelenlegi jogi helyzete és hogy kerülhetett be – a határidős piacok segítségével – a világ pénzügyi vérkeringésébe.

II. A bitcoinról dióhéjban

A témában rengeteg cikk, tanulmány, könyv született már, így jelen fejezetben a teljesség igénye nélkül röviden összefoglalnám azokat az információkat, melyek a tanulmány további részének megértéséhez elengedhetetlenek.

Jelen állás szerint több, mint 2000 kriptodeviza létezik, de ezek együttes kapitalizációja alig éri el a bitcoinét, így a továbbiakban a kriptopiac és a kriptodeviza alatt a bitcoint fogom érteni.[4]

A bitcoint 2009-ben találták ki, definíciója szerint egy olyan digitális eszköz, amely egy decentralizált számítógépes hálózatot használ az értékének megteremtésére, független bármilyen központi szabályozó szervezettől vagy banktól. Egy digitális deviza, tehát fizikai valójában nem létezik. A bitcoinok hálózaton belüli tranzakciók validálása által jönnek létre, ezt a folyamatot nevezzük bányászatnak. Amikor a bányászok sikeresen validálnak egy

[2] Arslanian – Fischer, 2019: The Future of Finance: The Impact of FinTech, AI, and Crypto on Financial Services. Hong Kong, Springer, pp. 15-17.
[3] Saifedean Ammous, 2018: The Bitcoin Standard. USA, John Wiley & Sons, pp. 168-175.
[4] Wewege – Thomsett, 2019: The Digital Banking Revolution. USA, De Gruyter, pp. 39-42.

tranzakció csomagot, akkor ők ezért a munkáért bitcoint kapnak. A bányászok létrehoznak és fenntartanak kriptografikus szabályokat, melyek a rendszer stabilitását biztosítják.[5]

A tranzakciók nyilvánosak, tárolásuk és ellenőrzésük egy digitális főkönyvben történik, ezt nevezzük blokkláncnak.

Jelenleg ~17 millió bitcoin van forgalomban, melyet 2009 óta kibányásztak, a számuk véges, egyes számítások szerint 2140-re értjük a 21 milliót, ami maximum elérhető mennyiség. Ez a véges mennyiség jelenti a kriptodeviza egyik alapértékét, hiszen korlátozott a kínálata. Számos módon lehet bitcoinhoz jutni: vásárolhatunk a kriptotőzsdéken valamilyen más devizáért cserébe, kaphatunk valakitől, vagy akár bányászhatunk is magunknak. Ahhoz, hogy a bitcoint tárolni tudjuk szükségünk lesz egy úgynevezett bitcoin pénztárcára, melyet számítógépre vagy okoseszközökre lehet letölteni. Egyedi azonosítója segítségével aláírhatjuk és végrehajthatjuk a tranzakciókat.

A mai világban a bitcoin széleskörű népszerűségnek és elfogadásnak örvend. Egyre több és több helyen fizethetünk vele árukért és szolgáltatásokért, ugyanakkor a legtöbben befektetési és spekulációs céllal tartják.[6]

2016-ban a világ egyik vezető tőzsdéje a Chicago Mercantile Exchange karöltve a kripto-szolgáltatókkal létrehozott két referencia értéket, hogy segítse és professzionálisabbá tegye a kripto tranzakciókat. Ezeket kevesen ismerik pedig jelentőségük óriási, hiszen a piaci szereplőknek hiteles és pontos referencia értékeket biztosítanak.

BRTI (*CME CF Bitcoin Real Time Index*): számítása valós időben történik, a bitcoin árfolyamát fejezi ki amerikai dollárban, másodpercenként egyszer 24 órán át keresztül az év minden napján. Az index jelentősége, hogy folyamatosan transzparens és megbízható árfolyamot biztosít.

Ezzel szemben a *BRR* (*CME CF Bitcoin Reference Rate*) egy napi referenciaérték, melyet naponta egyszer publikálnak, szintén a bitcoin árfolyamát mutatja meg az amerikai dollárral szemben minden nap londoni idő szerint délután 4 órakor. A *BRR* aggregálja a legnagyobb kriptotőzsdék árfolyamait meghatározott időpontokban, meghatározott kalkulációs ablakokban. A *BBR* ezeknek az értékeknek kereskedési mennyiség szerinti súlyozott átlaga.[7]

[5] Arslanian – Fischer, 2019: The Future of Finance: The Impact of FinTech, AI, and Crypto on Financial Services. Hong Kong, Springer, pp. 15-17

[6] Saifedean Ammous, 2018: The Bitcoin Standard. USA, John Wiley & Sons, pp. 168-175, pp. 193-196.

[7] Chicago Mercantile Exchange: CME CF Bitcoin Reference Rate & CME CF Bitcoin Real-Time Index. https://www.cmegroup.com/trading/cryptocurrency-indices/cf-bitcoin-reference-rate.html, (2022.02.02.)

III. Határidős piacok és szerződések

A modern pénzügyi világ mind a mai napig egyik legfontosabb eszközei a határidős szerződések (un. *futures contracts*). Ezek a szerződések rögzítik valamely áru vagy akár értékpapír vételét vagy eladását egy előre meghatározott áron. A szerződések minden részlete standardizált, mely lehetővé teszi, hogy ezekkel a papírokkal az úgynevezett határidős piacokon kereskedni lehessen, kereskedelmük tőzsdén történik.[8]

Egyszerűen fogalmazva, amennyiben megveszünk egy határidős szerződést, akkor kötelezzük magunk arra, hogy a szerződés által körülírt árut a szerződés lejáratakor a meghatározott áron megvesszük.

Ha belegondolunk ezek a piacok logikus okok miatt alakultak ki. Vegyük például a mezőgazdasági termékeket. Nehézkesen lenne megoldható, hogy az összes termelő egyszerre vigye el a termékét egy adott helyszínre. De talán ennél is fontosabb, hogy a határidős piacok hídként funkcionálnak a termelők és a felhasználók között. Csökkentik a szezonalitásból eredő extrém ármozgásokat, folyamatos bevételt teremtenek a termelőknek, transzparenciát és biztonságot nyújtanak a piaci szereplőnek csak a legfontosabb jellemzőket említve.

A határidős piacok igénye már az ókori Mezopotámiaban is felmerült. Hammurapi törvényeiben i.e. 1750-ben találunk áruk jövőbeli adás-vételére vonatkozó szabályokat, melyekre a mai határidős szerződések őseiként tekinthetünk.[9]

A modern korban az első szervezetileg is egységes határidős tőzsde 1697-ben alakult meg Osakában (Japán). Ebben az időszakban japán aranykorát élte, a Dojima körzetben élő rizskereskedők és a pénzváltók megalapították Dojima Rizstőzsdét, mely még abban az évben állami engedélyeket is kapott.

Amerikában az 1800-as években a kereslet és kínálat összetettsége, illetve a mezőgazdasági termékek szezonális jellege miatt jött létre első árutőzsde, mely rendszert hozott a káoszba és standardizált mederbe terelte a kereskedelmet. Chicago a természeti sajátosságainak köszönhetően lett a kereskedelem központja, ugyanis különböző folyókon és csatornákon keresztül kapcsolta össze az USA nagyvárosait. A Chicago Mercantile Exchange 1919-ben alakult meg az évtizedek alatt újabb és újabb határidős szerződéseket, innovatív termékeket hozott létre. A mérföldkövet 1992 jelentette, amikor a határidős szerződések elektronikus

[8] Arslanian – Fischer, 2019: The Future of Finance: The Impact of FinTech, AI, and Crypto on Financial Services. Hong Kong, Springer, pp. 15-17

[9] John C. Hull, 2017: Fundamentals of Futures and Options Markets. Canada, Pearson Education Limited, pp. 51-53.

kereskedelme elkezdődött a Globex platformon. Jelenleg naponta több tízmillió határidős ügylet zajlik le egy rendkívül széles palettát felvonultató globális elérhetőségű tőzsdén.[10]

De miért is jók ezek a határidős szerződések? A termelők finanszírozni tudják magukat azáltal, hogy előre eladják az árujukat, míg a vevők sok hónappal előre be tudják biztosítani a vételi árakat. Egy gyárnak létfontosságú, hogy folyamatos legyen az alapanyagellátottság, előre kiszámítható árakon. Természetesen a kereskedéssel együtt a spekuláció is megjelent és mind a mai napig velünk is maradt, de úgy gondolom, hogy ez a harmadlagos piaci kereslet – vagyis azok az entitások, akik se nem termelők, se nem felhasználói ezeknek a termékeknek – extra likviditást biztosítanak a piac minden szereplőjének.

A határidős szerződések tartalma az eszköz, melyre irányul, annak mennyisége, a szállítás helye és ideje. Az eszköz természetesen lehet tényleges áru (pl. arany, búza stb.), de lehet akár egy pénzügyi eszköz is, például valamilyen deviza.[11] A szállítás helyét, az áru minőségét a szerződés minden részletre kiterjedően tisztázza. A lejárati/kézbesítési idő nagyon fontos tulajdonság, piactól függően ez néhány hónaptól évekig terjed. A tőzsde szabályozza, hogy adott szerződéssel meddig lehet kereskedni, mely általában az esedékességi dátum előtti néhány nap.

A határidős szerződés minden eleme pontosan specifikált, így az elnevezésük és a kereskedési kódjaik is. A részvényekhez hasonlóan ezeknek is van egy rövid, két-három karakteres megjelenítési kódjuk, ehhez kapcsolódik hozzá a lejárati hónap – melyet latin betűvel jelölünk, illetve az utolsó két karakter az évet jelöli. Például GCJ22 az arany 2022 áprilisi határidős szerződésének jelölése, melyet beírva egy kereskedési platformba ténylegesen elérhetjük és kereskedhetjük azt.

[10] Chicago Mercantile Exchange : Timeline of CME Achievements., https://www.cmegroup.com/company/history/timeline-of-achievements.html, (2022.02.04.)
[11] John C. Hull, 2017: Fundamentals of Futures and Options Markets. Canada, Pearson Education Limited, pp. 55-57.

1. ábra: 2022 áprilisi arany határidős szerződés árfolyam görbéje
Forrás: Tradestation Inc.

IV. Határidős bitcoin és ethereum

Az előző két fejezetben megismerkedünk a kriptodevizákkal, illetve a határidős piacokkal. Tisztában vagyunk mind a két terület lehetőségeivel, tulajdonságaival.

Kijelenthetjük, hogy 2017 decembere történelmi jelentőségű volt a kriptovaluták életében, ugyanis ebben a hónapban a két legjelentősebb határidős tőzsdén (CBOT, CME) elkezdődött a kereskedés a bitcoin alapú határidős szerződésekkel.[12]

A pénzügyi világ már régóta várta ezt a lépést, ugyanis egy elképesztően innovatív eszközről van szó, mely az utóbbi években hatalmas spekulációs keresletet generált és kiemelkedő figyelmet kapott a vezető hírcsatornákon. Ugyanakkor a piac legnagyobb szereplői – pénzügyi alapok, befektetési bankok – jogi szabályzásuk miatt nem vehettek részt a kriptodevizák kereskedelmében, mely tekintve a korai befektetések megtérülési rátáját komoly hátrány jelentett rájuk nézve. Bármilyen gondolatai is voltak ezeknek a szereplőknek a kriptodevizákat tekintve, - akár hittek benne, akár ellene fogadtak volna – nem tudták tétjeiket megtenni ezeken a piacokon.

Ez változott meg 2017 decemberében, hiszen a bitcoin határidős szerződések bevezetésével bárki számára megnyílt az út, hogy úgy kereskedjen kriptodevizákkal, hogy ténylegesen nincs

[12] Chicago Mercantile Exchange: Bitcoin Futures - Contract Specs, https://www.cmegroup.com/markets/cryptocurrencies/bitcoin/bitcoin.html, (2022.02.02.)

a tulajdonában, ugyanakkor élvezze a CME által biztosított standardizált szerződések minden előnyét és biztonságát. A bevezetést megelőző várakozás természetesen árfelhajtó hatású volt, ugyanakkor 2018 első negyedéve az árfolyam beszakadását hozta magával. Egyesek szerint az esés a határidős szerződések bevezetésével függött össze, nevezetesen, hogy a pénzügyi alapok nem látták fundamentális értéket a bitcoinban, véleményük szerint az árfolyam túlértékelt, lufiszerű volt, ezért eladásra vették a szerződéseket, mellyel további eladási hullámot és bizonytalanságot generáltak, ezzel egyidőben persze szép hozamot realizáltak az eladásra vett pozícióikon.

2. ábra: Bitcoin határidős szerződés havi árfolyam alakulása
Forrás: Tradestation Inc.

A bitcoin határidős szerződések standardizáltságukat tekintve dollár alapúak, pénzügyi elszámolásúak, mely azt jelenti, hogy a szerződés lejártakor nem bitcoin cserél gazdát, hanem a felek dollárban teljesítik egymás felé a kötelezettségeiket. A szerződés alapja a *CME CF BRR*, amely egy naponta számított referencia érték és a bitcoin értékét fejezi ki dollárban. Dióhéjban a *BRR*-t naponta egyszer számítják ki londoni idő szerint délután négy órakor aggregálják és kereskedési volumen szerint súlyozzák a legjelentősebb bitcoin tőzsdék árait.[13] Egy szerződés értéke a *BRR index* ötszöröse – vagyis öt bitcoin. Segítségével a piaci szereplők hatékonyan valósíthatnak meg spekulatív, de akár fedezeti ügyleteket is, akár úgy is, hogy létező kriptodevizájukat védik le határidős szerződéssel.

[13] Chicago Mercantile Exchange: Bitcoin Futures - Contract Specs, https://www.cmegroup.com/markets/cryptocurrencies/bitcoin/bitcoin.html, (2022.02.02.)

A bevezetés óta eltelt három év ugyanakkor véleményem szerint, nem hozta meg azt az áttörést, melyre a CME és számos piaci szereplő számított. A kereskedés volumene számottevően nem tudott nőni, a bevezetés óta havi ~100 ezer szerződés cserél gazdát, mely csekélynek mondható. A likviditás pedig eltörpül a valós idejű bitcoin piacokhoz képest.

Ugyanakkor a CME sem könnyíti meg a volumen felfutását, a gyakran változó tőkeáttételi szabályok kiszámíthatatlanná teszik a határidős ügyletek tervezhetőségét. Továbbá a jelenlegi tőkeáttételi követelmények magas volta elveszi az előnyt a határidős szerződések elől. Például az aranynál a tőkeáttételi mutató harmincszoros, vagyis a vásárláshoz elég a szerződés értékének körülbelül 3% letétbe helyezni. Ugyanez a mutató a bitcoin esetén mindössze 2,5. Vagyis nem sok pénzügyi előnyünk származik abból, ha határidős szerződéssel kereskedünk tényleges bitcoin helyett.

Nem magyarázható a volatilitással a tőkeáttételi mutató alacsony értéke, a brókerek talán a spekulációs kereskedést akarják kontroll alatt tartani. A tőkeáttétel csökkentése ismert eszköz a piaci volatilitás időszakos csökkentésére. Amikor az árfolyamok esnek, a brókerek saját kockázatmenedzsment modelljük alapán a tőkeáttétel csökkentésével kényszerítik a részvevőket az eladásra vett pozíciók zárására, mely egy vételi hullámot indíthat el.[14] Való igaz, hogy a bitcoin mozgása méltán nevezhető hektikusnak. A terület annyira újnak és innovatívnak számít, hogy a tőkeáttételt biztosító brókerek kockázattűrő képessége nem terjed ennél tovább, ami érthető, mivel a bitcoin egy kormányoktól független, kvázi önszabályzó, önszerveződő pénzügyi eszköz. Árfolyama erősen kitett külső tényezőknek – egy-egy országi szabályzási törekvései óriási árfolyammozgásokat generálhatnak. Tőkeáttétel szempontjából mindegy, hogy az árfolyam melyik irányba rugaszkodik el. Eladásra vett szerződéseket tartó brókerszámlák ugyanolyan veszélyben vannak egy hirtelen felfelé irányuló mozgás esetén, sőt ebben az esetben a kockázat végtelen, mivel az árfolyamnak nincs elméleti felső határa. A másik érdekes felvetés, hogy az árfolyam elméletileg nem eshet nulla alá, de a határidős piacokon volt már erre is példa - a világjárvány kezdetén 2020 áprilisában a világsajtó a negatív olajáraktól volt hangos, melyek persze az éppen lejáró határidős szerződésre vonatkoztak. Tovább növeli a szakadékot a határidős piacokon likviditás hiánya, mely által az legjobb eladási és vételi ár közötti különbség - vagyis a *spread* – hatalmas, értelmetlenné téve a rövid távú kereskedést.

Természeten a tőzsdék próbálnak alkalmazkodni a felhasználói igényekhez. Ezt jól mutatja, hogy az innováció nem állt meg 2017 decemberében, a CME bevezette a bitcoin határidős

[14] Chicago Mercantile Exchange: Bitcoin Futures - Contract Specs, https://www.cmegroup.com/markets/cryptocurrencies/bitcoin/bitcoin.html, (2022.02.02.)

szerződések opcióit, majd ezt követte 2021 februárjában ethereum határidős szerződései és opciói is. További termékpaletta bővítést a mikró szerződések bevezetése jelentette, melynek célközönsége egyértelműen a néhány ezer dollárt kockáztató kisbefektetők.

V. Összefoglalás

Az előzőekben részletezett nehézségek ellenére elmondható, hogy a CME és a CBOT által – illetve egyéb tőzsdék által bevezetett határidős szerződések - hosszú távon segítették a kriptodevizákat. Ezeken keresztül bekerültek a pénzügyi világ legitim vérkeringésébe, bárki számára legálisan elérhetővég váltak.

Véleményem szerint azáltal, hogy a világ legnagyobb tőzsdéi ilyen terméket hoztak létre, sokak számára jelentette a kriptodevizák pénzügyi eszközként való elfogadását, legitimitásának megteremtését, illetve olyan garanciákat, hogy a bitcoin és a kriptodevizák hosszú időn keresztül velünk fognak maradni, esetleg mindennapi életünk szerves részévé fognak válni.

A határidős szerződések segítségével már 2017 decemberétől lehetősége volt bármely magyar állampolgárnak szabályozott tőkepiaci ügyletekkel kiváltani a kriptodeviza kereskedést, mely által ~20 %-os az adóelőny vált elérhetővé. A fejlődés töretlenségét mutatja, hogy 2022-től a NAV a kriptopiacokon végzett tranzakciókat adózás szempontjából egyenértékűnek tekinti a szabályozott tőkepiaci ügyletekkel.[15]

A jövőt senki nem tudja pontosan megjósolni, valószínűnek tűnik a kriptopiac népszerűségének további növekedése, mely magával fogja hozni az új és még innovatívabb határidős szerződések bevezetését is. Elképzelhető, hogy a határidős kriptopiacok összetettségük miatt sosem fognak olyan népszerűségnek örvendeni, mint a spot piacok, ugyanakkor megkérdőjelezhetetlen, hogy a világ vezető tőzsdéinek támogatása és termékei a kriptopiacok fejlődésének alappilléreit biztosítják.

[15] Nemzeti Adó és Vámhivatal: Új szabályok alapján adóznak a kriptovaluta-ügyletek. https://nav.gov.hu/ado/szja/uj-szabalyok-alapjan-adoznak-a-kriptovaluta-ugyletek, (2022.02.03.)

Gáspár Zsolt:[*] Money Laundering and Cryptocurrencies in the Hungarian and EU regulations

Abstract

The European Union's strategy regarding money-laundering has changed significantly between 2010 and 2021. Even though the regulations' speed exceeded the expectations, there are still areas of money-laundering of which the EU decided to keep the 'minimum-regulation principle'. One of the most important areas is the so-called cryptocurrencies. These assets are used more frequently day-by-day, so it is inevitable that a detailed regulation is needed. With the lack of the existence of the national level regulation, the law enforcement has also difficulties in such cases. The aim of the study is to overview the Hungarian and EU level instruments that can be used to fight money-laundering in those cases where cryptocurrencies are involved.

Keywords: *money-laundering, cryptocurrencies, AML, cybercrime*

I. Introduction

Over the last two decades, we have witnessed an incredible process of globalization and technological development that has surpassed all imagination, which has led to significant changes in, among other things, the manifestations of organized crime[1]. Despite the fact, that Bitcoin was released more than a decade ago, the so-called 'vacuum iuris' in the field of cryptocurrencies is still unfilled. Researchers in the field often fail to agree even at the level of definitions. The under-regulation based on the division and professional antagonism unfortunately favors criminals, as it facilitates to commit certain crimes – especially cybercrime[2] – by exploiting a certain degree of anonymity provided using cryptocurrencies. As the practical experience shows, cryptocurrencies are used extensively to engage in illegal transactions[3] (e.g., arms trafficking, drug trafficking) on the so-called dark web, but these assets

[*] PhD student, University of Pécs, Faculty of Law, Department of Criminology and Penal Enforcement

[1] See further on organized crime: Kőhalmi László, 2020: Szervezett bűnözés. In: Barabás, A. Tünde (eds.): Alkalmazott kriminológia. Budapest, Ludovika Egyetemi Kiadó, p. 461-474.
Tóth Dávid – Gál István László – Kőhalmi László, 2015: Organized Crime in Hungary. In: Journal of Eastern-European Criminal Law 2015/1, pp. 22-27.

[2] See further: Torma Adrienne – Bendes Ákos, 2018: Cybercrime, a jelen és a jövő kihívásai. In: Szabó, Csaba (eds.): Tavaszi Szél 2018 (Spring Wind 2018), Budapest, Doktoranduszok Országos Szövetsége (DOSZ), pp. 256-268.

[3] A good example to mention can be the infamous Silk Road webpage, managed by Ross Ulbricht, which conducted illegal activities (e.g., drug-trafficking) on the dark web for years. The payments and the transactions were typically

are often used in return for other illegal activities or services that are extremely dangerous to the society[4] (e.g., child pornography[5], assassinations). With the development of the cryptocurrency ecosystem[6], anyone with the minimum user-level knowledge in IT can now purchase these currencies besides, their value is growing significantly, they are becoming more stable, and their presence may also become part of the financial culture[7] in the future. The risks of money laundering and terrorist financing has risen by this phenomenon, which was also recognized by the European Union's institutes.

The aim of this study is to review the EU and domestic institutions, regulations, and sources against money laundering, in the terms of cryptocurrencies and, to assess the usability of cryptocurrencies for money laundering, under the existing regulations.

II. The Fight Against Money-Laundering in the European Union

2.1. European Institutions

Europol has a key role to play in the EU dimension of the fight against money laundering, with the main task of providing intelligence and judicial support to the Member States in this regard, to prevent and combat international money laundering activities.[8] Within Europol, there are several departments that are actively involved in EU actions against money laundering:

- The 'Europol Criminal Assets Bureau' (ECAB for short) is essentially Europol's office dealing with criminal assets. It is responsible for assisting in the search for assets derived from criminal offenses outside the jurisdiction of the Member States. Within this unit is the Camden Asset Recovery Inter-Agency Network (or CARIN for short), which contributes to ECAB's work by seizing, managing, and confiscating the assets mentioned above.[9]

fulfilled with cryptocurrencies. For more information about Silk Road see further: https://www.investopedia.com/terms/s/silk-road.asp, accessed: January 18th, 2021.

[4] About one of the main characteristics of crimes see further: Kőhalmi László, 2012: A büntetőjog alapproblémái. Pécs, PTE Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet, 2012

[5] See further: Torma, Adrienne – Bendes, Ákos: A cybercrime és a gyermekpornográfia összeolvadása. In: Bendes, Ákos – Nagy, Melánia – Tóth, Dávid (eds.): Lépést tud-e tartani a jog a XXI. század kihívásaival? Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, Doktori Iskola, 2019. pp. 5-29.

[6] See further on the cryptocurrency ecosystem: Kecskés András - Bujtár Zsolt, 2018: A kriptovaluta ökoszisztéma európai uniós és a svájci szabályozásának összehasonlítása. JURA 24. évf 2. szám pp. 424-439.

[7] See further on the topic: Szívós Alexander, 2020: Az adórendszer és a pénzügyi kultúra összefüggései. In: Szilovics, Csaba – Bujtár, Zsolt – Ferencz, Barnabás – Breszkovics, Botond – Szívós, Alexander Roland (eds.): Gazdaság és pénzügyek a 21. Században II. - Konferenciakötet = Business and Economy in the 21st Century II. – Conference Proceedings. Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, pp. 52-64.

[8] https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime/money-laundering, accessed: January 19th, 2021.

[9] Ibid.

- The ’Anti-Money Laundering Operational Informal Network’ (AMON for short) is an informal network of international investigators set up in 2012 to improve and optimize the existing legal framework for international cooperation in the field of money laundering.[10]
- In addition to the above, Europol also operates the ’Financial Crime Information Center’ (or shortly FCIC), a web-based interface for money laundering, asset recovery and criminal intelligence investigators, which facilitates the secure flow of information, meanwhile it also functions as a communication channel between the mentioned investigators.[11]
- The European Financial and Economic Crime Center (EFECC) was set up in June 2020 (also as an initiative of the Europol). This institution is set up in the spirit of combating financial and economic crime, including money laundering, as both an informative and operational network, as a support body. Since its inception, EFECC has hosted the secretariats of CARIN and AMON, among others, and collaborates with FIU.net and other advisory bodies, meanwhile it works closely with OLAF.[12]

In addition to Europol's money laundering units, it is also worth mentioning that the EU Policy Cycle between 2018-2021 also addresses issues such as cybercrime[13], organized crime and combating money laundering[14]. The policy cycle is a four-phase process, the first step of which is to assess the threats posed by organized crime. The Serious and Organized Crime Threat Assessment (SOCTA for short) makes recommendations to identify priorities for a given policy cycle. A multi-annual strategic plan is prepared based on SOCTA, followed by an actual operational plan. The cycle ends with an evaluation phase, during which the experts analyze the EMPACT cycle (also based on SOCTA). During this process, the results and errors of the cycle are also reviewed, based on which changes to the cycle can be made later.[15]

2.2. Directives

Although the risk of using virtual currencies for money laundering has been identified in the Directive 2018/1673/EU, the Directive (emphasizing the reasons of the minimum regulation)

[10] Ibid.
[11] Ibid.
[12] Ibid.
[13] Cybercrime cases play a significant role in the crime cases during the past decades. Due to this fact, it should be considered reasonably to broaden our knowledge about the topic. See further on computer-related crimes: Nagy Zoltán András, 2009: Bűncselekmények számítógépes környezetben. Budapest, Ad Librum
[14] See further about the connection between organized crime and money laundering: Szendrei Ferenc, 2018: A szervezett bűnözés gazdasági háttere és a pénzmosás. In: Magyar Rendészet 2018/5. pp. 77-91.
[15] https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact, accessed: January 19th, 2021.

leaves it to the Member States to address the risks associated with virtual payment in this regard and does not regulate the area. Further guidance on virtual currencies is provided by the Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. Regarding the virtual currencies, the Directive calls for the scope of Directive 2015/849/EU[16] to be extended to providers of exchange services between virtual currencies and regulatory money and, to custodian wallet providers.[17]

The problem with the above-mentioned EU directives, from the point of view of the regulation of cryptocurrencies, is that the European Union does not take a full position on the direction of regulation but remains in favor of minimum regulation. This may be a solution in several legal areas, but it may be problematic in the present case, especially for cross-border organized crime, in which cryptocurrencies play a significant role, besides it causes different legal classifications from country to country (e.g., legal definition of cryptocurrencies, their integration to the tax systems). The directives also divided the Member States, several countries were failing to implement them in a timely manner (including Hungary), and some Member States have introduced stricter regulations than necessary. The case of Germany can be a good example for that, where the implementing act[18] of the Directive entered into force on January 1st, 2020. According to this, the activity of the service providers dealing with cryptocurrencies was defined as a new financial service.[19] Due to that classification, such service providers must initiate an authorization procedure with BaFin (German Federal Financial Supervisory Authority).[20] Another important change is that virtual currencies have been categorized as financial assets if certain conditions are met. These conjunctive conditions are as follows:

- are not issued by a community or central institution[21],

[16] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

[17] 2018/843/EU (8)

[18] Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie

[19] It was the modification of the German Bank Act (Kreditwesengesetz, or shortly KWG).

[20] https://www.bafin.de/EN/Aufsicht/BankenFinanzdienstleister/Zulassung/Kryptoverwahrgeschaeft/kryptoverwahrgeschaeft_node_en.html, accessed: February 15th, 2021.

[21] According to this, CBDC is not under this category. See further: Bujtár Zsolt, 2020: Central bank-issued digital currencies: - ready, steady, go? In: Szilovics, Csaba – Bujtár, Zsolt – Ferencz, Barnabás – Breszkovics, Botond – Szívós, Alexander Roland (eds.): Gazdaság és pénzügyek a 21. században II. - Konferenciakötet = Business and Economy In The 21st Century II. – Conference Proceedings. Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, pp. 113-123., also

- do not legally fall into the category of means of payment, regulatory money,
- may be used by private or legal persons for payment or exchange of goods,
- serve investment purposes, and
- are stored, traded, and transmitted electronically.[22]

III. The Regulation of Money-Laundering in the Hungarian Law System[23]

In an economic sense, money laundering is an illegal economic service carried out under the guise of legal transactions, because of which the origin of the criminal assets can be proved to be verifiable, and any part of it is exhausted from the point of view of the criminal law.[24] Our Criminal Code[25] devotes an entire chapter (under number XL) to the money laundering. Under paragraph 399., the legislator describes the acts, which are considered money laundering:

- concealing the origin of an asset obtained from any punishable criminal offense, concealing the right to the asset, the location of the asset or any change in it,
- the taking over, concealing, transforming, transferring, using, engaging in the disposal of such asset, engaging in financial activities, or providing financial services for the purpose of concealing or disguising the origin of such asset, the right to the asset, the location of the asset or the change of the previously mentioned information,
- contributing to the confiscation or asset recovery against another person with the acts listed in point (b), or seeking to frustrate confiscation or asset recovery against another person,
- the acquisition, preservation, concealment, management, use, utilization, transformation, transfer, disposal, or acquisition of an asset derived from a criminal offense committed by others.[26]

In addition to the above-mentioned methods, the Criminal Code also penalizes the negligent figure, which punishes the offense with up to two years of imprisonment.[27]

Bujtár Zsolt, 2019: Central bank issued digital currencies, is it a solution or a problem? In: Glavanits Judit - Horváthy Balázs - Knapp László (szerk.): EU Business Law and Digital Revolution: Selected Studies from New Fields of Technology. Győr, Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar. pp. 71-89.

[22] https://kriptoakademia.com/2020/03/04/nemetorszag-a-bitcoin-torvenyes-penzugyi-eszkoz, accessed: February 15th, 2021.

[23] See further on the topic: Gál István László, 2019: 25 Years of Fight Against Money Laundering in Hungary. In: Journal of Eastern-European Criminal Law 2019/2. pp. 62-71.

[24] Gál István László, 2012: A pénzmosással és a terrorizmus finanszírozásával kapcsolatos jogszabályok magyarázata. HVG-ORAC Lap- és Könyvkiadó, Budapest,. p. 19.

[25] Act C of 2012 on the Criminal Code

[26] 399.§

[27] 400.§

Regarding the qualifying circumstances, the legislator partly relies on the establishment of thresholds. According to this, the basic form of money laundering is committed if the crime does not exceed a significant value. In addition, it assesses as a qualifying circumstance, if the money laundering is committed in a commercial scale; if it envolves a particularly considerable or greater amount of money; if it is committed by a public official; or if it is committed by a service provider, an official or an employee specified in the Act[28] on the Prevention and Suppression of Money Laundering and Terrorist Financing[29] if the crime in connection with the activities of the service provider.[30]

Compared to the old Criminal Code[31], the criminal law definition of money laundering has changed significantly. The object of the offense in the old regulation was 'the thing' derived from a punishable act, which was replaced by the 'asset' or 'property' obtained from a punishable act. The relevant definition of 'property' (which was implemented by the new legislation) can be found in Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law.[32] According to this, 'property' means assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or an interest in, such assets.[33]

IV. Cryptocurrencies and Money Laundering

As mentioned above, the possibility of using cryptocurrencies for money laundering arose years ago. Numerous studies over the past decade have addressed the abuse of virtual payment devices based on blockchain technology by criminals – especially organized crime groups – as many of their features can be beneficial to them. In most cases, it is not necessary to provide personal data for their use, nor do service providers require identification by identity documents during new registrations, nor do they conduct customer due diligence procedures. Considering

[28] The act also involves – among others – the attorneys-at-law. See further on the role of attorneys in money laundering:
Kőhalmi László, 2005: Ügyvédek és pénzmosás. In: Gál István László (szerk.) A pénzmosás elleni küzdelem aktuális kérdései. Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, p. 89-97.
Józan, Flóra – Kőhalmi, László: Lawyers and Money laundering. In: Journal of Eastern-European Criminal Law 2016/2. pp. 130-136.
[29] Act LIII of 2017 on the Prevention and Suppression of Money Laundering and Terrorist Financing
[30] 399.§
[31] Act IV of 1978 on the Criminal Code
[32] See further on the 4th AML Directive: Gál István László, 2018: The 4th EU Directive and the Hungarian AML Practice in 2018. In: Pavlović, Zoran (ed.): Yearbook. Human Rights Protection: "From Unlawfulness to Legality", Novi Sad, Institute of Criminological and Sociological Research, pp. 349-360.
[33] Directive (EU) 2018/1673, Article 2, paragraph (2)

this, while maintaining a high degree of anonymity, anyone with an email address can purchase cryptocurrencies. Anonymity is thus a favorable characteristic of cryptographic devices for money laundering. A great example can be the Costa Rican cryptocurrency service provider named 'Liberty Reserve', which was used to launder billions of US dollars.[34] The system operated in huge numbers, with more than 200,000 users in the United States alone. In May 2013, the U.S. Department of Justice indicted Liberty Reserve[35], and a first-instance decision on the case was made in December 2014.[36]

The role of the exchange providers (between cryptocurrency and regulatory currency) in money laundering can also be a problem. The case of RG Coins, run by Rossen G. Iossifov, can serve as an excellent example of the money laundering activities of such service providers. The cryptocurrency and fiat money exchange service was operated by the Bulgarian citizen under the name 'RG Coins'. His main customers were the members of the Alexandria Online Auction Fraud Network (AOAF Network), which was operating in Romania, which was engaged in fraudulent activities on auction sites (such as Craigslist or Ebay) targeting U.S. citizens. The frauds were carried out by publishing false advertisements, then the group was exchanging money confiscated from US citizens for cryptocurrencies and, after that phase they were sending it to exchange service providers such as Iossifov, who, with the lack of the identification or KYC processes (requesting ID documents, requesting information about the origin of the money), offered a discounted exchange rate to members of the AOAF Network. The process lasted nearly for 3 years, while Iossifov laundered nearly $ 5 million using cryptocurrencies, and the U.S. District Court sentenced the 53-year-old Bulgarian offender to 10 years in prison.[37]

The high liquidity of cryptocurrencies is also an advantageous feature in money laundering activities. With the help of the so-called 'mixers' (programs that allow you to exchange cryptocurrencies), cryptocurrencies can be easily mixed and exchanged with each other, and they can be converted to most of the regulatory currencies, too. Currency exchanges of this volume and speed can also raise problems for the investigating authorities, because in most cases, the authorities can follow the entry and the exit points of the cryptocurrency ecosystem,

[34] Alan Brill – Lonnie Keene, 2014: Cryptocurrencies: The Next Generation of Terrorist Financing? In: Defence Against Terrorism Review, 2014/1. p. 18-20.

[35] Valeriia Dyntu – Oleh Dykyi, 2018: Cryptocurrency in the System of Money Laundering. In: Baltic Journal of Economic Studies 2018/5. pp. 79.

[36] See further on the Liberty Reserve-case: https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/usa/2014/us_v_liberty_reserve_et_al..html, accessed: January 28th, 2021.

[37] https://www.justice.gov/opa/pr/owner-bitcoin-exchange-sentenced-prison-money-laundering, accessed: January 29th, 2021.

but shrinking deep into the system would require experts, high knowledge, and material sources. The biggest problem with cryptocurrencies – from the perspective of criminals – is the lack of stability. However, this feature raises several issues. On one hand, a certain number of criminals are skeptical about cryptocurrencies, as the possibility of even a small inflation for significant amounts can cause huge damage, and fluctuations in cryptocurrency exchange rates can sometimes be drastic. This, of course, does not deter all the criminals, but a certain proportion of them are scared by the possibility of losing their money in the possible collapse of a given cryptocurrency. On the other hand, a significant change in the exchange rates can also raise questions in the terms of the seizure and the confiscation. In this regard, if the detection of a given criminal act happened, distinguishing can be questionable between the assets obtained from a criminal offense and the surplus derived from the change of the exchange rates. An example can be the price of Bitcoin, which quadrupled its value between January 2020 and February 2021 (see Figure 1). If we suppose that an offender bought $ 10,000 worth of Bitcoin in January 2020 with the money obtained from a criminal offense, due to the drastic rise in the exchange rate, by February 2021, he already had $ 40,000 worth of Bitcoin.

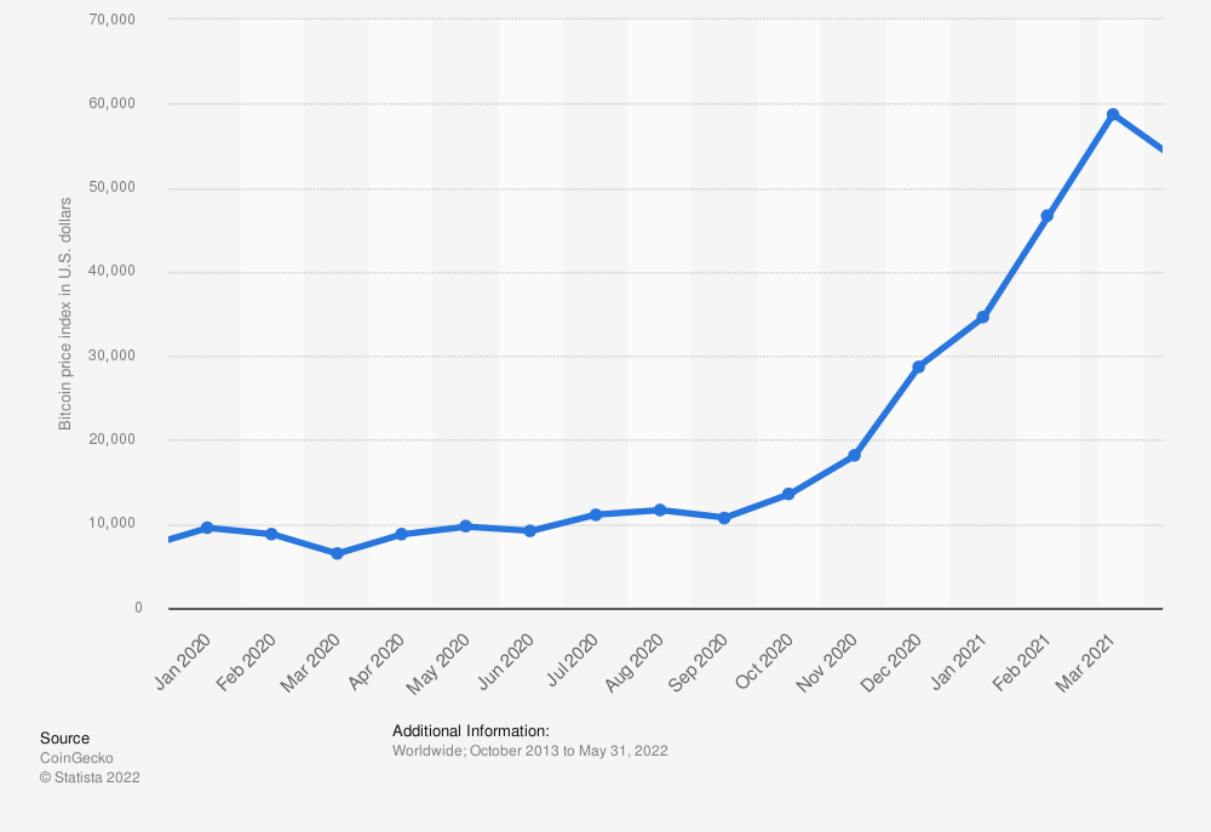


Figure 1.: The change of the exchange rates of Bitcoin between January 2020. and March 2021. Source: https://www.statista.com/statistics/326707/bitcoin-price-index/, accessed: May 13th, 2022.

If the Bitcoin account of the above-mentioned offender is seized or confiscated, several questions will arise. Firstly, can coercive measures, such as confiscation of property, be extended to the benefits of the assets derived from a criminal offense? On one hand, a logical solution to the issue could be to sell the seized Bitcoin, whether by auction or otherwise, so that the victims and the costs of the proceedings could be satisfied from the sold assets, but the problem of the remaining amount is questionable. On the other hand, if the cryptocurrency, in this case Bitcoin, experiences a decrease in the exchange rates, only a fraction of the amount invested can be regathered. In this case, the amount must be supplemented by the offender, so it would be reasonable, if the remaining amount in the first case would be repaid, as the business move - in this case the investment in Bitcoin - was the perpetrator's idea, so the profit was ultimately not a result of the crime. On the other hand, this could act as a motivation for the offenders, because even the repaid money after the criminal process would be a significant benefit and, from that phase, the repaid amount would have a legal origin, which it did not have previously.

V. Summary

In conclusion, the use of cryptocurrencies for money laundering activities is not yet safe, as unpredictable exchange rate fluctuations should also be considered a risk factor for criminals, although it should be noted that this does not deter all criminals from using them for this purpose. However, this fact does not mean that cryptographic money laundering will not become a common practice in the future, as - based on Bitcoin or Ethereum - it can be stated that the systems have an increasing number of users, which greatly affects the stability of these cryptographic devices, also if this adds to the low levels of regulation, it could cause serious problems. The legal regulation of cryptocurrencies, as they are increasingly the subject and/or the instrument of crime, has now become an urgent issue. Keeping pace with changes in crime trends, a reaction from the legislators can be expected, as it would be an unrealistic expectation for the law enforcement to operate in the absence of regulation in both criminal and civil law matters.

As a proposal, I would urge the establishment of a supervisory body specializing in cryptographic assets at the national level, which would perform its tasks as a body consisting of IT specialists and legal experts in accordance with the financial supervisory bodies of the EU and Hungary. As more and more people engage in the activity of exchanging cryptocurrencies and regulatory currencies, and as the exchange rates are not regulated, the exchange rate gap between two - independent - service providers may be high. Therefore, the oversight of cryptocurrency exchange rates could be entrusted to the body proposed above, which, as an official informative forum, would publish daily exchange rates, thereby helping individuals and legal entities while restricting the activities of exchange service providers by implementing a minimum and a maximum limit. This would also have the advantage that if coercive measures were required in a criminal proceeding, in which the assets obtained from the offense are in cryptocurrency accounts, there would be an official forum that could be used as a basis for the sale of the seized cryptocurrency.

Gáti Balázs*: A mesterséges intelligencia európai uniós szabályozásának egyes adatvédelmi kérdései

Absztrakt:

A mesterséges intelligencia alkalmazása különféle formákban az emberi tevékenységek egyre több területén játszik jelentős szerepet.

A széles körben történő alkalmazás miatt számos jogi norma szabályozza a mesterséges intelligencia felhasználásának feltételeit, figyelemmel a jelentősebb adatvédelmi szempontokra.

A 2016 májusában elfogadott adatvédelmi csomag - (EU) 2016/679 rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról; „GDPR" és az (EU) 2016/680 irányelv a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról; „Bűnügyi Adatvédelmi Irányelv" - célja, hogy felkészítse az uniós országokat a digitális korszakra, egyúttal az automatizált adatkezelés feltételeinek megszabásával általános szabályokat biztosít a mesterséges intelligencia használata tekintetében.

Az Európai Bizottság 2021. április 21-én nyújtotta be a mesterséges intelligencia harmonizált szabályainak megállapításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatát, amely szintén jelentős adatvédelmi vonatkozásokkal bír.

Tanulmányomban a mesterséges intelligenciára vonatkozó adatvédelmi szabályozás főbb jellemzőit kívánom bemutatni, figyelemmel az uniós szabályozással kapcsolatos aktuális kérdésekre.

Kulcsszavak: *mesterséges intelligencia, adatvédelem, EU*

* Dr. Gáti Balázs: PhD hallgató, Kriminológia és Büntetés-végrehajtási Jogi Tanszék, Pécsi Tudományegyetem Állam- és Jogtudományi Kar

I. Bevezetés

A mesterséges intelligencia (MI) gyorsan fejlődő technológia család, amely gazdasági- és társadalmi előnyök széles skálájához járulhat hozzá, emellett jelentős kockázatokat is hordoz.[1] Az uniós jogi szabályzás kezdetei 2017- re tehetők, utalva az Európai Parlament részéről a Bizottságnak címzett, a robotikára vonatkozó polgári jogi szabályokról szóló ajánlásokat tartalmazó, 2017. február 16-i állásfoglalására.[2]

2019-ig több mesterséges intelligenciához kapcsolható jogi szabályozás látott napvilágot, úgy mint

- az európai ipar digitalizálásáról szóló, 2017. június 1-jei állásfoglalás[3],
- az autonóm fegyverrendszerekről szóló, 2018. szeptember 12-i állásfoglalás[4],
- a digitális korban a nyelvek közötti egyenlőségről szóló, 2018. szeptember 11-i állásfoglalás[5],
- a Digitális Európa programnak a 2021–2027 közötti időszakra történő létrehozásáról szóló, 2018. június 6-i bizottsági javaslat[6],
- az európai nagy teljesítményű számítástechnika közös vállalkozás létrehozásáról szóló, 2018. szeptember 28-i (EU) 2018/1488 tanácsi rendelet [7].

A gazdasági- társadalmi előnyöket, és a kockázatokat is megfogalmazza az Európai Parlament 2019. február 12-i állásfoglalása a mesterséges intelligenciára és a robotikára vonatkozó átfogó európai iparpolitikáról[8].

Ennek alapján:

- „(…) *a mesterséges intelligencia és a robotika lehetőséget kínál életünk gazdagítására és képességeink bővítésére, mind egyénként, mind pedig a közjó érdekében;*

---

[1] Nagy Zoltán András, 2020: A mesterséges intelligencia és a jogi felelősség kérdése - 2010-2020-as évek fordulóján de lege ferenda.In: Madai, Sándor; Pallagi, Anikó; Polt, Péter (szerk.) Sic ictur ad astra. Ünnepi kötet a 70 éves Blaskó Béla tiszteletére. Budapest, Magyarország: Ludovika Egyetemi Kiadó, pp. 375-382. , p. 8.

[2] A robotikára vonatkozó polgári jogi szabályok Az Európai Parlament 2017. február 16-i állásfoglalása a Bizottságnak szóló ajánlásokkal a robotikára vonatkozó polgári jogi szabályokról (2015/2103(INL)),Hivatalos Lap C 252., 239. o.

[3] Az európai ipar digitalizálása Az Európai Parlament 2017. június 1-jei állásfoglalása az európai ipar digitalizációjáról (2016/2271(INI)), Hivatalos Lap C 307.163. o.

[4] Az Európai Parlament 2018. szeptember 12-i állásfoglalása az autonóm fegyverrendszerekről (2018/2752(RSP)), Elfogadott szövegek, P8_TA(2018)0341.

[5] Az Európai Parlament 2018. szeptember 11-i állásfoglalása a nyelvi egyenlőségről a digitális korban (2018/2028(INI) **),** Elfogadott szövegek, P8_TA(2018)0332.

[6] Javaslat Az Európai Parlament és A Tanács Rendelete a Digitális Európa programnak a 2021–2027 közötti időszakra történő létrehozásáról COM/2018/434 final

[7] A Tanács (Eu) 2018/1488 Rendelete (2018. szeptember 28.) az európai nagy teljesítményű számítástechnika közös vállalkozás létrehozásáról, Hivatalos Lap 252. 1. o.

[8]Az Európai Parlament 2019. február 12-i állásfoglalása a mesterséges intelligenciára és a robotikára vonatkozó átfogó európai iparpolitikáról (2018/2088(INI)),Elfogadott Szövegek, P8 TA(2019)0081

- *(…) a mesterséges intelligencia gyors ütemben fejlődik, és évek óta szerepet játszik mindennapi életünkben;*
- *(…) a mesterséges intelligencia és a robotika fellendíti az innovációt, ami új üzleti modelleket eredményez, és alapvető szerepet játszik társadalmaink átalakításában és gazdaságaink digitalizálásában számos ágazatban, például az iparban, az egészségügyben, az építőiparban és a közlekedésben*;"

A kockázatokat illetően ugyanakkor az alábbiakra hívja fel a figyelmet:

- „ (…) *a mesterséges intelligencia rosszindulatú vagy gondatlan alkalmazása veszélyeztetheti a digitális, a fizikai és a közbiztonságot, mivel az információs társadalom szolgáltatásaival és az azokhoz kapcsolódó gépekkel szembeni nagyszabású, pontosan célzott és rendkívül hatékony támadások, valamint dezinformációs kampányok végrehajtására használható fel, és általában korlátozza az egyének önrendelkezési jogát;*

Továbbá hangsúlyozza, hogy *„a mesterséges intelligencia rosszindulatú vagy gondatlan alkalmazása a demokráciára és az alapvető jogokra nézve is kockázatot jelenthet;"*

A mesterséges intelligencia fogalmának meghatározása az állásfoglalásokban, rendeletekben érhető tetten. Auer[9] szerint „*találhatóak jogirodalmi álláspontok és fogalomalkotási kísérletek, de arra nem találunk egységes és jó választ, hogy miként kell a mesterséges intelligenciát, mesterséges intelligenciához kapcsolódó jelenségeket (robot) jogi értelemben kezelni*" Ezt fogalmazza meg Gaszt[10] is.

2020-ban jelent meg a Fehér Könyv[11], amely a mesterséges intelligenciát technológiák és automatizmusok együtteseként definiálja. Ösztönzi az MI-technológiák elterjedését, egyúttal felhívja a figyelmet, hogy e technológiák tekintetében az európai etikai normáknak, jogi követelményeknek és társadalmi értékeknek történő megfelelés szükségességére.

Egységes fogalmi meghatározás jogi szempontból nincs[12] tekintettel arra, hogy az MI-rendszerek nem csupán a szoftverösszetevők összességei, mivel azok az őket körülvevő társadalmi-technológiai rendszert is magukban foglalják.

---

[9] Auer Ádám ,2021: Gondolatok a mesterséges intelligencia egyes polgári jogi kérdéseiről. Scientia et Securitas, 2021, 2. évf. 1. szám, pp. 106–113.

[10] Gaszt Csaba, 2019: A mesterséges intelligencia szabályozási kérdései, különös tekintettel a robotikára. Infokommunikáció és Jog, Vol. 17. No. 1. pp. 21–26.

[11] Az Európai Gazdasági és Szociális Bizottság (2020/C 364/12) Véleménye, Fehér könyv a mesterséges intelligenciáról - A kiválóság és a bizalom európai megközelítése (COM(2020)65)final. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_hu.pdf, (2021. febr.2)

[12]COM (2020) 65 final,„*2.8. Azt is meg kell jegyezni, hogy a jogi (az irányítás és szabályozás célját szolgáló) fogalommeghatározások különböznek a pusztán tudományos definícióktól, mivel számos különböző követelménynek kell megfelelniük, ideértve az inkluzivitást, a pontosságot, az állandó és átfogó jelleget, valamint*

Az Európai Bizottság 2021. április 21-én nyújtotta be a mesterséges intelligencia harmonizált szabályainak megállapításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatát[13], - a továbbiakban Javaslat - amely jelentős adatvédelmi vonatkozásokkal is bír.

A Javaslat a mesterséges intelligencia technológiákra egységes „mesterségesintelligencia-rendszer" (továbbiakban „MI-rendszer") megnevezéssel utal.

A MI-rendszer fogalmát a Javaslat az alábbiak szerint határozza meg:

„olyan szoftver, amelyet az I. mellékletben felsorolt technikák és megközelítések közül egy vagy több alkalmazásával fejlesztettek, és amely az ember által meghatározott célkitűzések adott csoportja tekintetében olyan kimeneteket, például tartalmat, előrejelzéseket, ajánlásokat vagy döntéseket képes generálni, amelyek befolyásolják azt a környezetet, amellyel kölcsönhatásba lépnek."

Ezek a technikák és megközelítések a következők:

- Gépi tanulási megközelítések, ideértve a felügyelt, a felügyelet nélküli és a megerősítő tanulást, a módszerek széles skálájának, többek között a mélytanulásnak az alkalmazásával
- Logikai és tudásalapú megközelítések, beleértve a tudás megjelenítését, az induktív – logikai - programozást, a tudásbázisokat, a következtetőmotorokat, az érvelést és a szakértői rendszereket
- Statisztikai megközelítések, Bayes-féle becslés, keresési és optimalizálási módszerek

A Bizottság ugyanakkor felhatalmazást kap arra, hogy a Javaslat 73. cikkének megfelelően felhatalmazáson alapuló jogi aktusokat fogadjon el abból a célból, hogy módosítsa az I. mellékletben felsorolt technikák és megközelítések listáját annak érdekében, hogy a listát aktualizálja a piaci és technológiai fejlemények fényében, az ott felsorolt technikákhoz és megközelítésekhez hasonló jellemzők alapján. A 2016 májusában elfogadott adatvédelmi csomag - (EU) 2016/679 rendelet[14] a természetes személyeknek a személyes adatok kezelése

a gyakorlatban való alkalmazhatóságot. Ezek közül néhány jogilag kötelező érvényű követelmény, némelyek pedig helyes szabályozási gyakorlatnak számítanak".

[13]Javaslat Az Európai Parlament és a Tanács Rendelete , A Mesterséges Intelligenciára Vonatkozó Harmonizált Szabályok (A Mesterséges Intelligenciáról Szóló Jogszabály) Megállapításáról és Egyes Uniós Jogalkotási Aktusok Módosításáról, Brüsszel, 2021.4.21.COM (2021) 206 Final

[14]Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről, Hivatalos Lap, L 119, 2016.5. 4. l,

tekintetében történő védelméről és az ilyen adatok szabad áramlásáról (továbbiakban: GDPR) és az (EU) 2016/680 irányelv[15] a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról - Bűnügyi Adatvédelmi Irányelv (továbbiakban LED) - és a EUDPR[16] célja, hogy felkészítse az uniós országokat a digitális korszakra, egyúttal az automatizált adatkezelés feltételeinek megszabásával általános szabályokat biztosít a mesterséges intelligencia használata tekintetében.

Tanulmányomban a mesterséges intelligenciára vonatkozó adatvédelmi szabályozás főbb jellemzőit kívánom bemutatni, figyelemmel a Javaslat által bevezetni kívánt szabályozási elvekkel kapcsolatos aktuális kérdésekre.

II. A Mesterséges Intelligenciáról Szóló Jogszabály

2021 április végén tette közzé az Európai Bizottság a mesterséges intelligencia szabályozására vonatkozó rendelettervezetét[17], amely a 2020. februárjában közzétett uniós MI stratégia – Fehér Könyv megvalósításának része, annak előzménye. A Fehér Könyv az MI-rendszereket illetően a bizalom és átláthatóság megteremtését tűzi ki célul. A bizalom megteremtése kapcsán a Fehér Könyv azt a hét kulcsfontosságú tényezőt említi meg, amelyet a Bizottság által létrehozott szakértői csoport fogalmazott meg az MI-re vonatkozó etikai ajánlásában[18], ezek a következők:

- emberi cselekvőképesség támogatása és emberi felügyelet
- műszaki stabilitás és biztonság
- adatvédelem és adatkezelés
- átláthatóság

[15] Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről, Hivatalos Lap , L 119, 4.5.2016, pp. 89–131 o.

[16] Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (EGT-vonatkozású szöveg.) PE/31/2018/REV/1, Hivatalos Lap 295, 21.11.2018, pp. 39–98.

[17] Javaslat Az Európai Parlament és A Tanács Rendelete A Mesterséges Intelligenciára Vonatkozó Harmonizált Szabályok (A Mesterséges Intelligenciáról Szóló Jogszabály) Megállapításáról és Egyes Uniós Jogalkotási Aktusok Módosításáról, COM/2021/206 Final

[18] Az Európai Bizottság által 2018 júniusában létrehozott ‚Mesterséges Intelligenciával Foglalkozó Magas Szintű Független Szakértői Csoport Megbízható Mesterséges Intelligenciára Vonatkozó Etikai Iránymutatása,(2019), https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_HU.pdf, (2021.10.10)

- sokféleség, megkülönböztetésmentesség és méltányosság
- társadalmi és környezeti jólét
- elszámoltathatóság

A Bizottság célja összességében az emberközpontú, fenntartható, biztonságos, befogadó és megbízható mesterséges intelligencia fejlesztése, amellyel összhangban a Javaslat konkrét célkitűzései az alábbiak:

- annak biztosítása, hogy az Unióban forgalomba hozott és használt MI-rendszerek biztonságosak legyenek, és tiszteletben tartsák az alapvető jogokra és az uniós értékekre vonatkozó hatályos jogszabályokat
- a jogbiztonság biztosítása a mesterséges intelligenciába történő beruházások és a mesterséges intelligenciát érintő innováció elősegítése érdekében
- az irányításnak és az MI-rendszerek tekintetében az alapvető jogokra és biztonsági követelményekre vonatkozó hatályos jogszabályok hatékony érvényesítésének a javítása
- a jogszerű, biztonságos és megbízható MI-alkalmazások tekintetében az egységes piac kialakításának elősegítése és a piac széttöredezettségének megelőzése

A Javaslat megfogalmazza az MI-rendszerek piaci bevezetésére, szolgáltatására, és használatára vonatkozó harmonizált szabályokat, egyes mesterséges intelligencia-gyakorlatok alkalmazására vonatkozó tilalmakat, a nagy kockázatú MI-rendszerekre vonatkozó különös követelményeket és az ilyen rendszerek üzemeltetőire vonatkozó kötelezettségeket, valamint a természetes személyekkel interakcióba lépő MI-rendszerekre vonatkozó harmonizált átláthatósági (transzparencia) szabályokat.

A megbízható mesterséges intelligencia kapcsán a Javaslatban kidolgozásra került szabályrendszer kockázatalapú megközelítést követ. E kockázatalapú megközelítés a Bizottság által valamennyi főbb érdekelt féllel folytatott konzultációjának eredménye, az érdekelt felek közé értve különösen a helyi önkormányzatokat, kereskedelmi és nem kereskedelmi szervezeteket, szociális partnereket, szakértőket, tudományos szakembereket és polgárokat. A mesterséges intelligencia fogalmának pontos meghatározása mellett az érdekelt felek többek között kiemelték a „*kockázat”*, a „*nagy kockázat”*, az „*alacsony kockázat”* és a „*távoli biometrikus azonosítás”* fogalmak meghatározásának szükségességét is.

A tiltott MI gyakorlatok közé – az elfogadhatatlan kockázat kategóriába azok az MI-rendszerek tartoznak, amelyek egyértelműen veszélyeztetik az emberek biztonságát, megélhetését és jogait - azaz amelyek használata elfogadhatatlannak minősül, mert ellentmond az uniós értékeknek, például az alapvető jogok megsértése miatt. A tilalmak azokra a gyakorlatokra vonatkoznak, amelyek képesek öntudatlanul, szubliminális technikák alkalmazásával nagymértékben manipulálni a személyeket, vagy kihasználni bizonyos veszélyeztetett csoportok, például a gyermekek vagy a fogyatékossággal élő személyek sebezhetőségét, hogy oly módon torzítsák magatartásukat, amely számukra vagy más személy számára valószínűsíthetően pszichológiai vagy fizikai károsodást okoz.

Ide tartoznak az olyan mesterséges intelligencia rendszerek vagy alkalmazások, amelyek manipulálják az emberi viselkedést a felhasználók szabad akaratának megkerülése érdekében - például kihasználják a gyermekek vagy a fogyatékossággal élő személyek sebezhetőségét, hogy oly módon torzítsák magatartásukat, amely számukra vagy más személy számára valószínűsíthetően pszichológiai vagy fizikai károsodást okoz-, valamint olyan rendszerek, amelyek lehetővé teszik a hatóság által végzett, általános célú „társadalmi pontozását".

A Javaslat a nagy kockázatú MI rendszerek két fő kategóriáját határozza meg:

- olyan MI-rendszerek, amelyeket harmadik fél által végzett előzetes megfelelőségértékelés hatálya alá tartozó termékek biztonsági alkatrészeként kívánnak használni
- egyéb, főként alapjogi vonatkozású, önálló MI-rendszerek, amelyeket a III. melléklet kifejezetten felsorol. Ezek az alábbiak:
    - természetes személyek biometrikus azonosítása és kategorizálása
    - kritikus infrastruktúrák (pl. közlekedés), amelyek veszélyeztethetik a polgárok életét és egészségét
    - oktatási vagy szakképzés, amely meghatározhatja valakinek az oktatáshoz való hozzáférését és az élete során a szakmai pályát (pl. vizsgák pontozása)
    - foglalkoztatás, munkavállalók irányítása és hozzáférés az önfoglalkoztatáshoz (pl. önéletrajz-válogató szoftver alkalmazása a toborzási eljárások során)
    - alapvető magán- és közszolgáltatások (pl. a természetes személyek hitelképességének értékelésére vagy hitelpontszámuk megállapítására szolgáló MI-rendszerek hitelbírálat)
    - bűnüldözés (pl. a bűncselekmények elemzésére szolgáló olyan MI-rendszerek, amelyek lehetővé teszik a bűnüldöző hatóságok számára a különböző

adatforrásokban vagy különböző adatformátumokban rendelkezésre álló, összetett és egymással nem összefüggő nagy adathalmazokban való keresést az adatokban megfigyelhető ismeretlen minták azonosítása vagy rejtett összefüggések feltárása érdekében.) Olyan bűnüldözési technikák[19], amelyek sértheti az emberek alapvető jogait (pl. a bizonyítékok megbízhatóságának értékelés

- migráció, menekültügy és határellenőrzés kezelése (pl. úti okmányok hitelességének ellenőrzése)
- Igazságszolgáltatás és demokratikus folyamatok (pl. MI-rendszerek, amelyek célja, hogy segítsék az igazságügyi hatóságokat a tények és a jog kutatásában és értelmezésében, valamint a jog konkrét tényállásra történő alkalmazásában).

A biometrikus adatok Javaslat által használt fogalma összhangban van a biometrikus adatoknak az (EU) 2016/679 európai parlamenti és tanácsi rendelet 4. cikkének 14. pontjában, az (EU) 2018/1725 európai parlamenti és tanácsi rendelet 3. cikkének 18. pontjában és az (EU) 2016/680 európai parlamenti és tanácsi irányelv 3. cikkének 13. pontjában meghatározott fogalmával, és azzal összhangban kell értelmezni. A Javaslat alapján valamennyi távoli biometrikus azonosító rendszer nagy kockázatúnak minősül, ezért azokat korlátozásokkal, illetve megfelelő garanciák megléte mellett lehet alkalmazni. A távoli biometrikus azonosító rendszerek élőben történő használata nyilvánosan hozzáférhető helyeken bűnüldözési célból elvi szinten tilos. A Javaslat elkülöníti a „*valós idejű*" és a „*nem valós idejű*" RBIS-t.
Amennyiben a „*valós idejű" távoli biometrikus azonosító rendszer* olyan távoli biometrikus azonosító rendszer, amelyben a biometrikus adatok rögzítése, az összehasonlítás és az azonosítása jelentős késleltetés nélkül történik. Ez nemcsak az azonnali azonosítást foglalja magában, hanem az intézkedések kijátszásának elkerülése érdekében a korlátozott rövid késleltetéseket is. Valós idejű rendszerek esetében a biometrikus adatok rögzítése, összehasonlítása és azonosítása azonnal, majdnem azonnal vagy mindenesetre jelentős késleltetés nélkül történik. A „*valós idejű*" rendszerek olyan „*élő*" vagy megközelítőleg „*élő*" anyagot, például videofelvételt használnak, amelyet kamera vagy hasonló funkciójú más eszköz generál.

[19] Nagy Zoltán András, 2021: Mesterséges intelligencia a bűnügyi munkában In: Ürmösné, Simon Gabriella; Kudar, Mariann (szerk.) Sokszinű Kar Konferencia III. : Absztraktfüzet Budapest, Magyarország : Nemzeti Közszolgálati Egyetem Rendészettudományi Kar (2021) p.20, p. 9., p.1.

A valós idejű RBIS lehetséges használata a nyilvánosság számára hozzáférhető helyeken[20] bűnüldözési célokból tiltott MI-gyakorlatnak minősül, kivéve, ha és amennyiben az ilyen használat az alábbi célok egyikéhez feltétlenül szükséges:

- a bűncselekmények konkrét potenciális áldozatainak célzott felkutatása, ideértve az eltűnt gyermekeket[21] is
- természetes személyek életét vagy fizikai biztonságát fenyegető konkrét, jelentős és közvetlen veszély, illetve terrortámadás[22,23] megelőzése
- a 2002/584/IB tanácsi kerethatározat 2. cikkének (2) bekezdésében említett bűncselekmények elkövetőinek vagy gyanúsítottjainak felderítése, lokalizálása, azonosítása vagy büntetőeljárás alá vonása, amennyiben e bűncselekmények esetében az érintett tagállam joga szerint e tagállamban a büntetési tétel felső határa legalább háromévi szabadságvesztés vagy szabadságelvonással járó intézkedés

A *nem valós idejű távoli biometrikus azonosító rendszer*: a *valós idejű* távoli biometrikus azonosító rendszertől eltérő távoli biometrikus azonosító rendszerként definiált. Azaz a biometrikus adatokat már rögzítették, és az összevetésre és az azonosításra csak jelentős késleltetéssel kerül sor. Ilyenek lehetnek a zártláncú televíziós kamerák vagy magánkészülékek által előállított képek vagy videofelvételek, amelyek a rendszer érintett természetes személyek tekintetében történő használata előtt keletkeztek.

A nagy kockázatú rendszerek használatával kapcsolatosan számos adatvédelmi szempontból is releváns feltételt határoz meg a Javaslat, úgy, mint az adatgyűjtés kritériumai, a technikai dokumentáció, a nyilvántartási kötelezettség, átláthatóság.

A Javaslat termékfelelősségi és az MI rendszerek megfelelőségével kapcsolatos részletes szabályokat is tartalmaz. Olyan mechanizmusok kialakítására törekszik, amelyek elősegítik a szabványosítást, a megfelelőségi vizsgálatokat, illetve tanúsítványok bevezetését az MI rendszerek alkalmazása során.

---

[20] Javaslat (9) „*E rendelet alkalmazásában a nyilvánosság számára hozzáférhető hely fogalma alatt bármely, a nyilvánosság számára hozzáférhető fizikai területet kell érteni, függetlenül attól, hogy a szóban forgó hely magán- vagy állami tulajdonban van-e"*

[21] Gál István László, Nagy Melánia, Ripszám Dóra, 2021: Gyermekkereskedelem a terrorizmus tükrében In: Mezőfi, Nóra; Németh, Kornél; Péter, Erzsébet; Püspök, Krisztián (szerk.) V. Turizmus és Biztonság Nemzetközi Tudományos Konferencia tanulmánykötet Nagykanizsa, Magyarország: Pannon Egyetem Nagykanizsai Kampusz (2021) p. 676., pp. 9-17., p.9.

[22] Kőhalmi László, 2015: Gondolatok a vallási indíttatású terrorizmus ürügyén, Belügyi Szemle: A Belügyminisztérium Szakmai Tudományos Folyóirata, 63: 7-8 pp. 52-71., 20 p.

[23] Tóth Dávid, 2014: A terrorizmus típusai és a kiberterrorizmus, In: Rab, Virág (szerk.) XII. Országos Grastyán Konferencia előadásai Pécs, Magyarország: PTE Grastyán Endre Szakkollégium (2014) p.333., pp. 286-296., p.11.

Amikor a mesterséges intelligencia rendszerekről beszélünk, nem lehet megkerülni a GDPR-t. Ennek oka, hogy a GDPR-nak volt a legnagyobb hatása a szabályozottabb adatpiac megteremtésében – miközben az adatok az MI-alkalmazások kulcsfontosságú összetevői. A GDPR számos speciális rendelkezése érinti az egyénekre vonatkozó mesterséges intelligencia-alapú döntéseket, különösen az automatizált döntéshozatal és profilalkotás vonatkozásában.[24]

III. Általános adatvédelmi megfontolások

A digitális Európa program már jól előkészített adatvédelmi háttérrel[25] készülhetett fel a negyedik ipari forradalom kihívásaira, így a mesterséges intelligencia rendszerek alkalmazására is. A jogi szabályozás alapján a már hatályban lévő uniós adatvédelmi jogszabályok – mint GDPR, EUDPR és LED – alkalmazandók a mesterséges intelligenciáról szóló rendelettervezet hatálya alá tartozó bármely személyes adat kezelésére is.

A GDPR 22. cikke fekteti le az automatizált döntéshozatal és profilalkotás általános korlátozására vonatkozó szabályokat, arra az esetre, ha a döntés kizárólag automatizált adatkezelésen alapul az érintett vonatkozásában – ideértve a profilalkotást is. Ezenkívül a GDPR 15. cikke lehetőséget biztosít az érintett számára a hozzáférési jog keretein belül, hogy megismerje a 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal tényét, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információkat, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

A GDPR már egyértelműen adatkezelésként nevesíti a profilozást[26] és személyes adatként az IP-címet, böngésző sütiket és a helymeghatározó adatokat is, csakúgy, mint a naplóállományokat, amennyiben azok egyéb információkkal összekapcsolva felhasználhatóak a természetes személyes profiljának létrehozására és az adott személy azonosítására.[27] A jogos érdekkel - mint adatkezelési jogalappal kapcsolatban - jogszerűnek nyilvánítja az olyan mértékű információbiztonsági célú személyes adatkezelést, „*amely a hálózati és informatikai biztonság garantálásához feltétlenül szükséges és arányos, vagyis adott titkossági szinten az érintett hálózat vagy információs rendszer ellenálló képessége az e hálózatokon és rendszereken tárolt vagy továbbított adatok, valamint az e hálózatok és rendszerek által nyújtott vagy rajtuk*

[24] 2016/679 Rendelet 22.Cikk
[25]Szőke Gergely László, 2015: Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén Budapest, Magyarország: HVG-ORAC, p.188.
[26] 2016/679 Rendelet 4. Cikk (4)
[27] 2016/679 Preambulum 30.

keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, integritását és bizalmas jellegét sértő véletlen eseményekkel, illetve jogellenes vagy rosszhiszemű tevékenységekkel szemben."[28] A monitorozás céljától függetlenül a jogos érdek csak akkor állapítható meg, ha az érintett ésszerűen számíthat arra, hogy adatkezelésre az adott célból a személyes adatok gyűjtésének időpontjában és azzal összefüggésben kerülhet sor, tehát már előre tudnia kell a profilalkotási eljárások alkalmazásáról. Tájékoztatási jog illeti meg az érintettet a profilozáshoz kapcsolódva. Amennyiben a profilalkotás során kialakult eredményre olyan döntés épül, ami az érintett helyzetét jelentős mértékben érinti akkor a tevékenység megkezdése előtt kötelező az adatvédelmi hatásvizsgálat[29] lefolytatása is. A Rendelet ugyanakkor számos adatbiztonsági előírást tartalmaz[30] valamint javasolja az álnevesítés (*pszeudonimizálás*) alkalmazását, ami azonban nem vezethet arra az eredményre, hogy a továbbiakban ne minősülne az adat személyes adatnak.

A Bűnügyi Irányelv egységes szabályokat állapít meg az EU valamennyi bűnüldöző szerve számára. A profilozással kapcsolatban kimondja, hogy „ *(…)az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés, amelynek joghatása az érintettre nézve hátrányos vagy őt jelentős mértékben érinti, tilos, kivéve, ha (…) uniós vagy tagállami jog teszi lehetővé, amely az érintettek jogaira és szabadságaira vonatkozó megfelelő garanciákról is rendelkezik, ideértve legalább az érintett jogát arra, hogy az adatkezelőtől emberi beavatkozást kérjen.*"[31]

Az MI alkalmazása jelentős részben igényel személyes adatokat vagy személyes jellegüktől megfosztott, ún. anonimizált adatokat. Ez vonatkozhat akár a gépi tanulási módszerek esetében szükséges adatokra, vagy akár az alkalmazások működésekor használt bemeneti adatokra is. A Mesterséges Intelligencia Koalíció Adatipar, adatvagyon munkacsoportja külön tanulmányban[32] elemezte a GDPR hatását a mesterséges intelligenciára épülő megoldásokra. Sikolya[33] ismertetése szerint a „*tanulmány megállapítja, hogy a GDPR 6. cikk (1) bekezdésében megengedett adatkezelési jogalapok többsége elvi vagy gyakorlati okokból nem vagy csak*

[28] 2016/679 Preambulum 49.
[29] 2016/679 Rendelet, 35. Cikk
[30] 2016/679 Rendelet, 32. Cikk
[31] 2016/680 Irányelv, 11. Cikk (1)
[32] „*GDPR konform adatfelhasználás, újrahasznosítás, anonimizálás, és más adatbiztonságot szolgáló technikák, hozzájárulás alkalmazhatósága és a releváns technikák vizsgálata (nyilvánosan nem közzétett tanulmány)*", idézi Sikolya Zsolt, 2019: Kormányzati Adatpolitika a Mesterséges Intelligencia korában. Áttekintés a mesterséges intelligenciában rejlő lehetőségek kiaknázásához szükséges kormányzati adatpolitikai feladatokról. Új Magyar Közigazgatás 12. évf. 4. szám, pp. 50-57.
[33] Sikolya Zsolt, Kormányzati … i.m. pp. 50-57.

nehézkesen alkalmazható személyes adatok mesterséges intelligencia számára történő felhasználására". Ezek:

- a jogos érdek alkalmazásának nehézségei - elsősorban a gépi tanulás során
- a hozzájárulás visszavonhatósága és beszerzésének nehézsége
- az automatizált döntéshozatalra, a profilalkotásra és az érintettek tájékoztatására vonatkozó szabályozás, ill. kapcsolódó iránymutatás erős korlátozásai
- a statisztikai célú adatkezeléssel kapcsolatos szabályozás határozatlanságai – például, hogy milyen adatkezelők esetében értelmezhető a statisztikai célú adatkezelés, és hogy ha a hivatalos statisztikán kívül is értelmezhető, akkor annak feltételeit mi szabályozza

Az idézett tanulmány szerint problémát jelent az adatgyűjtés céljától eltérő célból történő adatkezelésre vonatkozó szabályok alkalmazása. Az adatkezelés feltételei még szigorúbbak a különleges adatok esetében, például az egészségügyi adatok tekintetében.
Az anonimizálás kérdésével kapcsolatban felveti, hogy azok az eredetileg személyes adatok, amelyeket anonimizáltak, vagyis amelyek érintettjei többé nem azonosíthatók, már nem tartoznak a GDPR hatálya alá, felhívja a figyelmet arra is, hogy egyes esetekben fennáll annak veszélye, hogy éppen mesterséges intelligencián alapuló algoritmusokkal felfedhető az anonimizáltnak tekintett adatok kapcsolata az eredeti érintettekkel. Ezzel kapcsolatban levezeti, hogy nincs szükség az anonimizálásnál külön jogalap meghatározására, azt annak az adatkezelésnek a jogszerűsége dönti el, amelyhez az anonimizálást eszközként használják. Végül javasolja, hogy az MI alkalmazását nehezítő problémákat, a GDPR módosításával, állásfoglalásokkal, és nemzeti jog hatáskörébe utalva oldják meg.

Véleményem szerint az általános adatvédelmi rendelet egy bázis szabályozásnak tekinthető, és a technikai kihívások által szükségszerűen szabályozandó új területek sajátos, egyedi állásfoglalásokat tesznek szükségessé, adott esetben nemzeti hatáskörbe utalva bizonyos kérdések megoldását.[34]
Az adatvédelmi jogok az MI- rendszerekkel kapcsolatban is vonatkoznak az érintetettre, melyek a hozzáférési jog, a helyesbítéshez való jog, a törléshez való jog (az elfeledtetéshez való jog), az adathordozhatósághoz való jog, és az adatkezelés korlátozásához való jog.

[34] Erre jó példa a Budapesti Egyezmény II. Kiegészítő Jegyzőkönyvének tervezete, amely a kiberbűnözés elleni küzdelem további jogi kereteit szabályozza, és azon országok tekintetében, amelyek nem tartoznak a GDPR hatálya alá, a nemzeti jog keretébe utalja a szabályozást, annak érdekében, hogy a megkeresések a rendelet által meghatározott célt elérjék.(szerző megjegyzése)

IV. Az Európai Adatvédelmi Testület (EDPB) és az Európai Adatvédelmi Biztos (EDPS) 5/2021. számú közös véleménye a Javaslatról

II.

2021. június 21- én az EDPB és az európai adatvédelmi biztos közös véleményt fogadott el a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról szóló európai bizottsági rendelet javaslatával kapcsolatban.[35] Az európai adatvédelmi hatóság és az európai adatvédelmi biztos által bemutatott kérdések közül részletesebben mutatom be a Javaslat hatályával, a kockázat alapú megközelítéssel, a tiltással, a távoli biometrikus azonosítással és a megfelelőségi rendszerrel kapcsolatos aggályokat. Az állásfoglalás ezenkívül még foglalkozik az MI-rendszerek osztályozása, a „társadalmi pontozás", az európai adatvédelmi biztos kijelölése illetékes hatóságként és piacfelügyeleti hatóságként az uniós intézmények, ügynökségek és szervek felügyeletéért, a Mesterséges Intelligenciával Foglalkozó Európai Testület, a harmonizált jogérvényesítés, a mesterséges intelligenciát szabályozó teszt-környezetek, a magatartási kódexek részletes adatvédelmi szempontú szabályozásával.

Az állásfoglalás a Javaslat hatályával kapcsolatosan egyetért az MI-rendszerek Európai Unión belüli használata napirenden tartásának szükségességével, beleértve a MI-rendszerek uniós intézmények, testületek vagy ügynökségek általi használatát is. A nemzetközi bűnüldözési együttműködésnek a Javaslat hatálya alóli kizárása ugyanakkor aggályokat vet fel, mivel az ilyen kizárás jelentős kijátszási kockázatot jelent - például harmadik országok vagy olyan nemzetközi szervezetek esetében, amelyek nagy kockázatú alkalmazásokat működtetnek, amely szervezetek tevékenységére ugyanakkor az EU hatóságai szükségszerűen támaszkodnak. A vélemény a Javaslat alapjául szolgáló kockázatalapú megközelítéssel egyetért, úgy véli azonban, hogy az „*alapvető jogokat érintő kockázat*" fogalmát összhangba kell hozni az uniós adatvédelmi keretrendszerrel. Az EDPB és az európai adatvédelmi biztos ajánlása szerint az egyének csoportjait érintő társadalmi kockázatokat is értékelni és mérsékelni kell. Továbbá egyetértenek a Javaslattal abban, hogy egy MI-rendszer nagy kockázatúnak minősítése nem feltétlenül jelenti azt, hogy az önmagában jogszerű, és mint ilyen a felhasználó által alkalmazható. Szükségesnek tartják, hogy az uniós jogszabályokból eredő jogi kötelezettségeknek való megfelelés – ideértve a személyes adatok védelmére vonatkozó

[35] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) 18 June 2021, https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf, (2021.10.01)

jogszabályokat is – előfeltétele kell, hogy legyen annak, hogy az európai piacra tanúsítvánnyal - CE-jelöléssel - ellátott termékként léphessenek be.

Az EDPB és EDPBS tudomásul veszi a nagy kockázatú mesterséges intelligencia rendszerek a Javaslat II. és III. melléklete szerinti listáját. Hiányolja bizonyos típusú felhasználási esetek felsorolását, amelyek jelentős kockázatokat hordoznak magukban, mint például az MI használata a biztosítási díj megállapításához, vagy orvosi kezelések értékeléséhez, illetve egészségügyi kutatáshoz szükséges célokra. Ezért a fenti rendelkezéseket tartalmazó mellékletek frissítése álláspontjuk szerint kiemelt fontossággal bír.[36]

A Javaslat előírja a mesterséges intelligencia rendszer szolgáltatóinak kockázatértékelés elvégzését, azonban a legtöbb esetben az (adat)kezelők az MI-rendszerek felhasználói, nem pedig szolgáltatói - pl. egy arcfelismerő rendszer felhasználója „adatkezelő", ezért nem köti a nagy kockázatú mesterséges intelligencia-szolgáltatókra vonatkozó követelmény.[37] Ezenkívül a szolgáltatónak nem mindig lesz lehetősége felmérni előzetesen a mesterséges intelligencia-rendszer valamennyi későbbi felhasználását. Így a kezdeti kockázatértékelés megfelelő folyamatos compliance tevékenység biztosítása hiányában nagy eséllyel általánosabb lesz, mint az MI rendszer eredeti célok szerint meghatározott felhasználása. Még akkor is, ha a szolgáltató kezdeti kockázatértékelése nem jelzi, hogy a mesterséges intelligencia rendszer „*nagy kockázatú*" a Javaslat értelmében, ez nem zárhatja ki a későbbi értékelést - adatvédelmi hatásvizsgálatot (DPIA) - a GDPR 35. cikke alapján, valamint az EUDPR 39. cikke vagy a LED 27. cikke alapján.[38]

A mesterséges intelligencia tiltott használatának eseteivel kapcsolatos EDPB állásfoglalás szerint a mesterséges intelligencia rendszerek azon formáit – amelyek sértik az emberi méltóságot – a Javaslat 5. cikke értelmében *tiltott* mesterséges intelligencia-rendszereknek kell tekinteni ahelyett, hogy egyszerűen „nagy kockázatú" kategóriába sorolnák őket. Ez különösen vonatkozik az adatösszehasonlításokra, amelyek olyan személyeket érintenek, akik nem, vagy csak csekély okot adtak a rendőri megfigyelésre, vagy annak feldolgozására – mindezek sértik az adatvédelmi jog szerinti célhoz kötöttség elvét. Az MI használata nyilvános helyeken, a rendőrség és a rendvédelem által pontos, előrelátható és arányos szabályok alapján kell, hogy történjen, amelyeknek figyelembe kell venniük az érintett személyek érdekeit és azt, hogy milyen hatással vannak egy demokratikus társadalom működésére.[39]

[36] EDPB-EDPS Joint Opinion 5/2021, 19.
[37] EDPB-EDPS Joint Opinion 5/2021, 2.2 20.
[38] EDPB-EDPS Joint Opinion 5/2021, 2.3 21.
[39] EDPB-EDPS Joint Opinion 5/2021, 2.3 27.

A Javaslat 5. cikke (1) bekezdésének c) pontjában foglaltak szerint az MI használata „*társadalmi pontozásra*” diszkriminációhoz vezethet, és ellentétes az EU alapvető értékeivel. Magánvállalatok, különösen a közösségi média és a felhőszolgáltatás és egyéb szolgáltatók hatalmas mennyiségű személyes adatot dolgozhatnak fel, ezáltal ún. közösségi pontozást végezhetnek. Következésképpen a Javaslatnak *meg kell tiltania a társadalmi pontozás minden fajtáját.* Meg kell jegyezni, hogy a bűnüldözési összefüggésben a 4. cikk a LED alapján már jelentősen korlátozza – ha nem is tiltja – az ilyen típusú tevékenységeket.[40] Az állásfoglalás szerint az egyének nyilvánosan hozzáférhető helyeken történő biometrikus távoli azonosítása nagy kockázatot jelent az egyének magánéletébe való behatolás tekintetében. Az azonosító rendszerek átláthatósági problémákat és jogi vonatkozású kérdéseket is felvetnek az uniós jog szerinti adatkezelés alapján. Ezenkívül az egyének megfelelő tájékoztatásának módja, és az ezzel kapcsolatos adatkezelés továbbra is megoldatlan, valamint a magánszemélyek jogainak hatékony és időben történő gyakorlása sem megoldott.[41] Emiatt általános tilalmat javasolnak alkalmazni a következő esetekben:

- a mesterséges intelligencia bármilyen felhasználása az emberi tulajdonságok – például arcok, de a járás, az ujjlenyomatok, a DNS, a hang, a billentyűleütések és más biometrikus vagy viselkedési jelek – automatikus felismerésére nyilvánosság számára hozzáférhető helyeken, bármilyen kontextusban[42]
- a mesterséges intelligencia rendszerek, amelyek az egyéneket a biometrikus adatok alapján csoportokba sorolják etnikai hovatartozás, nem, valamint politikai vagy szexuális irányultság vagy a Charta 21. cikke szerinti egyéb megkülönböztetési okok szerint
- a mesterséges intelligencia használata természetes személy érzelmeinek kikövetkeztetésére[43] – kivéve: bizonyos jól meghatározott felhasználási eseteket, nevezetesen egészségügyi vagy kutatási célokat, mindig megfelelő biztosítékok mellett, beleértve a célhoz kötött korlátozást is.

Ezenkívül jogos elvárás a közterületen való névtelen megjelenés – ennek korlátozása közvetlen negatív hatással van a véleménynyilvánítási, a gyülekezési- és az egyesülési szabadság gyakorlására, illetve a mozgásszabadságra.

[40] EDPB-EDPS Joint Opinion 5/2021, 2.3 29.
[41] EDPB-EDPS Joint Opinion 5/2021, 2.3. 30.
[42] EDPB-EDPS Joint Opinion 5/2021, 2.3. 32.
[43] EDPB-EDPS Joint Opinion 5/2021, 2.3. 35.

Kérdés azonban, hogy mindezek milyen hatással vannak a bűnüldözéssel kapcsolatos szempontokra. A Javaslat 5. cikke (1) bekezdésének d) pontja kiterjedt listát tartalmaz a kivételekről, amelyekben megengedett a *valós idejű* távoli biometrikus azonosítás a nyilvánosan hozzáférhető helyeken bűnüldözési céllal.

Az európai adatvédelmi hatóság és az európai adatvédelmi biztos ezzel a megközelítéssel kapcsolatban több kifogást emel. Ugyanis nem világos, hogy a Javaslat mit ért „*jelentős késésleltetés*”[44] alatt, és ez milyen módon tekinthető enyhítő tényezőnek, tekintettel arra, hogy egy tömeges azonosítási rendszer néhány óra alatt több ezer egyedet képes azonosítani. Ezenkívül a feldolgozás intruzív (tolakódó) jellege nem mindig attól függ, hogy az azonosítás valós időben történik-e vagy sem. A távoli biometrikus azonosítás például politikai tiltakozás esetén valószínűleg jelentős hatással lesz az emberek alapvető jogaira és szabadságára, mint például a gyülekezési- és egyesülési szabadság, és általában véve a demokrácia alapelveire. Az adatkezelés intruzív jellege nem feltétlenül függ annak céljától. E rendszer más célokra, például magánbiztonsági célokra történő felhasználása ugyanolyan veszélyt jelent a magán- és családi élet tiszteletben tartásával kapcsolatosan, valamint a személyes adatok védelméhez fűződő alapvető jogokra nézve. Végül, még a tervezett korlátozások ellenére is, a bűncselekmények gyanúsítottjai vagy elkövetőinek potenciális száma szinte mindig „*elég magas*” lesz ahhoz, hogy indokolttá tegye a mesterséges intelligencia-rendszerek folyamatos használatát a gyanúsított felderítésére, annak ellenére, hogy a Javaslat 5. cikkének (2)–(4) bekezdésében meghatározott feltételeket állapítottak meg. „*A Javaslat indoklása úgy tűnik figyelmen kívül hagyja, hogy a nyílt területek nyomon követése során az uniós adatvédelmi jogszabályokból eredő kötelezettségeket nem csak a gyanúsítottakra, hanem mindazokra vonatkozóan kell teljesíteni, akiket a gyakorlatban megfigyelnek*”.[45] Ezekre az okokra hivatkozva kéri az EDPB és az EDPBS az MI- rendszerek emberi jellemzők automatizált felismerése céljából történő felhasználásának általános tilalmát nyilvánosan hozzáférhető helyeken.

Az emberi méltóságot is érinti, ha a valamilyen eszköz meghatározza vagy minősíti a jövőt. A hatóságok által használt mesterséges intelligencia rendszerek a természetes személyek egyéni kockázatértékelésének elvégzése során felmérik a természetes személy elkövetési kockázatát az ismételt bűncselekmények kapcsán.[46] Tényleges vagy potenciális bűnözői elkövetés

[44] JAVASLAT (8) megfogalmazása szerint : „ (…)A „*valós idejű” rendszerek esetében a biometrikus adatok rögzítése, összehasonlítása és azonosítása azonnal, majdnem azonnal vagy mindenesetre jelentős késleltetés nélkül történik” „(…) A „nem valós idejű” rendszerek esetében ezzel szemben a biometrikus adatokat már rögzítették, és az összevetésre és az azonosításra csak jelentős késleltetéssel kerül sor*.”

[45] EDPB-EDPS Joint Opinion 5/2021, 2.3. 31.

[46] JAVASLAT III. Melléklet III. 6. a) pontja

bekövetkezésének vagy megismétlődésének előre jelzésére használják a természetes személy profilalkotásán vagy személyiségjegyeinek felmérése alapján, vagy a múltbeli bűnözői magatartás alapján.[47] Ez a cél a rendőrségi és bírósági döntéshozatal sarkalatos alárendeléséhez vezet, és tárgyiasítja az érintett emberi lényt. Az ilyen MI-rendszerek megsértik a jog lényegét az emberi méltóságot, emiatt az 5. cikk értelmében ezeket az állásfoglalás szerint meg kell tiltani.[48]

A megfelelőség értékelési eljárással kapcsolatosan az EDPB és EDPBS ezen értékelések kiigazítását javasolja a Javaslat 43. cikke értelmében, hogy a nagy kockázatú MI esetében általában harmadik fél által végzett előzetes megfelelőségértékelésre kerüljön sor.[49]A Javaslat szerint[50] a nagy kockázatú mesterséges intelligencia-rendszerek esetében az új megfelelőség értékelési eljárást akkor kell alkalmazni, ha jelentős változás történik, például olyan MI-rendszerek esetén amelyeket a Javaslat előtt hoztak forgalomba és fejlesztésre kerültek. Fontos továbbá, hogy az MI-rendszerek teljes életciklusuk során megfeleljenek az MI-rendelet követelményeinek.[51] A Javaslatban felvázolt tanúsítási rendszerből hiányzik az egyértelmű kapcsolat az uniós adatvédelmi jogszabályokkal, valamint a nagy kockázatú mesterséges intelligencia-rendszerek egyes területeire alkalmazandó más uniós és tagállami jogszabályokkal. A Javaslatot éppen ezért módosítani szükséges az említett rendelet alapján kiállított tanúsítványok és az adatvédelmi tanúsítványok, pecsétek és jelölések közötti kapcsolat tisztázása érdekében.

Az EDPB és az európai adatvédelmi biztos emlékeztet arra, hogy az adatvédelmi hatóságok a személyes adatokat tartalmazó mesterséges intelligencia-rendszerek vonatkozásában már most is érvényesítik a GDPR-t és LED-et az alapvető jogok és különösen az adatvédelemhez való jog védelmének biztosítása érdekében. Ennek eredményeképpen az adatvédelmi hatóságok nemzeti felügyeleti hatóságként való kijelölése harmonizáltabb szabályozási megközelítést biztosítana és hozzájárulna az adatkezelési rendelkezések következetesebb értelmezéséhez az egész EU-ban, így a Javaslat alapján[52] nemzeti felügyeleti hatóságként történő kijelölésüket javasolja.[53] Mindenesetre az MI-rendszereknek a nyilvánosság számára hozzáférhető helyeken,

[47] JAVASLAT III. Melléklet 6. e) pontja
[48] EDPB-EDPS Joint Opinion 5/2021, 2.3 34.
[49] EDPB-EDPS Joint Opinion 5/2021, 2.4.1. 37.
[50] JAVASLAT 43. cikk (4)
[51] EDPB-EDPS Joint Opinion 5/2021, 2.4.1. 38.
[52] JAVASLAT 59. Cikk
[53] EDPB-EDPS Joint Opinion 5/2021,2.5.1 48.

bűnüldözés céljából, „valós idejű" távoli biometrikus azonosításra történő használatát érintő korlátozásokat – *független hatóságoknak* kell ellenőrizniük.[54]

Az egyén jogait illetően alapvetés, hogy az érintetteket mindig tájékoztatni kell, ha adataikat mesterséges intelligencia rendszerrel használják fel, - a feldolgozás jogalapjának előrejelzése, az eljárás általános magyarázata és az MI-rendszer hatálya tekintetében. E tekintetben az egyénnek joga van az adatkezelés korlátozásához[55] valamint az adatok törléséhez.[56] Az adatkezelőnek kifejezett kötelezettséget kell vállalnia arra, hogy tájékoztassa az érintettet a vonatkozó időszakokról, az MI-rendszernek képesnek kell lennie az összes ilyen feltétel teljesítésére.[57]

V. Összegzés

A mesterséges intelligencia használata egyértelműen számos kockázati elemet hordoz a természetes személyek jogai és szabadságai tekintetében, de megfelelő garanciákat és feltételeket tartalmazó szabályozással ezek a kockázatok csökkenthetők. A 2021 április végén megjelent mesterséges intelligencia szabályozására vonatkozó Javaslat jelentős előrelépés az Európai Unió jogalkotásában ezen a területen, aktualitása a technikai vívmányok nyomán szükségszerű, és a Fehér Könyv stratégiai megközelítésén alapul. Biztosított továbbá az összhang az Európai Unió Alapjogi Chartájával, illetve az adatvédelemre, a fogyasztóvédelemre, a megkülönböztetés mentességre és a nemek közötti egyenlőségre vonatkozóan meglévő másodlagos uniós jogszabályokkal. A Javaslat előfeltételei az általános adatvédelmi rendelet ((EU) 2016/679 rendelet), a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv ((EU) 2016/680 irányelv), valamint a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről szóló (EU) 2018/1725 rendelet. Kritikus területek az összhang tekintetében a nagy kockázatú MI-rendszerek tervezésére, fejlesztésére és használatára vonatkozó harmonizált szabályok, valamint a távoli biometrikus azonosító rendszerek bizonyos felhasználási módjaira vonatkozó korlátozások. Az Európai Adatvédelmi Testület (EDPB) és az Európai Adatvédelmi Biztos (EDPS) 2021 májusában véleményezte a Javaslatot az említett jogszabályok, az Alapjogi Charta vonatkozásában, és a megfelelőségi szabályokat illetően.

A Javaslat kockázatorientált megközelítésen alapul. Eszerint míg az „*elfogadhatatlan kockázatot*" jelentő mesterséges intelligencia-rendszereket betiltják, a „*nagy kockázatú*" MI-

[54] EDPB-EDPS Joint Opinion 5/2021,2.5.1 48.
[55] GDPR 18. cikk és EUDPR 20. Cikk
[56] GDPR 16.cikk és EUDPR 19.Cikk
[57] EDPB-EDPS Joint Opinion 5/2021, 3.1 60.

rendszerek szigorú kötelezettségek teljesítése mellett forgalomba hozhatók. A jogszabály legtöbb rendelkezése a nagy kockázatú rendszerekkel foglalkozik, kötelezettségeket telepít a szolgáltatókra, a felhasználókra és az MI-értéklánc többi résztvevőjére. Különös figyelmet fordít a megfelelőség értékelési eljárásokra, amelyeket követni kell a nagy kockázatú MI-rendszerek minden típusa esetében. Bár a kockázat alapú megközelítés alapvetően jó megközelítés, azonban a fogalmak értelmezése körül az EDPB és EDPBS szigorúbb kritériumokat szab, és a korlátoknak, valamint a tiltást illetően is nagyobb teret enged – utalok itt például a távoli biometrikus azonosítás általános tilalmára. További egyeztetés szükséges ezen területek vonatkozásában, - ideértve különösen a korlátozások egyértelműbb meghatározását, az időszakos - az MI -rendszerek további kiterjedtebb alkalmazásának újra értelmezését, a nemzeti szabályozás bevonásával a „nemzeti hatóságok" általi felügyeletet, - hogy az alapjogok védelme mellett az innováció fejlődése biztosítható maradjon. Kiemelt területet jelent a kivételek meghatározása egyes alkalmazások esetében, és a célok meghatározása, így például a bűnüldözési cél tekintetében, hiszen nyilvánvaló, hogy az egyének biztonsága ugyanolyan védendő érték, mint a személyes adatok védelme.

Ebers tanulmánya szerint, aki máris kritikáját adta a tanúsítási rendszereknek való megfelelőségnek,[58] a Javaslat középpontjában az új jogalkotási keret (New Legal Framework) szerinti szabványosításon nyugvó társszabályozás ötlete áll. A Javaslat szerint „*a szabványosításnak kulcsszerepet kell játszania abban, hogy az e rendeletnek való megfelelés biztosítására megfelelő műszaki megoldások álljanak a szolgáltatók rendelkezésére. A szolgáltatók az 1025/2012/EU Európai Parlamenti és Tanácsi rendeletben meghatározott harmonizált szabványoknak való megfelelés révén bizonyíthatják az e rendelet követelményeinek való megfelelést*."[59] Ezért a szabványok társszabályozással történő kidolgozása nélkülözhetetlen eleme a jövőbeli szabályozásnak. Ennek megfelelően a jogszabálytervezetnek jogilag előírt kötelezettségeket kell megállapítania a nagy kockázatú MI-rendszerekre vonatkozó alapvető követelmények tekintetében. Tehát további széleskörű konzultáció szükséges, amely a fogyasztóvédelmet, a civil szervezeteket is érinti a szabványosítást illetően.

A személyes adatok védelmét illetően egyetérthetünk az EDPB és EDBPS konklúziójával, mely szerint annak ellenére, hogy az európai adatvédelmi hatóság és az európai adatvédelmi biztos

[58] Ebers Martin, 2021: Standardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act In: The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, https://ssrn.com/abstract=3900378 or http://dx.doi.org/10.2139/ssrn.3900378, (2021.10.10)
[59] JAVASLAT Preambulum (61)

üdvözli a Bizottság javaslatát, és úgy ítéli meg, hogy egy ilyen szabályozás szükséges az uniós polgárok, és lakosok alapvető jogainak garantálásához, álláspontjuk szerint a Javaslat több kérdésben is módosítandó annak jobb alkalmazhatósága és hatékonysága érdekében.

Nagy Gergely Miklós*: A fintech - blockchain informatikai projektek kockázatmenedzsment stratégiájának megalapozása

Absztrakt:

A fintech - blockchain technológiai projektek tervezésénél a hátterében felmerülő szervezeti IT projektkockázatok kezelésének kérdéskörét fontos vizsgálni. A tanulmány célja bemutatni az IT projektek kockázatait és kockázatkezelési stratégiáit. A sikeres IT projekt egy komplex folyamat eredménye, amely megköveteli a tanácsadók, a menedzsment és a szervezet tagjainak szoros együttműködését. A vállalati észlelt tudás és a valós szakértelem közti különbség kiemelt kockázati tényező. Az IT projektek előrehaladásával a tanácsadói autonómia és döntésszabadság romlik, a vállalatvezetési intervenciók száma pedig nő. A nem megfelelően integrált kockázatmenedzsment szervezeti akadályokat jelent. Az IT projektkockázatokat célszerű projektmenedzsment kockázatokra, szervezeti kockázatokra, projektteljesítmény kockázatokra és technológiai kockázatokra bontani.

Kulcsszavak*: kockázatmenedzsment, projektmenedzsment, fintech, blockchain, IT, ICT*

I. Bevezetés

A tanulmány egy fókuszált áttekintése a gazdasági technológiai fejlődési pálya által meghatározott strukturális gazdaságfejlődés és a trendmeghatározó infokommunikációs technológiák kockázatkezelési dimenzióinak. Az elemzés során az IT (informatikai) erőforrások kockázatkezelését tekintjük elsődleges befolyásoló tényezőnek a szervezeti képességek kialakításának bemutatásakor.

II. A kockázatmenedzsment szerepe és folyamata

A kockázatmenedzsment egy rendszerszerű megközelítés, ami segít a vállalati kockázati elemek tényezőinek feltárásában és kiértékelésében a megfelelő kockázatmenedzsment akciótervek kidolgozása céljából. A kockázatoknak négy fő tulajdonsága van: bizonytalanság, dinamizmus, összekapcsoltság és komplexitás.[1]

* Nagy Gergely Miklós, Magyar Agrár- és Élettudományi Egyetem, Közgazdasági és Regionális Tudományok Doktori Iskola, PhD hallgató

[1] Wu D. D., Chen S. H., Olson D. L., 2014: Business intelligence in risk management: Some recent progresses, Information Sciences, Volume 256, 2014, pp. 1-7., ISSN 0020-0255, https://doi.org/10.1016/j.ins.2013.10.008.

A modern ICT eszközök szervezeti integrációja előtt a vállalatok jelentős része nem fordít elegendő erőforrást a saját üzleti folyamatainak felülvizsgálatára és a szükséges projektmenedzsmenti módszertan elemzésére.[2] A nem megfelelő folyamat implementáció operatív kockázatként, a software és hardware problémák technikai kockázatként, a hibás költségvetés pedig pénzügyi kockázatként jelenik meg az informatikai projekteknél.[3] A szükséges kiberbiztonsági szint elérése érdekében vállalatok számára kritikus feladat a kockázatokkal arányos felkészültségi szint elérése.

A projektek terjedelmén kívül álló kockázati forrásokat nehéz kezelni az egyes projektek keretében, ezekhez a szervezet egészének együttműködésére van szükség. Az integrált kockázatmenedzsment lényege a szervezet minden szintjére vonatkozó integráció.

A vállalat szolgáltatásának folytonossága és az adatbiztonság kiemelkedő szempont a kereskedelmi partnerek számára. A leghatékonyabb stratégia az ellátási láncok információellátásának biztosításához a kiberbiztonsági kockázatok aktív kezelése. Az ellátási láncok teljes integrációjának (szoftveres összekapcsolásának) a legnagyobb akadálya a megfelelő információbiztonság eléréséhez szükséges szakértelem és technológiai kapacitás hiánya. Az ellátási lánc mentén az egyes vállalatok gyakran egyedi szoftvereket használnak, amelyek összekapcsolása és integrálása biztonsági kockázatot jelent.[4]

Az ipar 4.0 információbiztonsági kockázatai

Operatív kockázati kategóriák	*Kockázat*
Termelési folyamat menedzsment	Adatvesztés és adatintegritás
Karbantartás	Adatelérhetőség és adatminőség
Operatív módszerek és eszközök	Hibás adatfeldolgozás
Termelési technológiák	Adatbiztonság és adatsebezhetőség
Humán erőforrás	A megfelelően képzett munkaerő hiánya
Gépi környezet	Internetes hálózati támadások, elektromágneses kompatibilitás és sugárzás okozta gépi problémák

Forrás: Tupa et al., 2017[5]

[2] Vujović V., Denić N., Stevanović V, Stevanović M., Stojanović J., Cao Y., Alhammadi Y., Jermsittiparsert K., Le H. V., Wakil K., Radojkovic I., 2020: Project planning and risk management as a success factor for IT projects in agricultural schools in Serbia, Technology in Society, Volume 63, 2020, 101371, ISSN 0160-791X, https://doi.org/10.1016/j.techsoc.2020.101371.

[3] Rekha J. H., Parvathi R., 2015: Survey on Software Project Risks and Big Data Analytics, Procedia Computer Science, Volume 50, 2015, pp. 295-300., ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.04.045.

[4] Boiko A., Shendryk V., Boiko O., 2019: Information systems for supply chain management: uncertainties, risks and cyber security, Procedia Computer Science, Volume 149, 2019, pp. 65-70., ISSN 1877-0509, https://doi.org/10.1016/j.procs.2019.01.108.

[5] Tupa J, Simota J, Steiner F., 2017: Aspects of Risk Management Implementation for Industry 4.0, Procedia Manufacturing, Volume 11, 2017, pp. 1223-1230., ISSN 2351-9789, https://doi.org/10.1016/j.promfg.2017.07.248.

A tradicionális kockázatelemzési technikákban a hardware és software kapcsolatok vizsgálata hiányos. A különköböző szoftvertípusok és felhasználási területek kockázat-menedzsmenti keretrendszere eltérő (pl. RiskUse, CMMI-DEV, SoftRisk, ISO31000). Az ISO 31000-es megközelítés általános kockázatmenedzsment tevékenységeket definiál a kommunikáció, terjedelemvizsgálat, kockázat-felismerés, kockázatelemzés, kockázatértékelés, kockázatkezelés, monitoring és adatrögzítés dimenziói szerint.[6]

A kockázati források sokfélesége miatt, a kockázati tényezők felmérése időigényes feladat. A kockázati tényező elemzését már az előkészítő vizsgálat során el kell végezni. A projekteltervezést megalapozó „üzleti tervrajz" elkészítése során a kockázati tényezőket megfelelő kockázatkezelési akciótervvel kell társítani. A rendszerbevezetés utáni post-implementációs fázisban már nem potenciális kockázatról beszélünk, mivel a nem megfelelően illesztett rendszer már ténylegesen realizált problémaforrássá válik.

A sikertelen projektek leggyakoribb buktatói[7]:

- *A felső vezetés részvételének és támogatásának hiánya:* nem megfelelő célrendszer és érdekegyeztetés a szervezeti hatékonyság drasztikus csökkenéséhez vezethet
- *A tanácsadói szolgáltatások nem megfelelő használata:* a külső tanácsadók kiválasztása a termék specifikus szakértelem alapján, a tanácsadó nem lehet projektmenedzser
- *A szoftvercégtől kapott támogatás diszfunkcionális:* a nem megfelelő támogatás esetén szükséges a szoftverváltás, a kapott támogatás sok esetben fontosabb, mint maga a rendszer
- *A felhasználók bevonásának hiánya:* a megfelelően motivált és tapasztalt embereket a projekt tervezési fázisa alatt fel kell menteni az általános feladataik alól
- *Alkalmatlan projektvezető vagy projektvezető hiánya:* olyan vezetőre van szükség, aki képes kezelni és leküzdeni a szervezeti ellenállást a projekt lefutása alatt

[6] Masso J., Pino F. J., Pardo C., 2020: Félix García, Mario Piattini, Risk management in the software life cycle: A systematic literature review, Computer Standards & Interfaces, Volume 71, 2020, 103431, ISSN 0920-5489, https://doi.org/10.1016/j.csi.2020.103431.

[7] Mamoghli S., Goepp V., Botta-Genoulaz V., 2018: An approach for the management of the risk factors impacting the model-based engineering methods in ERP projects, IFAC-PapersOnLine, Volume 51, Issue 11, 2018, pp. 1206-1211., ISSN 2405-8963, https://doi.org/10.1016/j.ifacol.2018.08.426.

- *A funkciók közti kommunikáció hiánya:* a rendszerek a vállalat egészére hatnak, szükséges a megfelelő kompromisszumok megállapítása, nem lehet csak a pénzügyi szempontokat érvényesíteni
- *Hibás projektmenedzsmenti technikák:* minden tervezési fázisnak célja van, a célok megvalósulását nyomon kell követni a szervezeti kontextusban
- *A projektcsapat nem megfelelő összetétele és a csapatmunka hiánya:* a diszfunkcionális projektcsapat új kockázati tényezőket jelent a projekt minden fázisa során

A kockázatmenedzsment tevékenység nem állhat le az IT rendszerek bevezetésével. A rendszerüzemeltetési kockázatokat folyamatosan kezelni kell. Ugyanakkor a bevezetési projektekkel szemben az üzemeltetési projektek szűkös erőforrásokkal működnek. Az Ipar 4.0 technológiák esetében a működtetés és a rendszermódosítások megszervezése a rendszerbevezetéssel azonos szakértelmet követel.

A vállalatok növekedésével és a vállalati struktúrák beágyazódásával, a vállalati kockázatvállalási hajlam csökken. A KKV-szektorban az erőforrások hiányában a kockázatmenedzsment hiányzó funkció, a kockázatok folyamatlapú, strukturált és stratégiával alátámasztott kiértékelése nem valósul meg.[8] A KKV-k körében a kockázatvállalási preferencia magas, a növekedési sebesség maximalizálása miatt.

III. A projektmenedzsmenti kockázatok kezelése

Az innovációs tevékenység irányításának a lényege az információbiztonság és a vállalati lendület biztosítása, a projekttámogató szervezeti hozzáállás fenntartásával.[9] A kockázatmenedzsment célja nem az összes kockázati tényező eliminálása, hanem az erőforrások összpontosítása a kockázati szint elfogadható határok között tartására.

Egy szoftver bevezetést az előkészületre, az implementációs és a post-implementációs fázisra tudjuk bontani. A menedzsment folyamat során a legfontosabb a projekttervezés, projektirányítás és projekt értékelés megalapozása. A sikeres ICT projektek esetében átlagban a pénzügyi források fele az előkészület és tervezési fázisra van allokálva. Az ipar 4.0 kockázatok definiáláshoz fontos az adatstruktúrák és kockázati mutatók egyértelmű

[8] Crovini C., Ossola G., Britzelmaier B., 2021: How to reconsider risk management in SMEs? An Advanced, Reasoned and Organised Literature Review, European Management Journal, Volume 39, Issue 1, 2021, pp. 118-134., ISSN 0263-2373, https://doi.org/10.1016/j.emj.2020.11.002.
[9] Ali A., Warren D., Mathiassen L., 2017: Cloud-based business services innovation: A risk management model, International Journal of Information Management, Volume 37, Issue 6, 2017, pp. 639-649., ISSN 0268-4012, https://doi.org/10.1016/j.ijinfomgt.2017.05.008.

definiálása.[10] Az erőforrás felhasználás hatékonyságának növelése érdekében a kockázati elemzésből kapott információkat már a szoftverfejlesztés tervezési fázisában figyelembe kell venni. Az előkészületi fázis fő eleme a megfelelő szoftvercsomag kiválasztása. Az „üzleti tervrajz" elkészítése és a telepítés az implementációs fázis során valósul meg. A post-implementációs fázis lényege az élesítés és a támogatás. A projektdokumentációk nem megfelelő minőségű elkészítése jelentős többletmunkát okoz a projektek zárásakor és veszélyezteti a bevezetett rendszer működésének transzparenciáját.

Az üzleti környezet dinamikus változásának hatására az IT projektekkel szembeni elvárások folyamatosan változnak és a projektek megvalósítására kiszabott időkorlátok szigorodnak. Továbbá a menedzsment elvárások, felhasználói elégedettség és a változásvezetés folyamata módosítja költségvetési korlátokat.[11]

IV. A szervezet és a projektcsapat kockázatainak kezelése

Az ICT technológiák által megalapozott kommunikációs csatornák megfelelő működtetésének kulcsa nem egy elkülönülő rendszer hatékony használatán, hanem a folyamatokat működtető összes rendszer egységes hatékonyságán múlik.

A szoftverekkel kapcsolatos kockázatmenedzsment megköveteli a résztvevők technikai tudását. A vállalati kríziscsapatokban az információbiztonsági kiber szakértők szerepe bevett gyakorlat. Az Ipar 4.0 projektcsapat ideális felépítése: folyamatfejlesztő, adatelemző, minőségbiztosítási szakember, termelési szakértő, szoftverfejlesztő, logisztikai menedzser, a karbantartásért felelős szakember és a felső vezetés képviselője.[12] A projektek előrehaladásával a résztvevők rendszerismerete folyamatosan nő, ezért a rendszerekkel szembeni elvárásuk is folyamatosan változik. Az IT projektek késéseinek fő forrása a felhasználói igények folyamatos változása, ezért érdemes már a projekt megkezdése előtt többletidővel kalkulálni.

A szervezeti működést transzformáló rendszerek bevezetésénél a legnagyobb kockázati forrás szervezeti felkészültség hiánya a projektek tervezési fázisában. A kvantitatív (QRA) és a valószínűség (PRA) alapú kockázatelemzési eszközöket érdemes kiegészíteni szocio-

[10] Tupa J, Simota J, Steiner F., 2017: Aspects of Risk Management Implementation for Industry 4.0, Procedia Manufacturing, Volume 11, 2017, pp. 1223-1230., ISSN 2351-9789, https://doi.org/10.1016/j.promfg.2017.07.248.

[11] Islam S., Mouratidis H., Weippl E. R., 2014: An empirical study on the implementation and evaluation of a goal-driven software development risk management model, Information and Software Technology, Volume 56, Issue 2, 2014, pp. 117-133., ISSN 0950-5849, https://doi.org/10.1016/j.infsof.2013.06.003.

[12] Hirman M., Benesova A., Steiner F., Tupa J., 2019: Project Management during the Industry 4.0 Implementation with Risk Factor Analysis, Procedia Manufacturing, Volume 38, 2019, pp. 1181-1188., ISSN 2351-9789, https://doi.org/10.1016/j.promfg.2020.01.208.

technikai eszközökkel (fókuszálva az emberek és gépek kapcsolatára, úgy, hogy az emberi értékek és a hatékonysági tényezők nem állnak egymással ellentmondásban).[13]

A szoció-technikai dimenziók két vagy több személy interakciója:

- Technológiával
- Belső munkakörnyezettel (fizikai és kulturális)
- Külső környezettel (társadalmi környezet, gazdasági környezet, stb…)
- A szervezeti struktúra menedzsment rendszereivel

A kockázati faktorok nyomon követése rendkívül fontos, mivel a felmerülő kockázatok alulbecslése csökkenti az alkalmazottak információ-feltárási hajlamát.[14] A kockázatmenedzsment gyakorlat szervezeti elfogadottságának növekedésével az alkalmazottak nyitottsága a releváns problémák reális időbeli jelzésére nő.[15]

V. A projektteljesítményi kockázatok kezelése

A kizárólagos összpontosítás a számszerűsíthető kockázatok kezelésére rontja a rugalmasságot, ezért fontos a szélesebb körű stratégiai szemlélet.[16]

Az innováció tervezés megalapozza a megfelelő üzleti partnerek kiválasztását, a vállalati rugalmasságot és a hatékony erőforrás allokációt. A kockázati elemek feltárása hozzájárul az általános üzleti célok összpontosításához. A vállalati teljesítménymérés és stratégiai tervezés részeként fontos a kulcs teljesítménymutatók (KPI) és kulcs kockázati indikátorok (KRI) társítása. A kockázatmenedzsment modellek felhasználási célterületei nincsenek kellőképpen definiálva. A dedikált kockázatkezelési modellek (ISO 27k, COBIT, ITIL, BSI) és technikák használata szelektív, helyettük a vállalatok az általános eszközöket (FMEA, brainstorming, CCA) preferálják.[17] Mivel technológiai fejlődés gyorsabb, mint a menedzsment gyakorlat válasza, ezért az IT képességeiket nem folyamatosan fejlesztő vállalatok nehezen tudnak IT projekteket sikeresen megvalósítani külső tanácsadók nélkül. Ugyanakkor az IT projektek

[13] Aven T., Ylönen M, 2018: A risk interpretation of sociotechnical safety perspectives, Reliability Engineering & System Safety, Volume 175, 2018, pp. 13-18., ISSN 0951-8320, https://doi.org/10.1016/j.ress.2018.03.004.
[14] Lee C. S., Watson-Manheim M. B., Chudoba K. M, 2014: Investigating the relationship between perceived risks in communication and ICT-enabled communicative behaviors, Information & Management, Volume 51, Issue 6, 2014, pp. 688-699., ISSN 0378-7206, https://doi.org/10.1016/j.im.2014.05.008.
[15] Fraser J. R. S., Quail R., Simkins B. J., 2021: Questions that are asked about enterprise risk management by risk practitioners, Business Horizons, 2021, , ISSN 0007-6813, https://doi.org/10.1016/j.bushor.2021.02.046.
[16] Arnold V., Benford T., Canada J., Sutton S. G., 2015: Leveraging integrated information systems to enhance strategic flexibility and performance: The enabling role of enterprise risk management, International Journal of Accounting Information Systems, Volume 19, 2015, pp. 1-16., ISSN 1467-0895, https://doi.org/10.1016/j.accinf.2015.10.001.
[17] Brunner M., Sauerwein C., 2020: Michael Felderer, Ruth Breu, Risk management practices in information security: Exploring the status quo in the DACH region, Computers & Security, Volume 92, 2020, 101776, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.101776.

során a vállalati észlelt tudás és tapasztalat felhalmozódásával a külső tanácsadók befolyása csökken.[18]

Az Ipar 4.0 projektek sikeres hosszú távú működtetéséhez mérlegelni kell a külső szakértők kilépésével kapcsolatos üzemeltetési kockázatokat. A vállalati tudásmenedzsment kritikus a felhalmozódott szervezeti tudás megőrzéséhez. Tudásmenedzsment stratégia nélkül a tapasztalt projektvezetők kilépésével, a szervezeti tudás elveszik.[19]

A szervezeti IT infrastruktúra szervezéséhez a menedzsment attitűdnek három elkülönülő megközelítése van. A passzív megközelítésre a technológiai lemaradás, a reaktív megközelítésre a magas munkaerő fluktuáció jellemző. A pragmatikus menedzsment rámutat, hogy a munka, ember és technológiai dimenziók együttesen változnak, ezért nem lehet elkülönülten kezelni őket.[20] A kiberbiztonsági kockázatok területén a vállalatok belső értékrendszerében jelentős aszimmetria mutatkozik a biztonsági kockázatok észlelésében és a megfelelő felkészültségi szintek megállapításában.[21] Az információs rendszerek hatékony fenntartásának akadálya a nem megfelelő rendszerhasználat és az IT képességein túlmutató menedzsment elvárások.[22]

A vállalati technológiai infrastruktúra információs rendszerek hálózata. A hálózatok méretének növelésével a kockázatok és kockázatkezelési költségek jelentősen megnövekednek. A vállalatok a felhő alapú szolgáltatásokat a költséghatékony skálázhatóság és infrastruktúra hiánya miatt választják. A felhő alapú szolgáltatások igénybevételével a vállalatok kiberbiztonsági és kockázatmenedzsment tevékenységének is át kell lépni a vállalati határokat, mivel a kockázatforrás és a vállalati sebezhetőség lényegében a külső partner adatbiztonsági gyakorlatán múlik. A disztributív megoldások kockázatkezelési tradicionális eszközökkel nem lehetségesek, a menedzsment szerepét teljesen újra kell definiálni.[23] A felhő

[18] Nguyen L. T: N., Fagerstrøm A., 2021: Understanding Client-Consultant Collaboration within Information Systems Design: A Case Study, Procedia Computer Science, Volume 181, 2021, pp. 730-737., ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.01.225.

[19] Filippetto A. S., Lima R., Barbosa J. L. V., 2021: A risk prediction model for software project management based on similarity analysis of context histories, Information and Software Technology, Volume 131, 2021, 106497, ISSN 0950-5849, https://doi.org/10.1016/j.infsof.2020.106497.

[20] Jarrahi M. H., Crowston K., Bondar K., Katzy B., 2017: A pragmatic approach to managing enterprise IT infrastructures in the era of consumerization and individualization of IT, International Journal of Information Management, Volume 37, Issue 6, 2017, pp. 566-575., ISSN 0268-4012, https://doi.org/10.1016/j.ijinfomgt.2017.05.016.

[21] Nam T., 2019: Understanding the gap between perceived threats to and preparedness for cybersecurity, Technology in Society, Volume 58, 2019, 101122, ISSN 0160-791X, https://doi.org/10.1016/j.techsoc.2019.03.005.

[22] Lopez C., Salmeron J. L., 2014: Dynamic risks modelling in ERP maintenance projects with FCM, Information Sciences, Volume 256, 2014, pp. 25-45., ISSN 0020-0255, https://doi.org/10.1016/j.ins.2012.05.026.

[23] Shrivastava S. V., Rathod U., 2015: Categorization of risk factors for distributed agile projects, Information and Software Technology, Volume 58, 2015, pp. 373-387., ISSN 0950-5849, https://doi.org/10.1016/j.infsof.2014.07.007.

alapú szolgáltatások kockázatának kezeléséhez szükséges az érintettekkel történő folyamatos kapcsolattartás, a folyamatos technológiai fejlesztés, az innováció tervezés és irányítás.

A vállalat kockázatmenedzsment stratégiájában a menedzserek magas rendszer-hozzáférési szintje kiemelt kockázati tényezőként szerepel. A nem költséghatékonyan kezelhető kockázati tényezőket közvetett eszközökkel kell kezelni. A kiber kitettség minimalizálásnak bevett gyakorlata a specifikus kiberbiztonsági biztosítás, amely sok esetben költséghatékonyabb kockázatkezelési lehetőséget jelent.

VI. A technológiai fejlesztés kockázatainak kezelése

A tradicionális szoftverfejlesztés a specifikációk teljes definiálásán, kivitelezésén és tesztelésén alapszik. Az agilis megközelítés ezzel ellentétben a követelményekhez való rugalmas alkalmazkodásra fókuszál. A terméktervezés során az agilis megközelítés működő verziókon keresztül folyamatosan újradefiniálja és alakítja az elvárásokat.

A klasszikus megközelítéssel szemben az agilis megközelítés egy nyitottabb általános projekteredmény elérésre fókuszál.[24] Az agilis szoftverfejlesztés fókuszában a kockázat és az értékteremtés áll. A kockázat a folyamatos visszacsatolásban, az értékközpontúság pedig a projektelvárások változásaihoz való rugalmas alkalmazkodásban valósul meg.[25] Az agilis megközelítésben a termék már a prototípus fázisban szervezetileg tesztelhető. Az agilis tervezés a prototípus tervezése során integrálja a kockázatkezelést. A disztributív szoftver fejlesztés (DSD) és a disztributív agilis fejlesztés (DAD) lehetővé teszi, hogy a vállalatok a szakértőkért a globális munkaerőpiacon versenyezzenek.

A szoftverekben rejlő kockázatok felmérésének alapja a szakértők által elkészített technikai dokumentáció.[26] A folytonosságot támogató automatikus döntés támogató szoftverek nélkül a komplex szoftverprojektek kockázatkezelése szinte lehetetlen.[27] Ugyanakkor a statisztikai előrejelzési modelleknek hatékonysága korlátozott olyan projektek esetében, ahol a kognitív

[24] Buganová K., Šimíčková J.,2019: Risk management in traditional and agile project management, Transportation Research Procedia, Volume 40, 2019, pp. 986-993., ISSN 2352-1465, https://doi.org/10.1016/j.trpro.2019.07.138.
[25] Beecham S., Clear T., Lal R., Noll J., 2021: Do scaling agile frameworks address global software development risks? An empirical study, Journal of Systems and Software, Volume 171, 2021, 110823, ISSN 0164-1212, https://doi.org/10.1016/j.jss.2020.110823.
[26] Thieme C. A., Mosleh A., Utne I. B., Hegde J., 2020: Incorporating software failure in risk analysis—Part 2: Risk modeling process and case study, Reliability Engineering & System Safety, Volume 198, 2020, 106804, ISSN 0951-8320, https://doi.org/10.1016/j.ress.2020.106804.
[27] Hu Y., Du J., Zhang X., Hao X., Ngai E. W. T., 2013: Ming Fan, Mei Liu, An integrative framework for intelligent software project risk planning, Decision Support Systems, Volume 55, Issue 4, 2013, pp. 927-937., ISSN 0167-9236, https://doi.org/10.1016/j.dss.2012.12.029.

bizonytalanság foka magas.[28] A neurális hálók a nem lineáris kapcsolati rendszerek esetén hatékonynak mutatkoznak a kockázati minták feltárásához.

Az IT rendszerek szervezeti feltételrendszere és a felhasználói elvárások egyaránt fontosak. A célvezérelt szoftverfejlesztés már a feltételrendszer megtervezése során kockázatmenedzsment megközelítést alkalmaz. A technológiai fejlesztés kulcsa a vállalati rendszerek kompatibilitásának folyamatos növelése.

A szoftverfejlesztést befolyásoló fő kockázati tényezők[29]*:*

- Részeredmények és előfeltételek időbeli csuszása
- A projekttagok a projekttel szembeni elkötelezettségének hiánya
- Projektdokumentáció minősége
- Kulcs csapattagok leterheltsége
- Kommunikációs csatornák működtetése
- A projektből kilépő tagok pótlása
- Idő és erőforráshiány
- Hiányos tudás a használt eszközökről
- Tapasztalat hiány
- A végfelhasználó igényeinek változása
- A használt rendszerek komplexitása
- A szükséges projektspecifikációk, elvárások begyűjtésének nehézsége
- Az egyes projektelemek kiszervezésének menedzsmentje
- Az üzleti tudás hiánya
- A fejlesztett rendszer rossz minősége
- Az elvárások módrációjának hiánya
- A munkavégzés helyének hiányossága

VII. A felhasználói kockázatok kezelése

Az információ biztonság területén a felkészültség hiánya vagy a túlköltekezés jellemző. A kibertámadásokkal szemben a legveszélyeztetettebbek a pénzügyi intézmények, a legveszélyesebb támadási forma pedig a „pszichológiai befolyásolás” (*social engineering*),

[28] Sangaiah A. K., Samuel O. W., Li X., Abdel-Basset M., Wang H., 2018: Towards an efficient risk assessment in software projects–Fuzzy reinforcement paradigm, Computers & Electrical Engineering, Volume 71, 2018, pp. 833-846, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2017.07.022.

[29] Alves L. M., Souza G., Ribeiro P., Machado R. J., 2021: Longevity of risks in software development projects: a comparative analysis with an academic environment, Procedia Computer Science, Volume 181, 2021, pp. 827-834., ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.01.236.

amelynek lényege a technológiai védelem kikerülése az emberek befolyásolásával.[30] A vállalatnak fel kell térképeznie a saját kiber ökoszisztémáját, amely rámutat külső működési környezetében lévő kockázati forrásaira (akár a stratégiai partnereinél megjelenő kockázatokként is megjelenhetnek). A külső és belső kitettségek összevetésével a vállalat költséghatékony kiberbiztonsági stratégiát tud kidolgozni. A *Fast Analytics, Big Data* és *Business Intelligence* a vállalatok információbázisának három fő pillére.[31]

Leggyakoribb kiberbiztonsági kockázati tényezők[32]

- *Felhő (cloud) alapú alkalmazások:* Az adatok és gyakran maga a szoftver egy külső partner szerverén található, a vállalatnak erre nincs rálátása.
- *Alkalmazottak saját eszközeinek használata munkavégzéshez (BYOD):* A saját eszközök (okostelefon, laptop, stb…) sebezhetőbbek, az egyes alkalmazottak kiberbiztonsági gyakorlata elmarad a vállalattól, ugyanakkor az eszközök folyamatos kapcsolatban vannak a vállalati hálózattal.
- *Hamis vezeték nélküli (Wi-Fi) hálózatok:* a hamis hálózatokhoz való csatlakozással támadhatóvá válnak a hálózati eszközök.
- *Hamis SMS linkek bankok/egyéb szolgáltatók nevében:* Az SMS-ben található hamis linkek megfertőzik és ellopják a felhasználó/vállalat adatait és akár a vállalati rendszerekhez is hozzáférést tudnak szerezni, amennyiben az eszköz csatlakozik a vállalati rendszerhez.
- *IoT eszközök összekapcsoltságának kihasználása:* Az IoT eszközök folyamatos kapcsolatban vannak egymással, az egész rendszer csak annyira biztonságos, mint a leggyengébb láncszem.
- *Túlterheléses támadás (DoS):* A vállalati rendszerek elérhetetlenné válnak, mivel a támadó tömeges hozzáférési kérelmeket küld a rendszernek, aminek a kapacitása ezt nem bírja.

[30] Varga S., Brynielsson J., Franke U., 2021: Cyber-threat perception and risk management in the Swedish financial sector, Computers & Security, Volume 105, 2021, 102239, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102239.
[31] Larson D., Chang V., 2016: A review and future direction of agile, business intelligence, analytics and data science, International Journal of Information Management, Volume 36, Issue 5, 2016, pp. 700-710., ISSN 0268-4012, https://doi.org/10.1016/j.ijinfomgt.2016.04.013.
[32] Lee I., 2021: Cybersecurity: Risk management framework and investment cost analysis, Business Horizons, 2021., ISSN 0007-6813, https://doi.org/10.1016/j.bushor.2021.02.022.

- *Biztonsági frissítések hiánya:* A szükséges rendszerkarbantartások nincsenek szervezetileg strukturálva.
- *Már nem fejlesztett régi rendszermaradványok:* Az egyes rendszerek lecserélésével szemben magas a szervezeti ellenállás ezért folyamatosan „foltozzák" őket, ami sebezhetőségeket generál.
- *A rendszervédelemhez használt szoftverek sebezhetősége:* A kiberbiztonsági szoftvereket is megfigyelés alatt kell tartani.

Minél komplexebb egy rendszer, annál nehezebb számszerűsíteni a benne rejlő kockázatokat. Az információbiztonsági technikák még mindig nagyban manuális adatgyűjtésen és komplex nem strukturált döntési folyamatokon alapszanak. A leggyakrabban használt kiberbiztonsági keretrendszerek: NIST, ISO/IEC 27001, COBIT, ANSI/ISA-62443-3-3, CKC.[33] Továbbá a Monte Carlo módszertannal szcenárióelemzést tudunk végezni az egyes ICT eszközök sebezhetőségéről.[34]

VIII. Összefoglalás

Az IT projekttel szembeni elvárások realizálásának feltétele a megfelelő menedzseri szemlélet. Az első lépés a projektköltség és komplexitás mérlegelése. A projekt komplexitását együttesen jelentik a szoftver konfigurációk és az implementációhoz szükséges erőforrások. A bevezetés előkészítésekor meg kell határozni a szervezet tagjainak vertikális és horizontális szerepét. A hatékony IT projektek erősségei között kiemelkedik az elkötelezett menedzsment, a szükséges erőforrások rendelkezésre állásának megtervezése, a megbízhatatlanságok kezelése, az időterv követése, a szervezeti átláthatóság folyamatos növekedése és az aktív oktatás. A kockázati tulajdonságok (terjedelem, módszertan, méret, fejlődés) hasonlóságainak elemzésével történeti kontextus építhető fel, amellyel elemezni tudjuk a projektpályát és a kockázati tényezőket. A kockázati tényezők beazonosításával fontos feltárnunk az ok-okozati kapcsolatokat. A kockázatelemzés során értékeljük a kockázatelemek kitettségének fokát. A kockázatértékelés a kockázatkezelési terv és az erőforrás allokáció alapjául szolgál, amely során a kockázati elemekből prioritás rendszert építünk. A projekt krízisterveket a projekt monitoring kontextusában folyamatosan értékeljük. Projektadatbázisok létrehozásával a

[33] Lee I., 2021: Cybersecurity: Risk management framework and investment cost analysis, Business Horizons, 2021., ISSN 0007-6813, https://doi.org/10.1016/j.bushor.2021.02.022.
[34] Baiardi F., Corò F., Tonelli F., Sgandurra D., 2014: Automating the assessment of ICT risk, Journal of Information Security and Applications, Volume 19, Issue 3, 2014, pp. 182-193., ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2014.04.002.

sikeres és sikertelen projektekkel megalapozott vállalati tudás költséghatékonyan támogatja az új projektek tervezési fázisait.

Nagy Zoltán András*: Nyomozás a blokkláncban a BTC után

Absztrakt:

A Bitcoin egy 2009-ben létrehozott digitális valuta. A blokklánc első verzióját a Bitcoin-protokoll vezette be. A blokklánc lényegében a tranzakciók digitális főkönyve, amely megkettőződik és szét van osztva a blokkláncon lévő számítógépes rendszerek teljes hálózatán. A lánc minden blokkja számos tranzakciót tartalmaz, és minden alkalommal, amikor új tranzakció történik a blokkláncon. Az adott tranzakció rekordja minden résztvevő főkönyvébe bekerül. A technológia alkalmas arra is, hogy különböző tiltott üzletkötést, bűncselekményből származó pénzek tisztára mosását és más bűncselekményeket hajtsanak végre.

Bitcoin is a digital currency created in 2009. The first version of the blockchain was introduced by the Bitcoin protocol. A blockchain is essentially a digital general ledger of transactions that is duplicated and distributed over the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and each time a new transaction occurs on the block chain. The record for that transaction is recorded in the general ledger of each participant. The technology is also capable of carrying out various illicit transactions, laundering the proceeds of crime and other criminal offenses.

Kulcsszavak: *Bitcoin, blokklánc, kiberbűnözés, nyomozás, Bitcoin, Blockchain, Cybercrime, Investigation*

I. Bevezető

A virtuális valuták létrejötte összefügg a mindig új megoldás utáni kutatás igényével és emellett a pénzügyi szféra iránti bizalom megrendülésével, a banki szférától való függőség megszűntetésének igényével. A kriptovaluták a szabadság – vágy (ezzel együtt a szabadosság, a visszaélések leplezésére irányuló törekvés) egyfajta új formában való kifejezése.

A bitcoinnak van egyfajta bizarr történelmi analógja egy ősi fizetőrendszerben, a mikronéziai („kicsiny szigetek" egyikén a) Yap szigeten a fizetőeszköz szimbolikus formájaként használtak.

* Dr. Nagy Zoltán András egyetemi docens, PTE ÁJK Büntetőjogi Tanszék, NKE RTK Bűnügyi-, Gazdaságvédelmi-, Kiber Bűnözés Elleni Tanszék

A yapik a *rai* nevű gyakran óriási mészkőkorongok formájában bonyolították le mindennapi üzleteiket. A kövekkel, amelyek nagy tömegük és sérülékenységük miatt jellemzően szanaszét hevertek a szigeten, sőt némelyek a tenger fenekén volt találhatóak.[1]

A yapik ezekkel a kövekkel kötöttek üzletet, ha létrejött az üzlet, akkor körbejárták a szigetet és elmondták mindenkinek. Az üzletkötés, a csere, az ajándékozás tehát a szigetlakók nyilvánossága előtt zajlott. A yapik emlékezetükben (memóriájukban) tárolták azokat, egyben tudomást szerezve arról, hogy kinek-kinek a köve cserélt „gazdát", anélkül, hogy a fizikai térben a helye megváltozott volna. Nem mellesleg a kövek eltulajdonítása értelmetlen volt, hiszen mindenki tudta az adott pillanatban azt, hogy kié a kő. A szigetlakók egymás között kommunikációja a kövek cseréjéről szóló főkönyv – amelyet a yapik által megosztott és nemzedékeken át öröklődő történetek meséltek el és amely – segített a közösségnek rögzíteni és közölni a *raik* tulajdonjogában bekövetkezett változásokat.

Ahogy a kövek cseréje több szigetlakó személy emlékezetében él, úgy a kriptovaluták tranzakciói több felhasználó számítógépéből álló hálózaton oszlik el, nyilvánosak, ezzel átláthatók, emiatt biztonságosak.

A tranzakciók digitális főkönyve lényegében a blokklánc, a blokkláncban lévő számítógépes rendszerek teljes hálózatán keresztül sokszorosítanak és osztanak szét.

A blokklánc egy elosztott főkönyv (Distributed Ledger Technology - DLT), amely ún. hash függvényeket használ[2] és ezzel minden tranzakcióról egyedi ujjlenyomatot hoz létre, így rögzítve és hitelesítve azokat. Amikor minden egyes tranzakciót aláírnak és egyedinek igazolnak, a rendszer elküldi azokat, hogy csatlakozzon más blokkhoz, és ezzel lehetetlenné válik a módosítása. Ezek a blokkok együtt alkotják a blokkláncot.

A technológia alkalmas arra, hogy készpénz (kövek ide-odaadogatásának) mellőzésével, az elektronikus adatokkal végzett pénzügyi műveletekre, internet banking és más szolgáltatások lebonyolítására és az internetes vásárlások megkönnyítésére. De tegyük hozzá mindezek elrejthetők a kíváncsi szemek előtt. Nem szükséges kizárólag pénzben gondolkodni, ugyanígy értékpapír is lehet tranzakciók tárgya.

A kriptovalutákkal, így a bitcoinnal a műveletek a blokklánc – más néven elosztott főkönyvi technológia alapján működhetnek.

Működési elve – vázlatszerűen:

---

[1] Kardos Sándor, Varga Péter, Papp Norbert: Kryptoda Bevezetés a kriptovaluták világába lásd https://kryptoda.com/wp-content/uploads/2021/06/KRIPTO-START-Bevezetes-a-kriptovalutak-vilagaba-V1.1.pdf (2022.03.25) 5-6. old.

[2] https://gobertpartners.com/what-hashing-algorithm-should-i-use-1 (2022.03.25.)

- a bitcoin vásárlása és eladása számítógépek hálózatába, úgynevezett csomópontokba kerül.

A több ezer csomópontból álló hálózat számítógépes algoritmusok segítségével próbálja megerősíteni a tranzakciót. Ezt bitcoin bányászatnak nevezik. Az a bányász, aki először teljesít sikeresen egy új blokkot, bitcoinnal jutalmazzák ezért.

- A vásárlás megerősítése után ez az eladás hozzáadódik egy blokkhoz az elosztott főkönyvben. Ezután a hálózat többségének meg kell erősítenie az eladást.
- A blokk véglegesen hozzá lesz láncolva az összes korábbi bitcoin-tranzakció blokkhoz, ezzel az eladás feldolgozásra kerül.

A kriptovaluták népszerűségének titka az – a fentiek alapján látható, - hogy az azokkal végzett tranzakciók egy központi intézménytől, in concreto a nemzeti bankoktól függetlenek, jellemzően decentralizáltak, konverziós költségeik nincsenek, továbbá a digitális valuták hamisíthatatlanok, valódi valutára vagy más virtuális valutára konvertálhatók. A felhasználók anonimok maradhatnak, nincs személyiséglopás. A kriptovaluták ellopása, a főkönyv megváltoztatása a rendszeren belül általában nem lehetséges.

További előnyként említhetjük, hogy a tranzakcióban részt vevő felhasználók egyenrangúak, amely a valós térbeli pénzügyi intézmény (bank, biztosító) és ügyfél kapcsolatban, bár de jure deklarált, ám de facto hagy maga után kívánnivalót (a pénzintézet által kidolgozott, érdekeit maximálisan kielégítő, diktált szerződési feltételek, az ügyfél kívánsága e szigorú feltételek között esetlegesen lehetséges stb.).

A hálózatban tranzakciókat lehet lebonyolítani anélkül, hogy azok bármelyik résztvevőjében - eladóban, vevőben vagy a bankban - meg kellene bízni. A bizalmat a rendszer matematikai alapjai helyettesítik: minden egyes Bitcoin egyedi, tehát nem lehet őket hamisítani. A tranzakció gyorsan végrehajtható, illetve nem visszavonható.

A virtuális valuta működését, használatát a Bitcoinon, mint a legnépszerűbb elektronikus fizetőeszközön keresztül mutatjuk be, ami egy virtuális valuta és fizetési rendszer is egyben, amelyet 2009-ben egy Satoshi Nakamoto felhasználó talált ki.

A Bitcoin nyílt forráskódú digitális valuta. A kliens program letöltését követően, annak egyidejű telepítésével, automatikusan létrehoz egy, az ügyfél azonosítására alkalmas fogadó címet és a hozzá tartozó jelszót. A rendszert használók ezt az azonosító számsort láthatják, - ismételjük - anélkül, hogy a mögöttük álló felhasználó beazonosítható lenne. Többféle módon tehet szert a felhasználó Bitcoinra:

„Bányászattal". A rendszert – természetesen nem véletlenül – úgy alakították ki, hogy a rendszerbe lépők érdekeltek legyenek a Bitcoin gyűjtésében, illetőleg a felhasználóknak

kiosztott „ajándék” Bitcoinok keresletet teremtsenek és ezzel a kínálati oldal (kereskedők, szolgáltatók) érdeklődését felkeltsék.

A felhasználó egy program telepítésével számítógépének kapacitását a Bitcoin - hálózatban folyó tranzakciók, a közös kriptográfiai feladatok megoldása - szolgálatába állítja. Minden elvégzett művelet után kap a felhasználó egy "lottószelvényt", amellyel a körülbelül tíz percenkénti sorsolásban részt vesz és ezzel meghatározott mennyiségű virtuális valuta nyerhető. A nyerési esély a minimálisnál is kevesebb, hiszen a világban felhasználók milliói közül kerülnek ki a nyertesek. „Bányász farmok” próbálnak pénzt nyerni ilyen módon, illetve ilyen farmmal szerez pénzt mind a mai napig az Iszlám Állam nevű terrorszervezet is. Az áramfogyasztás, valamint a CPU, a videókártya leamortizálása jóval többe kerül. Bitcoin adásvétel zajlik a Surface- éppúgy, mint a Deep- és ezen belül a Dark-Weben. Az adásvétel ellenőrizetlen és ellenőrizhetetlen (például két karibi ország bankszámlája érintett az ügyletben, de a pénz „körbejárja” a Földet, amíg megérkezik a vevő vagy eladó bankszámlájára) vagy P2P kapcsolaton keresztül zajlik, bár maga a művelet látható (azonosítószámok látszanak), ám az, hogy kit takarnak az azonosítószámok az nem tudható. Az eladó meghirdeti, hogy milyen árfolyamon kíván vásárolni vagy eladni, ha megfelel az árfolyam és a valutaneme is, akkor létrejön az üzlet.

Ma Bitcoinnal lehet legálisan fizetni árukért és szolgáltatásokért. A Bitcoin népszerűsítésével, a kereslet növelésével az ilyen üzleti tranzakciók bővítése céljából „oszt ki” a rendszer „ajándék” Bitcoinokat. A Bitcoint nemcsak az e-kereskedelem körén belül, hanem a valós térben is elfogadják, mint fizetőeszközt (pl. vendéglátóhelyeken, koncertjegyek értékesítésekor stb.).

Utcán, vendéglátóhelyen felállított automatán keresztül szintén vásárolható Bitcoin. A művelet elvégzésére szükség van egy mobiltelefonra, amellyel a „Bitcoin – tárca” QR kódja érvényesíthető. Majd jöhet a bankjegyeknek az automatába helyezése és a tranzakció ellenőrzése a mobiltelefonon. Budapesten a Pólus Centerben állították fel ilyen automatát.

Sajnos, szomorú tapasztalat digitális környezetben, hogy a bűnözők gyorsabban felhasználják az új technológiákat.[3]

A kriptovaluta új eszköz a bűnözők kezében pénzmosáshoz, tiltott dolgok vásárlásához stb. A Dark-web széles választékban áll a bűnözők rendelkezésére, hamis okirat, fegyver, kábítószer, pornográffelvételek, szerzői alkotások vehetők, botnet-hálózat-, bérgyilkos

[3] Eszteri Dániel, 2012: Bitcoin: Az anarchisták pénze vagy a jövő fizetőeszköze? Jura, 2012. 2. szám pp. 86 – 90.

bérelhető, bűncselekmény elkövetéséhez „specialista” kereshető és lehetetlen felsorolni az „áruválasztékot”.

A bűnözők ezirányú tudása, ismerete, kreativitása nemcsak a felhasználók, hanem a nyomozóhatóságok tudását is jellemzően meghaladja.

A Bitcoin alkalmas pénzmosásra, forgalmuk ellenőrizetlen, ellenőrizhetetlen és követhetetlen.[4] Nagy összegek cserélhetnek gazdák a felhasználók közötti közvetlen kapcsolat segítségével, egyes felhasználók több Bitcoinos „pénztárcával” rendelkezhetnek, nincs központja a hálózatnak, szerverek működnek valahol a „felhőben”, bár a tranzakciók ismertté válhatnak (nagy tömegű, folyamatos adatáramlás figyelemmel kísérése igencsak aggályos), a felhasználók nem válnak ismertté. Ezek a tulajdonságai persze felkeltették az illegális üzletet folytatók figyelmét is. Például az Internet egyik legsötétebb - emiatt népszerű - piaca volt a Silk Road I, majd a Silk Road II., ahol Bitcoinnal is lehetett közvetlenül fizetni.

III. II. Hogyan lehet feltárni a gyanús Bitcoinos tranzakciókat?

Az Europol internetes szervezett bűnözéssel foglalkozó részlege külön Ajánlást fogalmazott meg a virtuális valutákkal vagy azok használatával összefüggő bűncselekmények elleni fellépésről, amely szerint a következő lépéseket kell megtenni:
A nyomozóknak azonosítaniuk kell és bizalmi kapcsolatokat kell kialakítaniuk minden, a joghatóságukban működő kriptovalutával kapcsolatos vállalkozással, például pénzváltókkal, bányászati készletekkel vagy pénztárca-üzemeltetőkkel.

Egyre többet kell beruházniuk vagy részt kell venniük tagállamoknak a megfelelő szakképzésben és vizsgálati eszközökben annak érdekében, hogy növeljék kapacitásukat a kriptovaluták által felvetett problémák hatékony kezelésére.

A kriptovaluták vizsgálatának a kiberbűnözés nyomozóinak szerves készségévé kell válnia. A bűnüldözés és az ipar közötti szoros együttműködés az egyetlen módja annak, hogy sikeresen fel lehessen lépni a kiberbűncselekmények ellen, ezen belül is a kriptovalutákkal végrehajtott visszaélések ellen. Ennek lehetőségei körvonalazódnak, hiszen az érintett vállalkozások jelentős veszteségeket könyvelhetnek el a kriptopénzekkel elkövetett manipulációk miatt.[5]

[4] Miskolczi Barna – Szathmáry Zoltán, 2018: Büntetőjogi kérdések az információk korában. HVG-Orac, pp.146-165. és Jamie Bartlet, 2015: The DarkNet. Windmill Books, pp. 148-155

[5] https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018 full report, p. 64. (2021. november 20.)

Kezdjük a bűnügyi nyomozás lehetőségével.[6] Valós térben és a virtuális térben együttesen zajló nyomozati cselekmények, a különböző alosztályok szoros együttműködése vezethet sikerre ebben a jól leplezett pénzügyi üzletek megismerésében, a visszaélések feltárásban. Olyan nyomozókra van szükség, akik jártasak az informatikában, a blokklánc- és a kriptovaluták világában.

Kiindulási pont lehet az, hogy a felhasználó a Bitcoin-tranzakcióban nem „névtelen", hanem csupán „álnév" alatt ténykedik, és ez segíthet személyes adatainak, személyének felkutatására. A Bitcoin-műveletekhez két számsor szükséges. Egy „nyilvános (publikus)„ és egy „privát kulcs". A „nyilvános kulcs" az a szám- és betűsor, amelyet a Bitcoin-tulajdonosok a tranzakcióhoz használnak, míg a „privát kulcs" a pénztárca és a személy anonimitásának megőrzésére szolgál.

A nyomozói munka nem könnyű feladata az, hogy a nyilvános elosztott főkönyvben megjelenő „publikus kulcsot" kell összekapcsolni a „privát kulccsal", ami által megismerhető lesz a tranzakció végrehajtója és ez a további nyomozati cselekményekhez nyújt információt.
A valós térben megjelenő a bűncselekményt a kriptovalutával végzett műveletek kísérik, megelőzhetik vagy követhetik azt. Például „nagy szállítmány" érkezett vagy érkezése várható, amit a „piacon" terjesztenek (drogot, prostituáltakat), elszaporodtak a jelentős hasznot hozó bűncselekmények (rablások, embercsempészés, okirat hamisítások, [nyelvvizsgabizonyítványok]), továbbá zsarolóvírus-támadásról, túlterheléses támadás végrehajtásával történő zsarolásról érkezett információ, netán szokatlan forgalom a BTC-automatáknál, de bármely jogtalan haszon végett elkövetett bűncselekményeket követhetnek pénzmozgások a virtuális térben.

Ebben az esetben az adott bűncselekménnyel adekvát kriminál technikai, kriminál taktikai, illetve kriminálmetodikai módszerekkel történik az elkövetők, köztük a kriptovalutával üzletelő személy felkutatása, cselekményeik bizonyítása.

Másfelől a kriptovalutával végrehajtott blokklánc-művelet elemzése révén juthatnak a hatóságok a „privát kulcs" tulajdonosához. Mivel a főkönyv nyilvános, a BTC-műveletekből kitudható, a felhasználó mennyit, mikor, hol, milyen időközönként költötte a kriptovalutát. Feltérképezhető a felhasználó által elköltött pénz mennyisége, iránya, a vásárolt áru, pénz, szolgáltatás utalhat életvitelére. Ez az elkövetőre vonatkozó profilalkotáshoz nyújt információkat, esetleg utalva a cselekményére is. Viszont egyszersmind a felhasználó is zsarolhatóvá válhat más bűnözők által.

[6] Simon Béla, 2018: Kriptovaluták – rendészeti válaszok. Belügyi Szemle , 66 (10), pp. 71-87.

Minden egyes „digitális morzsa” az elkövetőről vagy cselekményéről fontos adalék a sikeres nyomozáshoz. Kiber nyomozók kreatív munkája az elsődleges lehetőség a sikerhez. A hazai kiber nyomozókat a nemzetközi kapcsolatrendszer segíti, hiszen ezek a tranzakciók – jellemzően – nem országhatáron belül bonyolódnak.

A kriptovalutás tranzakciók, ahogy fentebb is említés történt, sok esetben különféle bűncselekményt vagy visszaélést valósítanak meg vagy azok pénzügyi hátterét képezik.[7]

Ezek a tranzakciók azonban különböző vállalatok pénzügyi érdekeit is sértik, amelyeknek fizetési rendszerük biztonságának fokozása és az okozott kár megtérülése az érdeke.

Ezt a piaci igényt felismerve több magánvállalkozás jött létre[8], amelyek különböző – általuk használt - módszerekkel, magas díjazás fejében a megbízó kívánságának megfelelően a gyanús vagy gyanúsnak vélt kriptovalutával végrehajtott tranzakciót nyomon követhetik, feltárhatják a visszaéléseket vagy azok forrásait.

IV. III. Összegzés

Bebizonyosodik az, hogy ahol komoly pénzügyi érdekek megjelennek, ott ezen érdekek védelme erős motiváció, és ott utat tör a vállalkozói kedv.

Ez az – egyébként – profitorientált tevékenység a bűnüldözés sikeréhez nagyban hozzájárulhat, ha a sérelmet szenvedett vállalkozások a visszaélések feltárását követően feljelentést is tesznek megjelölve azok bizonyítékait.

Ezzel szembe mehet az, hogy a vállalkozások a kemény piaci versenyben – joggal – féltik a goodwilljüket. Nyilván piacrontó tényező a vállalkozás informatikai rendszerének sebezhetősége, az ügyfelek, betétesek befektetései, pénzügyi műveletei nem biztonságosak, veszélyben vannak. Ugyan így az, ha az ügyfelek pénzei „ebek harmincadjára kerülnek”.

Kérdés az, hogy a pénzintézetek goodwillje vagy a bűncselekmény felderítése lesz elsődleges? Ez a bankkártya visszaélések kapcsán is komoly dilemma a pénzintézetek számára, üzleti veszteségnek betudva leírják a veszteségeket vagy feljelentést tesznek.

A vállalkozások és a nyomozó hatóságok érdekei tehát összeérnek, egymást erősíthetik. Együttes fellépésük – elvileg - közös érdek, a nyomozások sikerét ígéri.

[7] Marc Goodman, 2015: Future Crimes. Penguin Random House., pp. 309-315.

[8] TRM Labs, https://www.trmlabs.com/; Elliptic Co. https://www.elliptic.co/; Chainalysis: https://www.chainalysis.com/, (2021. november 20.) További vállalkozások is dolgoznak ezen a területen. A vállalkozások tevékenységükről, kapcsolatfelvételről és más részletekről a honlapjaikról lehet tájékozódni. Módszereik természetesen nem nyilvánosak.

Prisznyák Alexandra*: „Tradicionális” bankok front/middle/back office területeinek mesterséges intelligencia (AI), gépi tanulás (ML) implementációja

Absztrakt:

A „tradicionális bankok” digitális transzformációja az élenjárok, követők és lemaradók esetében a mesterséges intelligencia, gépi tanulás és kapcsolódó technológiák eltérő mértékű adaptációjával társul. A nagy mennyiségű adatokon nyugvó mesterséges intelligencia és gépi tanulás tradicionális banki folyamatokba történő integrálása nagymértékben hozzájárul a komplex problémák megoldásához, előrejelzés készítéshez, döntéstámogatáshoz, a napi rutinfeladatok automatizálásához. Jelen tanulmány áttekintést nyújt a banki front/middle/back office területeken alkalmazott mesterséges intelligencia és gépi tanulás megoldásokról, kiemeltképpen vizsgálva az alábbi területeket: marketing, portfólió- és vagyonkezelés, tőzsdei árfolyamok előrejelzése, kockázatkezelés (modell validáció, visszamérés, revízió), hitelezési folyamatok, emberi erőforrás menedzsment, Compliance, pénzmosás és terrorizmusfinanszírozás megakadályozása, csalásmegelőzés. A mesterséges intelligencia és gépi tanulási megoldások piacon alkalmazott formáinak áttekintése iránytűként szolgálthat a hazai tradicionális bankok adaptációs szintjének felméréséhez, hatékonyságuk és eredményességük növeléséhez, továbbá a jogszabályi megfelelőség biztosításához.

Kulcsszavak*: Mesterséges intelligencia, gépi tanulás, algoritmus, tradicionális bankok, front/middle/back office*

JEL- kódok: C45, C80, G21, G32, O33

* Prisznyák Alexandra, PTE KTK Gazdálkodástani Doktori Iskola, PhD hallgató

I. Bevezető

A mesterséges intelligencia és gépi tanulás bankszektorban történő implementációja exponenciálisan nő, áthatva a tradicionális bankok front/middle/back office területeit. A Fintech, BigTech fenyegetettség árnyékában működő tradicionális bankok mesterséges intelligencia és kapcsolódó technológiák implementációja, fejlesztése és üzemeltetése elengedhetetlen a digitális éra fogyasztói társadalmában. A Fintech és BigTech vállalatok digitális technológiai megoldásai a nyújtott granuláris pénzügyi szolgáltatáson keresztül minden korábbinál magasabb fogyasztói élménynyújtáshoz vezetett (Alt és Puschmann, 2016).[9] A pénzügyi szolgáltatást nyújtó vállalatok mesterséges intelligencia és kapcsolódó technológiai felhasználási területei jellemzően az ügyfélminősítési, hitelelemzés és scoring, kereskedési tevékenység, ügyfélprofilok kialakítása, csalás detektálás (pénzmosás és terrorizmusfinanszírozás megakadályozása) és egyéb kockázatkezelés (működési, piaci, likviditási, hitelezési, modell validációs, egyebek), működés optimalizálás (tőkeoptimalizálás, költségcsökkentés, hatékonyságnövelés), megkülönböztető szolgáltatásnyújtás az ügyfélélmény fokozására és ennek eszközei: chatbotok, kereskedési tevékenység (portfólió) menedzselése.[10]

A digitális korszak hiperversenyében a BigTech, Fintech vállalatok fejlett adatgyűjtési és elemzési technológiája, pénzügyi szolgáltatásnyújtása jelentős kihívás elé állítja a tradicionális bankokat. Az egymással összeköttetésben lévő okoseszközök adatgenerálása jelentősen növekedett az elmúlt években, amely 2025-re egyes becslések alapján eléri a 175 zettabyte-ot.[11] A Fintech, BigTech vállalatok pénzügyi szolgáltatásokkal összefüggő tevékenysége jelentős nyomást gyakorol az inkumbens bankok digitális transzformációjának ütemére.

II. Tradicionális bankok, Fintech, BigTech

A bizalomra épülő bankszektor tradicionális piaci szereplői új versenytársakkal találták magukat szemben az elmúlt években. A fogyasztói társadalom fizetési szolgáltatási szokásaiban bekövetkező változása indukálta a bankok szervezeti változásának szükségességét.[12]

[9] Alt, R., – Puschmann, T., 2016: Digitalisierung der Finanzindustrie– Grundlagen der Fintech-Evolution. Springer Gabler, Berlin, Heidelberg. pp. 55-117., ISBN978-3-662-50541-0. https://doi.org/10.1007/978-3-662-50542-7.
[10] FSB, 2017: Artificial intelligence and machine learning in financial services Market developments and financial stability implications.https://www.fsb.org/wp-content/uploads/P011117.pdf
[11] McKinsey, 2020: Finance 2030: Four imperatives for the next decade. https://www.mckinsey.com/business-functions/operations/our-insights/finance-2030-four-imperatives-for-the-next-decade
[12] Liaw, T., 2021: The Routledge Handbook of Fintech. Abingdon, Oxon, New York, NY: Routledge, 2021. ISBN 9780429292903

A Fintech vállalatok által nyújtott hitelmodellek eredetileg decentralizált platformok köré szerveződtek, amelyek esetében az egyes hitelezők választják a hitelfelvevőket, illetve hitelezendő projektetek körét adott piaci keretek között. Az alkalmazott platformok segítenetek megoldani az aszimmetrikus információk problémáit a kiválasztási módszereik, alkalmazott technológiájuk és kockázatértékelési lehetőségeik révén. Ezzel megteremtve a kifinomultabb hitelezési modellek elterjedésnek alapjait.[13] A Fintech vállalatok a BigTech vállalatokhoz hasonlóan, szintén (jellemzően) magas automatizáltsági fokkal és agilis szoftver fejlesztési folyamatokkal rendelkeznek, amelyet globális ügyfélkiszolgáló tevékenységük által szolgáltatott adatalapú működés támogat. Buckley, Douglas és Barberis (2016)[14] alapján a tradicionális bankok számára versenyterületként az alábbi öt fő Fintech centrikus területet jelentkezik: (1) pénzügyi termékek értékesítés, befektetés és tőzsdei kereskedés, (2) operáció és azzal összefüggő kockázatkezelés, (3) fizetési rendszerek, (4) kiberbiztonság, (5) ügyfélkapcsolat és élménynyújtás.

A Fintech vállalatokkal szemben a BigTech vállalatok főtevékenysége jellemzően nem pénzügyi jellegű szolgáltatás nyújtására irányul, ugyanakkor üzleti modelljük a hálózati hatás (szolgáltatási platformok összefüggő hálózata) és technológia centrikusság (kutatás és fejlesztés) révén jelentős eltérést mutat a pénzügyi intézmények üzleti modelljétől. A BigTech vállalatok technológia érintettségű főtevekénységükből eredően jelentős (meglévő) ügyfél bázissal rendelkeznek, amelyre piaci létjogosultságuk és növekedési potenciáljuk nagymértékben visszavezethető.[15] A rendelkezésükre álló nagy méretű (BigData, BD) adatbázisok jellemzően nem kizárólag pénzügyi tevékenységre vonatkozó információt tartalmaznak, hanem jelentős mértékben építkeznek az ügyfélhez kapcsolódó egyéb „soft" adatok meglétéből, megteremtve ezáltal a lehetőséget a kizárólag ügyfél és tranzakciók banki adatokon alapuló tradicionális bankokkal szemben az információs aszimmetriából eredő torzítások enyhítésére, az ügyfélről alaposabb megismerésére. A tranzakciós és ügyféladatok mellett ezen „soft" jellegű adatok modellépítés során való felhasználása a korábbinál magasabb hozzáadott értékkel bíró, megbízhatóbb döntéstámogató rendszerek kialakulást eredményezi.

A BigTech, Fintech piaci feltörekvésének ugyanakkor megvannak a sajátos gátló tényezői. Az Európai Unió állampolgárai alapvető jogainak védelme, valamint a magánélet és személyes

[13] Jagtiani, J. Lemieux, C., 2019: The roles of alternative data and machine learning in Fintech lending: Evidence from the LendingClub consumer platform. In: Financial Management. Volume 48, Issue 4. pp. 1009-1029. https://doi.org/10.1111/fima.12295

[14] Buckley, R., Douglas, A., Barberis, J., 2016: The Evolution of Fintech: A New Post-Crisis Paradigm? In: Georgetown Journal of International Law. 47. pp. 1271-1319. http://dx.doi.org/10.2139/ssrn.2676553

[15] Bank for International Settlements, 2019: BigTech and the changing structure of financial intermediation (No. 779). https://www.bis.org/publ/ work779.pdf

adatok szigorú kezelése, továbbá az ezzel kapcsolatos etikus piaci magatartás kiemelt szabályozói oldali tényezőként jelentkezik az Európai Unióban. [16] [17] [18] Az Európai Unió összefüggésben a mesterséges intelligencia és gépi tanulás európai gazdaságra gyakorolt hatásával, több ízben is tárgyalja az AI, ML szabályozási lehetőségeit a tagállami szabályozások széttöredezettségének megakadályozása, valamint az Európai Unió koordinált mesterséges intelligencia stratégiájának biztosítása érdekében.[19] [20] Szorgalmazva ezáltal a mesterséges intelligencia, gépi tanulás, robotika és kapcsolódó digitális technológiákat érintő, bizalmat és kiválóságot támogató, stratégia és szabályozási keretrendszer kialakítását az adatalapú globális versenyben.

A Fintech, BigTech vállalatok előretörésének végeredményeképpen a BIS[21] az alábbi forgatókönyveket körvonalazza:

- Inkumbens piaci szereplők (tradicionális bankok) modernizációja és digitális átalakulása révén a korábbinál magasabb szolgáltatási színvonalat reprezentáló bankok létrejötte. A tradicionális bankok átalakulásának eredményeképpen a hagyományos banki tevékenység magas fogyasztói ügyfélélményt kínáló digitális ügyfélkiszolgálásra fókuszál. [22]
- Az internet és mobiltelefon alapú „neo" és (mobiltelefon alapú) „challanger" bankok ((például az Atom Bank, Monzo Bank (UK), Bunq (Hollandia), WeBank (China), Simple és Varo Money (US), N26 (Németország), Fidor (UK, Németország), Wanap (Argentína)) növekedése és a tradicionális bankok háttérbe szorulása.

[16] European Commission, 2018: Reform of EU data protection rules. https://ec.europa.eu/commission/sites/betapolitical/files/data-protection-factsheet-changes en.pdf.
[17] FRA, 2020: Getting the future right artificial intelligence and fundamental rights. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf
[18] FRA, CoE, 2018: Handbook on European non-discrimination law. 2018 edition, Luxembourg, Publications Office, June 2018, p. 35., https://fra.europa.eu/en/publication/2018/handbook-european-non-discrimination-law-2018-edition
[19] European Parliament, 2020: Artificial intelligence: how does it work, why does it matter, and what can we do about it? Online: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf
[20] Európai Bizottság, 2018: Coordinated Plan on Artificial Intelligence, COM (2018) 795. https://knowledge4policy.ec.europa.eu/publication/coordinated-plan-artificial-intelligence-com2018-795-final_en
[21] Bank for International Settlements, 2017: Sound Practices: Implications of Fintech developments for banks and bank supervisors., https://www.bis. org/bcbs/publ/d431.pdf
[22] Lu, L., 2017: Financial Technology and Challenger Banks in the UK: Gap Fillers or Real Challengers? In: Journal of International Banking Law and Regulation, 32(7), pp. 273–282.

- Banki tevékenység felosztása, fregmentációja a tradicionális banki szereplők és Fintech vállalatok között. Eredményeképpen innovatív fizetési szolgáltatások, robot-tanácsadók és hitelezési platformok térnyerése.
- Tradicionális bankok tevékenységi körének szűkítése és alvállalkozók szerződtetése a digitális technológián alapuló szolgáltatások magasszintű kiszolgálásának biztosítása érdekében.
- A kiszorított tradicionális bankok elhagyják a piacot.

A felvázolt forgatókönyvekhez kapcsolódóan megjegyzendő, hogy az ázsiai régióban már 2019-ben körvonalazódtak olyan megoldási javaslatok a pénzügyi szektort érintő digitális átalakulás menedzselése érdekében, amelyek digitális banki engedélyek kiterjesztését célozták a nem pénzügyi tevékenységet folytató vállalatokra. A Szingapúri Monetáris Hatóság (Monetary Authority of Singapore, MAS) 2019 június 28-án bejelentette a „teljeskörű digitális bank" (Digital Full Bank, DFB) illetve a „digitális kereskedelmi bank" (Digital Wholesales Bank, DWB) engedélyek bevezetést és azok meglévő digitális banki keretrendszerbe (Internet banking Framework) történő integrálását. Az említett új engedélyek bevezetése olyan ázsiai alapítási hellyel bíró technológiai cégek számára kívánja megteremteni a szabályozói kereteket, amelyek a pénzügyi szektort érintő technológiai megoldásuk révén jelentős szerepet vállalnak a tradicionális banki tevékenység reformációjában.[23] [24] Ösztönzve ezáltal a bankszektor tradicionális piaci szereplőinek digitalizációs korszak kihívásaihoz való felzárkózását.

A granuláris szolgáltatásnyújtással magas fogyasztói élményt nyújtó Fintech/BigTech megoldásokkal szemben védekező tradicionális bankok versenyképességük fenntartása érdekében a digitális pénzügyi szolgáltatások növelésének irányába fordultak. Az inkumbens tradicionális bankok digitális felzárkózást és versenyképességet célzó törekvései elsősorban a költségcsökkentést, hatékonyságnövelés, megkülönböztetést és fogyasztói élménynyújtás fokozása körül körvonalazódnak. A digitális éra transzformatív hatása működési folyamataik egészére hatással.[25][26] Ugyanakkor, a szervezet digitális képességeinek növelése a szervezeti kultúra átalakulását, a változásmenedzsment hatékonya menedzselését, valamint edukációs

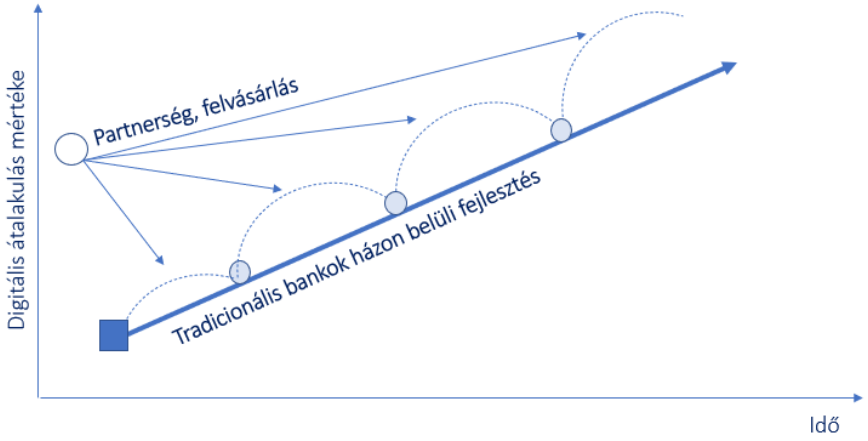
[23] Monetary Authority of Singapore, 2019: Digital full bank framework.Annex A., https://www.mas.gov.sg/-/media/Annex-A-Digital-Full-Bank-Framework.pdf

[24] Monetary Authority of Singapore, 2019: Eligibility criteria and requirements for digital banks. https://www.mas.gov.sg/-/media/Digital-Bank-Licence/Eligibility-Criteria-and-Requirements-for-Digital-Banks.pdf

[25] Alt, R., Beck, R., Smits, M. T., 2018: Fintech and the transformation of the financial industry. In: Electronic Markets, https://doi.org/10.1007/s12525-018-0310-9

26 Horváth Dóra, 2020: A Fintech-jelenség hagyományos kereskedelmi bankokra gyakorolt hatásának vizsgálata. In: Vezetéstudomány / Budapest Management Review lI. Évf. 2020. 09. Szám/ ISSN 0133-0179 https://doi.org/10.14267/VEZTUD. (2020.09.02)

kezdeményezéseket is szükségképpen maga után vonja. A tradicionális bankok digitális transzformációjának megvalósítási módját tekintve jellemzően négy stratégia különíthető el: (1) Fintech/BigTech vállalat felvásárlása (részesedés növelés) (2) partnerség kialakítása, (3) házon belüli (in-house) AI, ML megoldások fejlesztés, (4) hibrid stratégia: a felsorolt lehetőségek kombinációja révén[27], Schena és szerzőtársai,[28] amelyet az 1. ábra hivatott szemléltetni.



1.ábra: Tradicionális bankok digitális átalakulás stratégiái
Forrás: Saját ábra

Az Európai Bankhatóság[29] a Fintech/BigTech szolgáltatásnyújtás térnyerésével párhuzamosan hangsúlyozza a prudenciális kockázatelemzés és kapcsolódó innovatív lehetőségek kiaknázásának fontosságát. A digitális transzformációval járó új pénzügyi infrastruktúra előirányozza a meglévő szabályozás revízióját és a mesterséges intelligenciával összefüggő módosítások eszközölését, amely mögött a Fintech/Bigtech térnyerés következtében megjelenő új kockázatok jelentkeznek.[30] A Fintech/BigTech vállalatok piacra lépése számos módon járulhat hozzá a pénzügyi rendszer stabilitásával is összefüggő kockázat kialakulásához:

[27] Tanda, A., Schena, C., 2019: Introducing the Fintech Revolution. In: FinTech, BigTech and Banks. pp.1-5. 10.1007/978-3-030-22426-4_1.
[28] Schena, C., et al 2018: The development of Fintech. Opportunities and risks for the financial industry in the digital age. The Quaderni FinTech (FinTech Papers) Series. ISBN 9788894369755.
[29] European Banking Authority, 2020: EBA report on Big Data and Advanced analytics. https://www.eba.europa.eu/sites/default/documents/files/document_library/Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf
[30] World Economic Forum, 2016: The future of financial infrastructure An ambitious look at how blockchain can reshape financial services. https://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

- az inkumbens tradicionális bankok jövedelmezősége csökkenhet a piacra lépő Fintech/Bigtech vállalatok tevékenységének következtében.
- Az új piaci szereplők megjelenésével párhuzamosan jelentkező profitcsökkenésre a tradicionális bankok megnövekedett kockázatvállalási hajlandósággal reagálhatnak, ami
- a fokozott kockázatvállalás a prudenciális szabályozás szigorodásán keresztül elősegítheti az árnyékbanki tevékenység térnyerését.

A tradicionális bankok jellemzően nem alkalmaznak ügyféladatként a közösségi média különböző platformjain keresztül elérhető „puha (soft)" adatokat, amelyeket a Fintech/ BigTech vállalatok előszeretettel alkalmaznak. Vallee és Zeng[31] kimutatták, hogy a finanszírozott hitelek átvilágításakor információs előnyt jelent az ügyfélre vonatkozó szofisztikált információ használat. Az információ banki silókon túlmenő gyűjtése és alkalmazása a támogatott AI, ML modellek révén jelentősen növelheti az intézmények egyes banki folyamatokban nyújtott tevékenységét.

Az OECD [32] a Fintech és BigTech vállalatok térnyerésével kapcsolatosan a pénzügyi piacok működésében potenciálisan jelentkező zavarokra hívja fel a figyelmet. Az Európai Bankhatóság[33] kiemeli, hogy a mesterséges intelligenciával és kapcsolódó digitális megoldásokkal összefüggésben jelentkező kockázatok (adatvédelmi kérdések, IT és kiberbiztonság, versenyszabályozás, csalásmegelőzés egyebek) fontos jogszabályi megfelelőségi, működési, pénzügyi rendszerrel kapcsolatos kérdéseket vetnek fel. Az AI és ML alkalmazása olyan új és váratlan kockázatokat mozdíthatnak elő, amelyek megzavarhatják a pénzügyi piacok és pénzügyi intézmények harmonikus működését. Ezen kockázatok megfelelő szintű - így jogszabályok, ajánlások alkotása, vállalati szintű kezelése- elengedhetetlen.

Kiemelt területként jelentkezik a személyes adatok védelmét támogató Általános Adatvédelmi Rendelet (General Data Protection Regulation, GDPR) AI, ML keretek között történő sikeres menedzselése. Az Európai Unióban tevékenykedő vállalatok az Európai Parlament, Európai Bizottság és egyéb nemzetközi, hazai intézmények iránymutatásai, kötelező érvényű jogszabályai, rendeletei és egyéb ajánlásait szem előtt tartva szükséges, hogy

[31] Vallee, B., Zeng, Y., 2018: Marketplace Lending: A New Banking Paradigm? In: Review of Financial Studies, Volume 32, Issue 5, May 2019, pp. 1939–1982., https://doi.org/10.1093/rfs/hhy100

[32] OECD, 2020: Digital Disruption in Banking and its Impact on Competition http://www.oecd.org/daf/competition/digital-disruption-in-financial-markets.htm

[33] Bank for International Settlements, 2017: Sound Practices: Implications of Fintech developments for banks and bank supervisors. Online: https://www.bis. org/bcbs/publ/d431.pdf

kialakítsák digitális működésük alapjait – biztosítva az Európai Unió állampolgárainak magánéletéhez és személyes adataihoz kötődő adatok védelmét.

A mesterséges intelligenciát érintő nemzetközi és hazai szintű szabályozás stratégiai fontosságú versenypiaci kérdéseket is felvet. Különösen érdekes e tekintetben a mesterséges intelligencia alapú nemzetközi verseny intenzitásának fokozódása és az adott térségek (USA, Ázsia, EU) jogi keretrendszerének összevetése, az adatkezelés szabályozásának mértéke.

III. Banki front/middle/back office AI, ML alkalmazása

A banki front/middle/back office területeken a mesterséges intelligencia, gépi tanulás eltérő üzleti és IT célú megfontolásokkal társulva járul hozzá a szervezet működés hatékonnyá tételéhez. Az alábbiakban néhány kiemelt terület áttekintése következik.

1. Marketing

Az értékesítés támogatása számos alterületen keresztül valósulhat meg, így az jellemzően túlmutat a fizetési szolgáltatások és kapcsolódó modernizációján. A front office területhez kapcsolódó marketing és fogyasztói kapcsolatok menedzselése (Customer Relationship Management, CRM) területeken jellemzően az alábbi mesterséges intelligencia megoldások alkalmazása figyelhető meg: CRM stratégiák, churn ráta előrejelzés, beavatkozási akciótervek, ajánlatok készítése (virtuális ügynök), chatboot, természetes nyelvek feldolgozása (Natural Language Processing, NLP), valós idejű tranzakció menedzsment, ügyfélcsoport kialakítása, keresztértékesítési stratégiák meghatározása és támogatása, biometrikus azonosítás, humanoid robotok (ügyféltérben), ügyfélazonosítás, dokumentum strukturálatlan adatainak értelmezése, felhasználása gépi tanulási modellek révén, cybersecurity, csalásmegelőzés, egyebek.

2. Portfólió- és vagyonkezelés

A gépi tanulás alkalmas tőzsdei árfolyamok előrejelzésére, részvényportfólió kezelésre, trend előrejelzésre, így hozzájárul a részvénypiaci kockázatok minimalizálásához. Sudeepa és társai[34] véletlen erdő (Random Forest, RF) modell segítségével olyan modellt fejlesztettek, amelyek a részvények várható hosszú távú hozamát ML algoritmusok együttes tanulás (*ensemble learning*) révén jelzik előre.

További alkalmazási területként jelentkezik a befektetési tevékenység, illetve vagyongazdálkodás. A vagyongazdálkodás területén is terjedőben vannak a robot tanácsadók (Robot Advisor, RA), amelyek a modern portfólióelméletet alapul véve hozzájárulnak a

[34] Sudeepa R. D., et al., 2016: Predicting the direction of stock market prices using random forest." In: The North American Journal of Economics and Finance Volume 47, January 2019, pp. 552-567., https://doi.org/10.1016/j.najef.2018.06.013

portfólió optimalizáláshoz és eszközallokációhoz.[35] Beketov, Lehmann és Wittke[36] több, mint kétszáz robot tanácsadót elemezve kimutatták, hogy a robot tanácsadók által kezelt eszközállomány volumene magasabb az újabb és szofisztikáltabb rendszereken alapulva. Bartram, Branke, Motahari [37] a vagyonkezelés területet elemezve felhívja a figyelmet arra, hogy bizonyos kiugró események, anomáliák (például fekete hattyú jelenség) az irreleváns minták, összefügések feltárásán keresztül torzíthatják a ML modellt.

3. Tőzsdei árfolyam előrejelzés

Jasic és Wood[38] a nyereséges tőzsdei kereskedés támogatása érdekében a tőzsdeindex-hozamok előrejelzésére egyváltozós neurális hálózatot fejlesztett ki, amelyhez több globális részvénypiac historikus (1965-1999) adataira támaszkodtak. A mesterséges neurális hálózat teljesítményének értékelése során a neurális háló prognosztizáló képességét egy benchmarkként funkcionáló lineáris autoregresszív modellhez viszonyították. Megállapították, hogy a modell előrejelzési képessége javult az S&P500 és DAX indexek vonatkozásában. Chong, Han, Park[39] a tőzsde elemzéséhez és előrejelzéshez mélytanulási (Deep learning, DL) technikát alkalmaz. Rouf és társai[40] részvények értékesítésével összefüggésben a részvényárfolyam (ár-és tőzsdeindex értékek) előrejelzésére alkalmazott ML algoritmusok alkalmazásának lehetőségei vizsgálta. Elemzése keretében az alábbi algoritmusok hatékonyságát, eredményességét elemezte: tartóvektor-gép modell (SVM), lineáris regresszió, véletlen erdő modell, valamint egyes mélytanulás technikákat, mint az mesterséges neurális hálózatok (Artificial Neural Networks, ANN), illetve ismétlődő neurális hálózatok (Recurrent Neural Networks). Strader és szerzőtársai[41] a ML tőzsdei előrejelzés készítésével kapcsolatosan kimutatták, hogy a mesterséges neurális hálózatok használata alkalmas a terület teljesítményének növelésére.

[35] Marchinares, A., Alonso, I.A., 2020: Project Portfolio Management Studies Based on Machine Learning and Critical Success Factors. In: 2020 IEEE International Conference on Progress in Informatics and Computing (PIC)369-374. https://doi.org/10.1109/PIC50277.2020.9350787

[36] Beketov, M., Lehmann, K. és Wittke, M., 2018: Robo Advisors: quantitative methods inside the robots. In: Journal of Asset Management 19 (2018): pp. 363-370., http://doi.org/10.1057/s41260-018-0092-9

[37] Bartram, S. M., Branke, J., Motahari, M., 2020: Artificial intelligence in asset management. In: CFA Institute Research Foundation Literature Reviews, August 2020. ISBN 978-1-952927-02-7.

[38] Jasic, T., Wood, D., 2004: The profitability of daily stock market indices trades based on neural network predictions: case study for the S&P 500, the DAX, the TOPIX and the FTSE in the period 1965-1999. In: Applied Financial Economics, 2004, vol. 14, issue 4, pp. 285-297., https://doi.org/10.1080/0960310042000201228

[39] Chong, E., Chulwoo, H., Chongwoo, F. P., 2017: Deep learning networks for stock market analysis and prediction: Methodology, data representations, and case studies. In: Expert System with Applications. 83: 187-205. https://doi.org/10.1016/j.eswa.2017.04.30

[40] Rouf, N., et al, 2021: Stock Market Prediction Using Machine Learning Techniques: A Decade Survey on Methodologies, Recent Developments, and Future Directions. In: Electronics 2021, 10, 2717. https://doi.org/10.3390/ electronics10212717

[41] Strader, T.J., et al, 2020: Machine Learning Stock Market Prediction Studies: Review and Research Directions. In: Journal of International Technology and Information Management. Volume 28, Issue 4, article 3. pp. 63–83. https://scholarworks.lib.csusb.edu

Hagenau, Liebmann és Neumann[42] az automatizált hírolvasáson alapuló részvényárfolyam-előrejelzést vizsgálták kontextust elemző funkciók alkalmazásával, illetve szövegbányászati módszerek (szöveg ábrázolás, szemantikailag releváns attribútumok és piaci visszajelzés beépítése) segítségével. A modelljük továbbfejlesztése növelte az osztályozási pontosságot, illetve a csökkentette a túlillesztés problémáját.

4. Hitelezési folyamatok

A mesterséges intelligencia hitelezési folyamatban számos területet támogathat humán, illetve virtuális hitelügyintézők révén. A ML modellek a hitelezési folyamat legfőbb tevékenységeihez hozzájárulva csökkentik a kihelyezett hitelek visszafizetés nem fizetésének kockázatát: scoring rendszerek, hitelelemzés, ügyfélminősítés, ügyfélprofil kialakítás, biztosítékok, jelzálogkezelés. Gambacorta és szerzőtársai[43] a banki hitelminősítő rendszereket vizsgálva megállapították, hogy a gépi tanulási technikákkal támogatott rendszerek pontosabb előrejelzési képességet biztosítanak a menedzsment számára. Nica és szerzőtársai[44] a ML technikák használatával támogatott jelzálogkezelés területén alkalmazott kliens profilok automatikus értékelési modelljét és annak előnyeit elemezte. A banki ügyfelek hitelképességének vizsgálatára épített modellt Aniceto, Barboza és Kimura[45] a nemteljesítés/teljesítés valószínűségének előrejelzésére a hitelkockázat menedzselésének elősegítése érdekében.

5. Compliance

A kliensek onboardingjának elősegítését a mesterséges intelligencia e-KYC, AML/video alapú KYC, AML megoldásai segítik elő, amelyek lehetővé teszik, hogy a jogszabályok által előírt, új ügyfelekhez kapcsolódó szükséges adatfelvétel korábbinál rövidebb időn belül valósuljon meg.[46] A Compliance területeken alkalmazott mesterséges intelligencia, gépi tanulás

[42] Hagenau, M., Liebmann, M., Neumann, D., 2013: Automated news reading: Stock price prediction based on financial news using context-capturing features, In: Decision Support Systems, Volume 55, Issue 3, pp. 685-697, ISSN 0167-9236, https://doi.org/10.1016/j.dss.2013.02.006.

[43] Gambacorta, L., et al., 2020: Data vs collateral. BIS Working Papers No 881. ISSN 1682-7678 (online). https://www.bis.org/publ/work881.pdf

[44] Nica, I., et al, 2021: Automated Valuation Modelling: Analysing Mortgage Behavioural Life Profile Models Using Machine Learning Techniques, In: Sustainability, MDPI, Open Access Journal, vol. 13(9), pp. 1-27. https://doi.org/10.3390/su13095162

[45] Aniceto, M., Barboza, F., Kimura, H., 2020: Machine learning predictivity applied to consumer creditworthiness. In: Future Business Journal. 6., Article: 3 to et al. Futur Bus J 2020, 6(1):37, https://doi.org/10.1186/s43093-020-00041-w

[46] Infosys Ltd, 2020: Being Resilent. Transforming customer onboarding with AI. https://www.infosys.com/industries/financial-services/insights/documents/transforming-customer-onboarding-ai.pdf

és kapcsolódó technológiákat vizsgálja továbbá van Wegberg és társai[47], valamint Johari és társai.[48]

A pénzügyi intézményekkel kapcsolatos ML megoldásokat vizsgálta van Liebergen[49], a normál tekintetben vett kereskedői magatartás, teljesítménytől való eltérés alapján. A ML algoritmusok alkalmazásának egyik fontos kérdése a tanulási módszer típusa és az elérhető adatok minősége, teljessége, címkézése.

6. Pénzmosás és terrorizmusfinanszírozás megakadályozása, csalásmegelőzés

A globális pénzügyi válságot követően a bankok kockázatkezelése kiemelt hangsúlyt kap, mind a tudományos életben, mind a gyakorlatban. Párhuzamosan a banki kockázatkezelési szabályozás szigorodásával a mesterséges intelligencia és gépi tanulás növekvő hatást gyakorol az üzleti folyamatok front/middle/back office területein. A banki kockázati modellezéssel (stressztesztelő modellek, tőkekövetelmények) és egyéb kockázatkezelési tevékenységgel összefüggésében alkotott AI, ML modellek, így: a hitelezési, működési, likviditási, működési kockázatok kezelésében betöltött szerepe exponenciálisan nő. A kockázatkezelés back office területének egy másik aspektusa a pénzügyi bűncselekmények megelőzése a mesterséges intelligencia segítségével. A mesterséges intelligencia és gépi tanulás alkalmazásának exponenciálisan fejlődő területe a pénzmosás megakadályozása (Anti-Money Laundering, AML), terrorizmusfinanszírozás megelőzése (Counter Terrorism Financing, CFT) és csalásmegelőzési területek. Drezewski és szerzőtársai[50] elemzés során meghatározott jellemzők alapján klasztereket alakítottak ki az ügyfél tranzakciós viselkedésének önmaga historikus adatain nyugvó viselkedésmintájával, illetve egyéb - hasonló tulajdonságokkal rendelkező - ügyfelek csoportjával. Luo [51] osztályozáson alapuló algoritmust javasol a pénzügyi tranzakciók elemzésére és a gyanús tranzakciós ügyletek felderítésére. Patil, Dharwadkar[52] felügyelt

[47] van Wegberg, R., Oerlemans, J. J., van Devente, O., 2018: Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. In: Journal of Financial Crime, 25(2): pp. 419–435., http://doi.org/10.1108/JFC-11-2016-0067

[48] Johari, R. J., et al., 2020: Money Laundering: Customer Due Diligence in the Era of Cryptocurrencies. In: AEBMR, Volume: 123., https://doi.org/10.2991/aebmr.k.200305.033

[49] van Liebergen, B., 2017: Machine Learning: A Revolution in Risk Management and Compliance? In: Journal of financial transformation 45, pp. 60-67.

[50] Drezewski, R., Sepielak, J., Filipkowski, W., 2012: System supporting money laundering detection, Digital Investigation, Volume 9, Issue 1, 2012, pp. 8-21., https://doi.org/10.1016/j.diin.2012.04.003.

[51] Luo, X., 2014: Suspicious Transaction Detection for Anti-Money Laundering. International Journal of Security and Its Applications Vol.8, No.2 (2014), pp.157-166., http://dx.doi.org/10.14257/ijsia.2014.8.2.16

[52] Patil, P. S., Dharwadkar, N. V., 2017: Analysis of banking data using machine learning. International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp. 876-881., http://doi.org/10.1109/I-SMAC.2017.8058305.

mesterséges neurális hálózat algoritmust alkalmaztak osztályozási célokra ügyfélmegtartás és csalásfelderítési célokra.

Az elosztott főkönyvi technológia (Distributed Ledger Technology, DLT) egy olyan tranzakciós adatbázis, amely egy dedikált központi helyen való tárolás helyett több számítógépből álló hálózaton oszlik el. Leggyakrabban előforduló formája a blokklánc (blockchain), amelyben a tranzakciók csoportonként (blokkonként) kronologikus sorrendben egymáshoz kapcsolódva egy láncot képzenek. Az innovatív blocklánc (blockchain) technológia pénzügyi szektorba történő implementálását elemzi Qamruzzaman.[53] A szakirodalom ML algoritmusok AML és CFT területen való alkalmazásának elemzésén túlmenően, a szerző felméri a DLT technológia alkalmazási lehetőségeit és javaslatot tesz egy neurális hálózat alapú modell készítésére az illegális jövedelem felhasználásának kiszűrése érdekében. A blockchain a bankszektorban meglévő bizalmas információk nyújtásának, tárolásának, a tranzakcióban résztvevők anonimitásának biztosítására alkalmazott hatékony eszköznek tekinthető. A pénzmosás és terrorizmus finanszírozás megakadályozásának területeként jelentkezik a digitális valutákkal összefüggő tranzakciók elemzése is.

7. Kockázatkezelés –modell validáció, visszamérés, revízió

A gépi tanulási modellek a hitelezési, működési, likviditási kockázatkezelésen túlmenően fontos szerepet töltenek be a készített modellek ellenőrzésében, tűréshatárainak tesztelésében, optimalizálásában. Szerepük a stressz forgatókönyvek, szcenáriók validációjában, tőkeoptimalizálásban, automatizált rendszerek (hiteljóváhagyás, portfólió kezelés) működésének elősegítésében jelentős hatékonyság növekedést jelenthetnek.

8. Bankbiztonság

A mesterséges intelligencia a biztonságos banki működést számos területen, így többek között az ügyfélazonosítása során is támogatja. Alkalmazott módszerek az ügyfelek azonosítása során olyan technológiákat is magukba foglalnak, amelyek képesek biometria alapján arc/mikró kifejezések elemzésére, azonosítására, hang, video és képelemzés támogatására, illetve ezen adatforrásokból strukturáltalan adatok kinyerését és NoSQL alapú feldolgozását is támogatják.

[53] Qamruzzaman, M., 2021: Blockchain Technology -A Catalyst for Innovativeness: Recent Literature Survey. In: International Journal of Management. 12(2):355-373., http://doi.org/10.34218/IJM.12.2.2021.036

9. Emberi erőforrás menedzsment

A szervezetek digitális transzformációjának kiemelkedő eleme a munkavállalók képességeinek bővítése a digitalizáció által megkövetelt technológiai képességek körével.[54] A mesterséges intelligencia és kapcsolódó technológiák átalakítják a munkaerőállomány megújításának (toborzás, kiválasztás, képzés) módjait és ezzel párhuzamosan a munkavállalók szervezet iránti elköteleződését és termelékenységét is fokozhatják.[55] Az AI-alapú rendszerek a humán erőforrás menedzsmentet (Human Resource Management, továbbiakban HRM) elsősorban a döntéstámogatási, előrejelzés, munkaerő tervezés tevékenységben támogatják. Chaudhuri[56], Donepudi[57] felhívja a figyelmet a ML toborzásban és a kiválasztási folyamatban, teljesítményértékelésben, kompenzáció menedzsmentben betöltött szerepére. A mesterséges intelligencia alapú technológiai közvetlen HRM megoldások alkalmazása révén hozzájárul a toborzási költségek és időszükséglet csökkentéséhez. Közvetett módon – a munkafolyamatba ágyazva - a munkavállalói leterheltség csökkentéséhez, továbbá a monotonitás és frusztráció redukálásához. Eredményképpen hozzájárul a fluktuáció csökkenéséhez, a minőség növekedéséhez (az operáció során jelentkező hiba csökkentésén keresztül). A mesterséges intelligencia alapú rendszerek és ML algoritmusok az önéletrajzok áttekintése, értékelése és szűrése révén segíthetik a kiválasztási folyamatot és a megfelelő jelöltek kiválasztását. A kiválasztási folyamatban a videóinterjúk során történő alkalmazása és a megfelelő jelölt jelfelismerésen alapuló kiválasztása jelenthet előnyt a HR munkatársak számára.[58]

A munkavállalók teljesítményértékelése során gyűjtött adatok elemzése révén a gépi tanulás hozzájárulhat az adott munkavállaló teljesítménye mögött meghúzódó indikátorok feltérképezéséhez és kijelölheti a fejlesztendő kompetenciák körét. A munkavállalók képzése (training) során a mesterséges intelligencia egyéb megoldásai nyújthatnak segítséget, mint például a virtuális valóság (VR), illetve a kiterjesztett valóság (AR). Kiegészítésképpen az AI-

[54] Jaiswal, A., Arun, C. J., Varma, A., 2021: Rebooting employees: upskilling for artificial intelligence in multinational corporations, In: The International Journal of Human Resource Management, https://doi.org/10.1080/09585192.2021.1891114

[55] Vasantham, T., S., 2021: The Role of Artificial Intelligence in Human Research Management. In: Engineering and Scientific International Journal (ESIJ). Volume 8, Issue 2, April-June 2021. pp. 499-509. http://doi.org/10.30726/esij/v8.i2.2021.82013

[56] Chaudhuri, K., Varma, A., Malik, A., 2020: Artificial Intelligence as an antidote for managing people in organizations: How realistic? In: British Academy of Management Conference.

[57] Donepudi, P. K., 2017: AI and Machine Learning in Banking: A Systematic Literature Review. In: Asian Journal of Applied Science and Engineering, 6(3), pp. 157–162. http://doi.org/10.5281/zenodo.4109672

[58] Ahmed, O., 2018: Artificial Intelligence in HR. In: IJRAR december, Volume 5, Issue 4. pp. 971-978., https://www.ijrar.org/papers/IJRAR1944797.pdf

alapú coaching eszközök új perspektívákat jelenthetnek, mind a HR szakértők, mind a munkavállalók részére.

A tradicionális bankok front/middle/back office területek során alkalmazott AI, ML megoldásokat, valamint a (feldolgozott) kapcsolódó kutatásokat szemlélteti az 1. Táblázat.

1. **táblázat: Banki front/middle/back office területek tipikus AI és ML alkalmazási módjai**

	FRONT OFFICE	MIDDLE OFFICE	BACK OFFICE
Banki terület	Marketing & CRM Értékesítés • Befektetési tevékenység • Tőzsdei kereskedés • Portfólió és vagyonkezelés • Hitelezés • Számlavezetés és fizetés kezdeményezés • Termék tanácsadás Treasury (pénzügyi termékek tanácsadása ügyfeleknek)	Operáció Kockázatkezelés • Hitelelemzés, • Scoring tevékenység, • Ügyfélminősítés, • Ügyfél profil kialakítás	Kockázatkezelés • Terrorizmusfinanszírozás és pénzmosás megakadályozása, Csalásmegelőzés • Compliance (KYI, KYC) • Modell validáció (Scoring hitelkockázati modellek; Stressz teszt) és egyéb banki kockázatok menedzselése (hitelezési, működési, likviditási, piaci, egyebek) Emberi erőforrás menedzsment IT& Bankbiztonság Data management Ügyfélszolgálat Továbbá: Treasury (saját pozíciók zárása); Pénzügy, Kontrolling, Belső audit, Követeléskezelés; Számlavezetés; Fizetési rendszerek, Számlaforgalom (betéti, központi számla, egyebek); Jogi részleg; Projektmenedzsment (belső folyamatok); K+F, Termékfejlesztés
Alkalmazott AI, ML	CRM stratégiák, churn ráta előrejelzés, beavatkozási akciótervek, ajánlatok, chatboot, NLP, ügyfélkezelés, valós idejű tranzakció management, ügyfélcsoport kialakítása, azonosítása, elérési stratégiák meghatározása, biometrikus azonosítás, humanoid robotok (ügyféltérben), erős ügyfél identifikáció, dokumentum szkennelés, cybersecurity, csalásmegelőzés	kockázatértékelés, kockázati besorolás, rating, ügyfél profilok kialakítása, pontosabb előrejelzés készítése	Csalásminták feltérképezése, ügyfélprofil kialakítás, gyanús ügyfelek és tranzakciók azonosítása, Fals pozitív találatok csökkentése, illetve ezen gyanús tranzakciókra fordított idő és költségminimalizálás, threshold küszöbök finomítása, monitoring és jelző rendszerek (Compliance, AML) fejlesztése, pénzügyi bűncselekményeknek való kitettség kockázatának csökkentése, anomália észlelés, kibertámadások megelőzése,
Felhasznált szakirodalom	Khaidem, Saha, Dey (2016), Marchinares és Alonso (2020), Beketov, Lehmann, Wittke (2018), Bartram, Branke, Motahari (2020), Jasic és Wood (2004), Chong, Han, Park (2017), Rouf és társai (2021), Strader és szerzőtársai (2020), Haenau, Liebmann, Neumann (2013)	Gambacorta és szerzőtársai (2020), Nica és szerzőtársai (2021), Aniceto, Barboza, Kimura (2020)	Aggarwal és szerzőtársai (2020), Wegberg és társai, 2018; Johari és társai, 2020, Chen és társai (2018), Kannan és Srinath (2017), Kerimov és társai (2020), (B. van Liebergen, 2017), Donepudi (2017), Wislow, (2017), Donepudi (2017), Chaudhuri (2020), Jaiswal, Arun, Varma (2020), Drezewski, R., Sepielak, J., Filipkowski, W. (2012), Luo, X. (2014), Patil, P. S., Dharwadkar, N. V. (2017)

Forrás: Szerző saját táblázat

10. Konklúzió

Jelen tanulmány a mesterséges intelligencia és gépi tanulás banki front/middle/ back office területeken betöltött szerepét tárgyalja. Ennek keretében a gépi tanulás felhasználási, alkalmazási lehetőségeit az alábbi aspektusokból ismerteti: marketing, portfólió- és vagyonkezelés, tőzsdei árfolyam előrejelzés, hitelezési folyamatok, banki kockázatkezelés – modell validáció, visszamérés, revízió, bankbiztonság–, compliance, pénzmosás és terrorizmusfinanszírozás megakadályozása, csalásmegelőzés, emberi erőforrás menedzsment. Az áttekintést követően nyilvánvalóvá válik, hogy a front office területeken megvalósuló mesterséges intelligencia és gépi tanulás módszerek elsősorban az értékesítési és marketing tevékenység támogatását szolgálják, míg a middle office területen a kockázat elemzésben (hitelelemzés, ügyfélminősítés) van szerepe. A back office területre is átnyúló kockázatkezelés elsősorban a pénzügyi bűncselekmények megelőzése, illetve Compliance területeket támogatja, ugyanakkor a banki kockázatkezelés egyéb területeit is támogatja (hitelezési, működési, likviditási, piaci és egyéb kockázatok és kapcsolódó modell validációs feladatok). Szerepe jelentős ütemben nő a pénzmosás és terrorizmus finanszírozás elleni harcban, valamint a csalásmegelőzés, illetve a jogszabályi megfelelőséget támogató Compliance területeken, mint például az *„Ismerd meg az ügyfeled!”* (KYC), illetve *„Ismerd meg a közvetítőd!”* (KYI) tevékenységben.

11. Limitációk

A téma szakirodalmi kutatások áttekintésén keresztül vizsgálja a banki front/middle, illetve a *back office* területeivel összefüggő mesterséges intelligencia és gépi tanulás alkalmazásának módjait. A magyarországi tradicionális bankok bevonásán keresztül megvalósuló visszamérés eredménye a jövőben kerülhet publikálásra.

Projics Nárcisz*: A polgári peres eljárás a digitalizáció világában

Absztrakt:

Az elektronikus technológia gyors fejlődése és az elektronikus eszközök egyre nagyobb térnyerése jelentős hatást gyakorolt a polgári peres eljárásra, ezért indokolt annak vizsgálata, hogy az elektronikus ügyintézés és az elektronikus technológia alkalmazása hogyan jelenik meg a polgári perben. A polgári perrendtartásról szóló 2016. évi CXXX. törvénynek (a továbbiakban: Pp.) a technikai vívmányok következtében számos változásra kellett reagálnia, már a Pp. Koncepciójában a szabályozási célok és elvek között nevesítve szerepelt az „elektronizáció szerepének erősítése". Jelen tanulmány az elektronikus kapcsolattartás és az elektronikus hírközlő hálózat igénybevételének alapvető szabályait és egyes gyakorlati kérdéseit kívánja bemutatni, valamint rövid áttekintést kíván nyújtani a vizsgált tárgykörhöz kapcsolódó, veszélyhelyzet idején alkalmazandó szabályokról. Továbbá bemutatásra kerülnek az illeték megfizetésének lehetséges módjai elektronikus kapcsolattartás esetén és az ezzel kapcsolatos szabályok. Az elektronikus út vizsgálata során a Pp. szabályai mellett az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény kapcsolódó rendelkezéseit is górcső alá kell venni, mivel az elektronikus kapcsolattartást szabályozó joganyagot elsősorban e jogszabály határozza meg.

Kulcsszavak: *elektronikus ügyintézés, kapcsolattartás, polgári per*

I. Bevezető gondolatok

A technológiai fejlődés figyelemre méltó hatást gyakorolt mind a polgári peres eljárásra, mind pedig egyes polgári nemperes eljárásokra. Ezért indokolt az elektronikus ügyintézési mód és az elektronikus eszközök alkalmazásának vizsgálata a polgári perben. A polgári perjog, ezen belül a polgári perrendtartásról szóló 1952. évi III. törvény felülvizsgálatát elrendelő, a polgári perjogi kodifikációról szóló 1267/2013. (V. 17.) Korm. határozatban a felülvizsgálat célkitűzései között szerepelt a technikai vívmányokat figyelembe vevő szabályozás megteremtése. A polgári perrendtartásról szóló 2016. évi CXXX. törvénynek .) a technikai vívmányok következtében e területen is számos változásra kellett reagálnia, amely nagy kihívást jelent a jogalkotó számára. A Pp. 2015 januárjában elfogadott Koncepciója tizenhat pontban nevesítette azokat a szempontokat, illetve szabályozási célokat, amelyek mentén

* Dr. Projics Nárcisz, PTE ÁJK Büntető és Polgári Eljárásjogi Tanszék, PhD hallgató

kialakításra kerültek a törvény rendelkezései, ezek között szerepelt az „*elektronizáció szerepének erősítése*”.[1]

Fontosnak tartom megjegyezni, hogy az elektronikus kapcsolattartás 2013. január 1. óta biztosított a törvényszék előtti eljárásokban, valamint 2015. január 1. óta már valamennyi bíróságon. Azonban az elektronikus út, mint lehetőség adott volt a jogalkalmazók számára és nem kötelezettséget rótt rájuk.[2]

Két fő területen vizsgálható a digitalizáció hatása a polgári perben. Az egyik témakör az elektronikus kapcsolattartás, illetve az elektronikus úton történő eljárás. A vizsgált tárgykörhöz kapcsolódóan főként egyes gyakorlati kérdéseket, valamint problémás eljárási cselekményeket kívánok bemutatni. A másik terület a meghallgatáshoz és a bizonyítás-felvételhez kapcsolódó, a koronavírus járvány, illetve a veszélyhelyzet miatt jelentős szerephez jutó, a tárgyalások megtartásánál előtérbe kerülő, elektronikus hírközlő hálózat igénybevétele.

A Pp. Tizedik Részében „*Az elektronikus technológiák és eszközök alkalmazása*” cím alatt rendelkezik az elektronikus kapcsolattartásról, annak szabályairól és az elektronikus hírközlő hálózat útján történő meghallgatásról.

II. Elektronikus kapcsolattartás

1. Bírósággal történő kapcsolattartás a polgári perben

A polgári perben a feleket kapcsolattartási mód szempontjából alapvetően két csoportra tudjuk osztani; vannak az elektronikus kapcsolattartásra kötelezettek és az elektronikus kapcsolattartásra nem kötelezettek. Tehát a polgári perben nem minden fél köteles elektronikus úton tartani a kapcsolatot a bírósággal. Az elektronikus kapcsolattartásra kötelezettek körét az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (a továbbiakban: E-ügyintézési tv.) határozza meg, ennek alapján elektronikus ügyintézésre köteles az ügyfélként eljáró gazdálkodó szervezet, állam, önkormányzat, költségvetési szerv, ügyész, jegyző, köztestület, egyéb közigazgatási hatóság, valamint az ügyfél jogi képviselője.[3] Aki nem köteles elektronikus kapcsolattartásra, választhatja az elektronikus úton történő eljárást.[4]

[1] Wopera Zsuzsa (szerk.), 2019: Kommentár a polgári perrendtartáshoz. Kommentár a polgári perrendtartásról szóló 2016. évi CXXX. törvényhez. Budapest, Wolters Kluwer Hungary Kft., p. 22.
[2] Grébecz Kristóf Balázs, 2017: Az elektronikus kapcsolattartás szabályai egyes bírósági eljárásokban. In: Adóvilág. 5. szám p. 37.
[3] E-ügyintézési tv. 9. §
[4] Pp. 605. § (1) bek.

2. Az elektronikus kapcsolattartás alapjai

A Pp. 604. §-a utaló szabályt alkalmaz, amely alapján elektronikus kapcsolattartás során a Pp. valamennyi szabályát alkalmazni kell, hacsak a XLVI. Fejezet[5] eltérően nem rendelkezik. Azonban a Pp. azon szabályait nem kell alkalmazni, amelyeket az E-ügyintézési tv. rendez. Az elektronikus út vizsgálata során tehát a Pp. szabályai mellett más jogszabályokra is figyelemmel kell lenni, ilyen az elektronikus kapcsolattartást szabályozó joganyagot elsősorban meghatározó E-ügyintézési tv., amelynek kapcsolódó rendelkezéseit mindenképp górcső alá kell venni. Továbbá a vizsgálódás során tekintettel kell lenni az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendeletre, valamint a bírósági ügyvitel szabályairól szóló 14/2002. (VIII. 1.) IM rendeletre.

3. Választható elektronikus kapcsolattartás

Akik nem kötelesek elektronikus ügyintézésre, választhatják az elektronikus úton történő eljárást, amely számukra egy lehetőség. Fontos leszögezni, hogy kapcsolattartás szempontjából lehetnek vegyes eljárások, mivel az elektronikus kommunikáció mellett a hagyományos, papír alapú eljárás is jelen van a polgári perben. Az elektronikus úton történő kapcsolattartásra vonatkozó bejelentés az eljárás bármely szakaszában megtehető az eljáró bíróságnál, valamint a beadvány elektronikus úton történő benyújtása is az elektronikus út vállalásának minősül. Elektronikus kapcsolattartás választása esetén a fél vagy képviselője köteles elektronikus úton tartani a kapcsolatot a bírósággal és a bíróság is minden iratot elektronikusan küld meg részére az eljárás egész folyamán, kivéve a tárgyaláson csatolt vagy kézbesíthető iratot, illetve határozatot. Amennyiben rendkívüli perorvoslatra kerül sor, arra is kiterjed az elektronikus út vállalásának hatálya. Amennyiben az elektronikus kapcsolattartásra nem kötelezett fél nem vállalja az ily módon történő kapcsolattartást és a másik fél számára az kötelező vagy vállalta, a papír alapú okiratot benyújtó fél beadványait digitalizálja a bíróság és elektronikusan kézbesíti a másik fél részére.[6]

A választható elektronikus kapcsolattartással összefüggésben a Civilisztikai Kollégiumvezetők Országos Tanácskozása (a továbbiakban: CKOT) azzal a kérdéssel foglalkozott, hogy a rendelkezési nyilvántartást (RNY-t) elegendő-e a keresetlevél beérkezésekor lekérdezni vagy azt minden kiadás előtt meg kell-e nézni. A CKOT állásfoglalásában rögzítette, hogy minden hivatalos kézbesítés előtt le kell kérdezni a nyilvántartás (RNY) adatait. Azonban az RNY-ben lévő meghatalmazás esetén a félnek

[5] XLVI. Fejezet: „*Az elektronikus kapcsolattartás*”
[6] Pp. 605. §

(képviselőjének) kell hivatkoznia arra, hogy az RNY-ben meghatalmazása van, és ezért nem kerül(t) sor annak csatolására. A Pp. ugyanis kimondja[7], hogy a per folyamán adott vagy módosított, az RNY-ben szereplő meghatalmazás a bírósággal szemben csak annak bejelentésétől hatályos.[8]

4. Papír alapú kapcsolattartásra történő áttérés

Annak a félnek, akinek a bírósággal történő elektronikus kapcsolattartása vállaláson alapszik, lehetősége van papír alapú kapcsolattartásra áttérni. A fél, aki vállalta az elektronikus kapcsolattartást utóbb kérelmezheti a papír alapú eljárásra történő áttérés engedélyezését. A kérelemben valószínűsíteni kell, hogy a körülményeiben olyan változás következett be, ami miatt a továbbiakban aránytalan megterheléssel járna az ily módon történő kapcsolattartás.[9] A körülmények változását elegendő valószínűsíteni, amelyekre hivatkozva az áttérést kérelmezi. Ezzel kapcsolatban felmerül a kérdés, hogy a bíróság mely változásokat fog olyannak tekinteni, amelyek a papír alapú eljárásra történő áttérést indokolják.[10] E körben a Kúria egyik állásfoglalását emelem ki, amely szerint alaptalan a fél igazolási kérelme arra hivatkozással, hogy a beadványát azért nem tudta határidőben benyújtani, mert a jogi képviselőjének számítógépe meghibásodott, mivel az elektronikus kapcsolattartást választó felet terheli a kötelezettség, hogy gondoskodjon azokról a műszaki feltételekről, amelyek biztosítják az OBH által működtetett informatikai rendszer biztonságos alkalmazását. A Kúria megállapította, hogy a jogi képviselő által készített fellebbezés és meghatalmazás számítógéppel készült a kérdéses határidő utolsó napján, így ekkor még a jogi képviselő rendelkezésére állt olyan eszköz, amellyel beadványát a fél által választott módon elkészítette és a bírósághoz eljuttathatta. Arra is rámutatott, hogy a méltányosság alkalmazása során magasabb az elvárhatóság mértéke a jogi képviselőkkel szemben.[11]

Amennyiben a bíróság engedélyezi a papír alapú kapcsolattartásra történő áttérést, erről szóló döntését nem kell külön határozati formába foglalnia, tehát nem kell külön végzést hoznia. Azonban az áttérés iránti kérelem elutasításáról vagy visszautasításáról végzést hoz a bíróság, amely fellebbezhető. A fellebbezés előterjesztési módjára vonatkozóan nincs

[7] Pp. 69. § „(2) *Ha a per megindítását követően kerül sor a meghatalmazás rendelkezési nyilvántartásba vételére vagy a rendelkezési nyilvántartásba vett meghatalmazás módosítására, e jognyilatkozatok a bírósággal szemben a bíróságnak történő bejelentéstől, az ellenféllel szemben pedig a vele történő közléstől hatályosak*."
[8] CKOT 45. számú állásfoglalás
[9] Pp. 606. § (1) bek.
[10] Dombi-Nyárádi Gabriella, 2019: Az elektronikus kapcsolattartás. In: Wopera Zsuzsa: Kommentár a polgári perrendtartáshoz. Kommentár a polgári perrendtartásról szóló 2016. évi CXXX. törvényhez. Budapest, Wolters Kluwer Hungary Kft., p. 1371.
[11] BH2018. 314.

korlátozás, az akár papír alapon is előterjeszthető.[12] A visszautasító vagy elutasító végzés elleni fellebbezés esetén kérdésként merülhet fel, hogy a fellebbezés elbírálásáig a félnek beadványait papír alapon vagy elektronikusan kell-e benyújtania a bírósághoz. Soltész álláspontjában kifejti, hogy a jogszabály értelmezéséből az adódik, hogy a fellebbezés elbírálásáig a beadványokat már az elektronikus kapcsolattartás szabályai szerint kell előterjeszteni és kézbesíteni. Majd a fellebbezés elbírálásának eredményétől függően változhat a kapcsolattartás módja. Ezen gyakorlat helyességét igazolja, hogy amennyiben papír alapú kapcsolattartás érvényesülne az elbírálásig, a fellebbezés visszautasítása, illetve a kérelmet elutasító elsőfokú határozat hatályában történő fenntartása esetén az addig papír alapon benyújtott beadványokban foglalt nyilatkozatok hatálytalanná válnának.[13] Azonban mindenképp figyelembe kell venni azt a rendelkezést, hogy a beadvány elektronikus úton történő benyújtása az elektronikus út vállalásának minősül. Továbbá, ha a fellebbezés elbírálásáig a fél elektronikusan nyújtaná be a beadványait, ezzel azt igazolná, hogy tudja elektronikus úton tartani a kapcsolatot a bírósággal. A beadvány elektronikus úton történő előterjesztése akár a fellebbezés időszakában is az elektronikus kapcsolattartás vállalásának tekintendő. A Pp. rendelkezéseiből mindkét álláspont levezethető, ezért e kérdésben a bíróság feladata jogértelmezését kialakítani.[14] Véleményem szerint helyesebb, ha a fél papír alapú kapcsolattartásra jogosult a fellebbezés elbírálásáig, mivel éppen azért kérelmezi az áttérést, mert az elektronikus út számára aránytalan nehézséggel járna vagy a továbbiakban nem lehetséges.

5. Kötelező elektronikus kapcsolattartás

Az elektronikus kapcsolattartásra kötelezettek körét az E-ügyintézési tv. 9. § (1) bekezdése határozza meg. Az elektronikus kapcsolattartásra kötelezettek minden beadványt kizárólag elektronikus úton nyújthatnak be a bírósághoz és a bíróság is elektronikusan kézbesít részükre, kivéve a tárgyaláson csatolt vagy kézbesíthető iratot, illetve határozatot.[15] A polgári perben a félnek vagy a képviselőnek a beadványokat űrlapon kell előterjesztenie. Az E-ügyintézési tv. 25. § (7) bekezdése szerint, ha jogszabály az ügyfél számára valamely jognyilatkozat megtételére formanyomtatvány vagy elektronikus űrlap alkalmazását írja elő, vagy az elektronikus ügyintézést biztosító szerv számára formanyomtatvány vagy elektronikus űrlap rendszeresítését teszi lehetővé, az elektronikus ügyintézést biztosító szerv a formanyomtatvány

[12] Pp. 606. § (2) bek.
[13] Soltész Ilona, 2019: Az elektronikus kapcsolattartás. In: Petrik Ferenc: Polgári eljárásjog - Kommentár a gyakorlat számára. Harmadik kiadás. Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., p. 1303.
[14] Dombi-Nyárádi Gabriella: Az elektronikus… i. m. p. 1372.
[15] Pp. 608. § (1) bek.

helyett a jogszabályban meghatározott nyilatkozatok megtételét az ügyfél számára interaktív alkalmazás rendszeresítése útján is biztosíthatja. Az E-ügyintézési tv. 25. § (10) bekezdése kimondja, hogy az elektronikus ügyintézést biztosító szerv az elektronikus kapcsolattartási lehetőség megváltozása előtt - az informatikai biztonság sérülésének veszélye vagy bekövetkezése kivételével - a változást a honlapján a változást megelőző 30 nappal közzéteszi és az Elektronikus Ügyintézési Felügyeletnek bejelenti. Az elektronikus ügyintézést biztosító szerv a honlapján a módosítást követő 14 napon keresztül jelzi annak tényét, hogy a kapcsolattartás módja megváltozott. A Büsz. ehhez kapcsolódóan úgy rendelkezik, hogy az OBH elnöke a beadvány elektronikus úton történő előterjesztése esetére űrlapot rendszeresíthet, a központi honlapot el kell látni a nem rendszeresített űrlapok előterjesztésének jogkövetkezményeire, valamint az űrlap kitöltésének módjára vonatkozó tájékoztatással.[16]

Az űrlap benyújtásakor az elektronikus úton kapcsolatot tartó fél beadványa a kézbesítési rendszer útján informatikai szempontból ellenőrzésre kerül. Ha a beadvány nem felel meg az informatikai követelményeknek, akkor az elektronikus úton kapcsolatot tartó erről a benyújtási folyamat részeként közvetlenül értesítést kap. Amennyiben a beadvány megfelel az informatikai követelményeknek, erről a benyújtó értesítést, úgynevezett befogadás-visszaigazolást kap, amely tartalmazza a feladó nevét, az érkeztetési számot, a befogadás időpontját és az azonosításra alkalmas információkat. A beadvány akkor tekintendő benyújtottnak, ha befogadás-visszaigazolást küldött az informatikai rendszer.[17]

Elektronikus kapcsolattartás esetén fontos említést tenni a mellékletekről, illetve arról, hogy azok milyen formátumban csatolhatók. E kérdéskörre vonatkozóan nincs jogszabályi rendelkezés, hanem a Büsz. 75/F. § (1) bekezdés d) pontja alapján az Országos Bírósági Hivatal feladata tájékoztatást adni az elfogadott fájlformátumokról, valamint a befogadható fájlméretekről. Ez a tájékoztató a www.birosag.hu honlapon található meg. A beadványok benyújtása előtt mindenképp érdemes a honlapon tájékozódni, mert amennyiben a fájlformátum vagy fájlméret nem felel meg az ott rögzítetteknek, a beadvány nem minősül szabályszerűen benyújtottnak.[18]

A civilisztikai kollégiumvezetők vizsgálták azt a kérdést, hogy van-e helye hiánypótlásnak, visszautasításnak, ha a jogi képviselő által benyújtott keresetlevélben a szükséges azonosító adatok vagy egyéb adat nem teljes körűen szerepel, de a hiányzó adatok a keresetlevél mellékleteiből vagy az ÁNYK-ból megállapíthatóak. A CKOT 13. számú állásfoglalásában

[16] Büsz. 75/C. § (2b) – (2c) bek.
[17] Büsz. 75/C. § (2f) bek.
[18] Dombi-Nyárádi Gabriella: Az elektronikus… i. m. p. 1375.

kimondta, hogy a keresetlevél mellékletei (pl. biztosítási szerződés, bankkölcsönszerződés) nem fogadhatók el a peres felek azonosítására. A félnek a Pp. 170. § (1) bek. b)-c) pontja alapján a keresetlevélben konkrét állítást kell tennie a felek megnevezésére, azonosító adataira vonatkozóan. Az ÁNYK nem része a keresetlevélnek, így nem pótolja a keresetlevélben feltüntetni elmulasztott adatok hiányosságát. Funkcióját tekintve az ÁNYK elektronikus kapcsolattartás esetén olyan, mint papír alapú kapcsolattartás esetén a boríték.[19] Ez arra az esetre vonatkozik, ha a felperes vagy a jogi képviselő a keresetlevelet az ÁNYK nyomtatvány mellékleteként csatolja. Ha a felperes vagy a jogi képviselő a keresetlevelet a nyomtatványon terjeszti elő, akkor a keresetlevél részét képezi annak adattartalma.

Indokolt a jogi képviselő fogalmát megvizsgálni elektronikus kapcsolattartás esetén, ugyanis a Pp. 608. § (2) bekezdése kimondja, hogy jogi képviselőnek kell tekinteni a jogi előadót és az ügyvédjelöltet is, ha a perben eljárhatnak. E szabályozás célja, hogy a kapcsolattartási mód ne változhasson csak azért, mert egy adott beadványt nem a jogi képviselő, hanem jogi előadó vagy ügyvédjelölt nyújt be.[20] A civilisztikai kollégiumvezetők ezzel kapcsolatban azt vizsgálták, hogyan kell a fél jogi képviselőjének benyújtania a keresetlevelet a jegyző birtokvédelmi ügyben hozott határozata ellen. Kizárólag elektronikus úton vagy papír alapon is? A CKOT állásfoglalásában azt fogalmazta meg, hogy a jegyző birtokvédelmi ügyben hozott határozata elleni keresetlevelet a jogi képviselő a jegyzőhöz is csak elektronikus úton adhatja be.[21]

6. Egyes eljárási cselekmények problematikája

6.1. Képviseleti jog igazolása

Fontosnak tartom kiemelni az elektronikus kapcsolattartás körében, hogy a képviselő hogyan igazolhatja képviseleti jogát. Elektronikus kapcsolattartás esetén a képviselőnek az első, általa a bírósághoz benyújtott beadványhoz kell mellékletként csatolnia a meghatalmazását. Ha a meghatalmazás elektronikus okiratként rendelkezésre áll, akkor azt kell csatolni. Amennyiben elektronikus okiratként nem áll rendelkezésre a meghatalmazás, akkor a képviselő digitalizálja és úgy kerül csatolásra. A képviselőnek nem kell a meghatalmazását csatolnia, ha az szerepel a rendelkezési nyilvántartásban.[22] Amennyiben a képviselő számára adott meghatalmazás

[19] CKOT 13. számú állásfoglalás
[20] Dombi-Nyárádi Gabriella: Az elektronikus… i. m. p. 1376.
[21] CKOT 53. számú állásfoglalás
[22] Pp. 611. § (1) bek.

szerepel az általános meghatalmazások - OBH elnöke által működtetett - országos és közhiteles nyilvántartásában, a képviseleti jogosultságot ugyancsak nem kell külön igazolni.[23]

A képviseleti jog igazolásával kapcsolatban kérdésként merült fel, hogy hogyan kell a képviseleti jogot a bíróság előtt igazolni, ha még a jogi képviselő nem küldött beadványt a bírósághoz, így nem kerülhetett sor annak csatolására. Ebben a helyzetben kérdéses, hogy elegendő-e a meghatalmazást a bíróság előtti megjelenés alkalmával bemutatni vagy előtte meg kell-e küldeni a bíróság részére. Ez a helyzet akkor fordul elő, ha a meghatalmazott ügyvéd vagy ügyvédi iroda a helyettesítésével más ügyvédet vagy ügyvédi irodát bíz meg. Soltész ezzel kapcsolatban a következő álláspontot ismerteti: *„A kötelező elektronikus kapcsolattartásra vonatkozó szabályok alkalmazása során kérdésként merülhet fel, hogy milyen következmény érvényesül akkor, ha az első vagy valamely folytatólagos tárgyaláson a korábban jogi képviselő nélkül eljáró fél helyett olyan jogi képviselő jelenik meg, aki az ügy vitelére szóló meghatalmazását előzetesen elektronikus úton nem nyújtotta be. A Pp. 227. § (4) és (5) bekezdése értelmében, ha a képviseleti jog igazolása nem szabályszerű, a bíróság rövid határidővel felhívja a megjelent személyt a képviseleti jog igazolására. Szabályszerűen benyújtott meghatalmazás hiányában a bíróság az eljárást folytathatja, a megjelent fél kérelmére folytatja. Ha a megadott határidőn belül a mulasztást nem pótolták, a megjelent személy valamennyi perbeli cselekménye hatálytalan és a mulasztásra vonatkozó rendelkezéseket kell alkalmazni. Semmi sem indokolja, hogy a bíróság az elektronikus kapcsolattartással eljáró fél esetében pusztán az eltérő kapcsolattartási forma miatt hátrányosabb szabályokat alkalmazzon. Mindezekre tekintettel a meghatalmazás előzetes elektronikus benyújtását elmulasztó jogi képviselőt az általános szabályok szerint e körben hiánypótlásra kell felhívni, s csak ennek eredménytelen eltelte után alkalmazhatók a mulasztás jogkövetkezményei.*”[24] Az E-ügyintézési tv.-ből másik értelmezés vezethető le, amely szerint nincs helye elektronikus ügyintézésnek olyan eljárási cselekmény esetén, ahol ez nem értelmezhető. Ebből levezethető, hogy amennyiben a jogi képviselőnek korábban nem kellett beadványt küldenie a bíróságnak és így a meghatalmazás csatolására sem kerülhetett sor, a személyes megjelenés olyan eljárási cselekmény, ahol már az elektronikus ügyintézés nem értelmezhető.[25]

[23] Vitvindics Mária, 2017: Az elektronikus technológiák és eszközök alkalmazása. In: Wopera Zsuzsa: A polgári perrendtartásról szóló 2016. évi CXXX. törvény magyarázata. Budapest, Wolters Kluwer Hungary Kft., p. 685.
[24] Soltész Ilona: Az elektronikus… i. m. p. 1310.
[25] Dombi-Nyárádi Gabriella: Az elektronikus… i. m. pp. 1379-1380.

E körben mindenképp meg kell említeni a CKOT 3. számú állásfoglalását, amely azzal a kérdéssel foglalkozott, hogy mi a jogkövetkezménye, ha a tárgyaláson megjelent - a fél képviselőjeként korábban el nem járó – jogi képviselő elektronikus úton nem csatolta a meghatalmazását. Az állásfoglalás szerint ebben az esetben a bíróságnak fel kell hívni a jogi képviselőt rövid határidő tűzésével a képviseleti jog igazolására. Ha a képviseleti jog igazolása nem szabályszerű, akkor a bíróság rövid határidővel felhívja a megjelent személyt a képviselet szabályszerű igazolására. Ha a jogi képviselő a tárgyaláson, de papír alapon igazolja képviseleti jogát, az nem megfelelő, de mivel a képviseleti jogának igazolása nem szabályszerű, ennek igazolására kell felhívnia a bíróságnak. Amennyiben a felhívásban szereplő határidőben történő igazolást elmulasztja, akkor lesz valamennyi perbeli cselekménye hatálytalan.[26]

A Pp. hatálybalépése óta 2020. december 31-ig a Pp. 608. § (1) bekezdése szerint „*Az E-ügyintézési tv. alapján elektronikus úton történő kapcsolattartásra kötelezett minden beadványt kizárólag elektronikusan - az E-ügyintézési tv.-ben és végrehajtási rendeleteiben meghatározott módon - nyújthat be a bírósághoz, és a bíróság is elektronikusan kézbesít a részére*". A Pp. 605. § (3) bekezdése a következőképp rendelkezett a Pp. hatálybalépésétől 2020. december 31-ig: *„Az (1) bekezdés szerinti elektronikus út választása esetén az eljárás folyamán - ideértve az eljárás minden szakaszát és a rendkívüli perorvoslatot is - a fél, illetve képviselője köteles a bírósággal a kapcsolatot elektronikus úton tartani és a bíróság is valamennyi bírósági iratot elektronikusan kézbesít a részére."* A CKOT állásfoglalásának megfogalmazásakor az ismertetett, a vizsgált kérdéskörhöz kapcsolódó rendelkezések voltak hatályosak.

A Pécsi Ítélőtábla Polgári Kollégiuma a 2/2019. (III. 27.) számú ajánlásában fogalmazta meg, hogy a tárgyaláson teljesítendő eljárási cselekményre az E-ügyintézési törvény 8. §-ának (4) bekezdése értelmében az elektronikus kapcsolattartás nem értelmezhető, ezekre az eljárási cselekményekre az E-ügyintézési törvény hatálya nem terjed ki, és a Pp. elektronikus kapcsolattartásra vonatkozó rendelkezései sem alkalmazhatók. Az ajánlásban kifejtésre került, hogy az a jogértelmezés, amely szerint a tárgyalást el kell halasztani azért, hogy a fél a tárgyaláson rendelkezésre álló meghatalmazást vagy egyéb okiratot elektronikusan nyújtsa be, nem csak az E-ügyintézési tv., hanem az Alaptörvény 28. §-ában megfogalmazott „józan ész" követelményével és a Pp. Preambulumában megfogalmazott jogalkotói céllal is ellentétes volna.[27]

Azonban 2021. január 1-jétől a polgári perrendtartásról szóló 2016. évi CXXX. törvény módosításáról szóló 2020. évi CXIX. törvény (a továbbiakban: I. Pp. Novella) 75. § 31. pontja

[26] CKOT 3. számú állásfoglalás
[27] Pécsi Ítélőtábla Polgári Kollégiuma 2/2019. (III. 27.) kollégiumi ajánlás

alapján a Pp. 608. § (1) bekezdése a következőképp változott: „*Az E-ügyintézési tv. alapján elektronikus úton történő kapcsolattartásra kötelezett minden beadványt kizárólag elektronikusan - az E-ügyintézési tv.-ben és végrehajtási rendeleteiben meghatározott módon - nyújthat be a bírósághoz, és a bíróság is elektronikusan kézbesít a részére, kivéve a tárgyaláson csatolt vagy kézbesíthető iratot, illetve határozatot”*. Szintén 2021. január 1-jétől az I. Pp. Novella 75. § 31. pontja alapján változott a Pp. 605. § (3) bekezdése: *„Az (1) bekezdés szerinti elektronikus út választása esetén az eljárás folyamán - ideértve az eljárás minden szakaszát és a rendkívüli perorvoslatot is - a fél, illetve képviselője köteles a bírósággal a kapcsolatot elektronikus úton tartani és a bíróság is valamennyi bírósági iratot elektronikusan kézbesít a részére, kivéve a tárgyaláson csatolt vagy kézbesíthető iratot, illetve határozatot.”* Az I. Pp. Novella hatálybalépéséig a joggyakorlatban nem alakult ki egységes gyakorlat, azonban a módosítás választ adott arra a kérdésre, hogy az elektronikus kapcsolattartásra kötelezettek, illetve elektronikus kapcsolattartást választó személyek becsatolhatnak-e iratot a tárgyaláson. Ez alapján megengedett, hogy a tárgyaláson benyújtsanak iratot. Ez a módosító szabály összhangban áll az E-ügyintézési tv. 8. § (4) bekezdésével, amely szerint nincs helye elektronikus ügyintézésnek olyan eljárási cselekmény esetében, ahol ez nem értelmezhető.

6.2 Perköltség felszámítása

Felvetődik a kérdés, hogy az utolsó tárgyaláson felmerült perköltség felszámítása miként történhet a polgári peres eljárás során. Az Új Pp. Konzultációs Testület állásfoglalást fogalmazott ezzel kapcsolatban, amely szerint mód van a tárgyaláson felmerült költségek felszámítására papír alapon vagy a fél képviselője azt jegyzőkönyvbe is mondhatja.[28] Az állásfoglalás megfogalmazása idején a Pp. 81. § (5) bekezdése szerint „*A jogi képviselővel eljáró fél a perköltségét kizárólag jogszabályban meghatározott költségjegyzék előterjesztése útján számíthatja fel”*. Kettő álláspont alakult ki, az egyik szerint kizárólag elektronikusan nyújthatja be a jogi képviselővel eljáró fél a tárgyalás berekesztésére történt figyelmeztetés és a határozathirdetés közötti időszakban, míg a másik álláspont szerint lehetőség van a tárgyaláson a költségek felszámítására. Az I. Pp. Novella a következőképp módosította a Pp. 81. § (5) bekezdését: „*A jogi képviselővel eljáró fél a perköltségét jogszabályban meghatározott költségjegyzék előterjesztése útján is felszámíthatja*”; ezzel választ adva a vizsgált kérdésre. A jogi képviselővel eljáró félnek tehát már nem kötelező a jogszabályban meghatározott

[28] Új Pp. Konzultációs Testület 46. számú állásfoglalás

formanyomtatványon előterjeszteni költségigényét, ez a továbbiakban lehetőség és már nem kötelezettség számára.

7. Az elektronikus kapcsolattartás szabályainak megszegéséhez kapcsolódó jogkövetkezmény

Fontosnak tartom áttekinteni, hogy az elektronikus kapcsolattartásra vonatkozó szabályok megszegésének milyen következményei vannak. Ha az elektronikus úton kapcsolatot tartó fél nem elektronikus úton vagy elektronikus úton, de nem az E-ügyintézési tv.-nek megfelelően nyújtja be a bírósághoz a keresetlevelet, az ellentmondást, a fellebbezést, a felülvizsgálati kérelmet vagy a perorvoslati kérelmet, akkor azokat a bíróság visszautasítja, az egyéb beadványban foglalt nyilatkozat pedig hatálytalan.[29] Az Új Pp. Konzultációs Testület 43. számú állásfoglalásában rögzítette, hogy amennyiben a jogi képviselő a kötelező elektronikus kapcsolattartásra vonatkozó szabályok figyelembevétele nélkül a perorvoslati kérelmet papír alapon (nem elektronikus úton), vagy elektronikus úton, de nem megfelelő módon terjeszti elő, a bíróság hiánypótlási felhívás kiadása nélkül visszautasítja.[30]

8. Az illeték megfizetése

Az illeték megfizetésére több módon is sor kerülhet elektronikus ügyintézés esetén a polgári per folyamán. Az illetékekről szóló 1990. évi XCIII. törvény (a továbbiakban: Itv.) rögzíti, hogy a bírósági eljárási illetéket főszabály szerint elektronikus fizetési és elszámolási rendszeren (a továbbiakban: EFER) keresztül vagy illetékbélyeggel az eljárást kezdeményező iraton kell megfizetni. E szabály alól kivételt képez az olyan eset, amikor jogszabály más fizetési módot is megenged, vagy ha az illeték viseléséről a bíróság az eljárást befejező határozatában dönt.[31] Az Itv. 74. § (1a) bekezdése alapján a 10 000 forintot meghaladó eljárási illetékkiszabás alapján készpénz-átutalási megbízás útján vagy az állami adóhatóság által meghatározott számlaszámra átutalással, illetve amennyiben erre lehetőség van, bankkártyával is megfizethető. Az Itv. 74. § (1b) bekezdése szerint, ha a keresetindítási határidő legalább 31 nap és a bírósági eljárás kezdeményezésekor fizetendő illeték összege az 500 000 forintot meghaladja, az eljárási illetékkötelezettség önadózással is teljesíthető.

Az eljárási illetékek megfizetésének és a megfizetés ellenőrzésének részletes szabályairól szóló 44/2004. (XII. 20.) PM rendelet (a továbbiakban: Itv. vhr.) kiegészíti az Itv. rendelkezéseit, amely szerint a bírósági eljárásban elektronikus úton eljáró fél az illetéket az EFER-en keresztül

[29] Pp. 618. § (1) bek.
[30] Új Pp. Konzultációs Testület 43. számú állásfoglalás
[31] Itv. 74. § (1) bek.

vagy az illetékes bíróság Kincstárnál vezetett illetékbevételi számlájára átutalással fizeti meg. Az Itv. vhr. meghatározza, hogy átutalás esetén a közleményrovatban milyen adatokat kell feltüntetni, ezek a következők: az eljáró bíróság jelzőszáma és az eljárási illetékfizetésre kötelezett fél neve, a beadvány bírósági érkeztetési azonosító száma és - ha az ismert a - lajstromszáma. Az Itv. vhr. kimondja, hogy átutalás esetén az illetéket annak a bíróságnak az illetékbevételi számlájára kell megfizetni, amely bíróság előtti eljárásban az illetékfizetési kötelezettség keletkezik.[32]

Az Itv. vhr. 6/A. § (4) bekezdése szerint, ha az illetéket az elektronikus úton eljáró fél a bíróság Kincstárnál vezetett illetékbevételi számlájára történő átutalással kerül megfizetésre

a) a fellebbezési illetéket

aa) ha a fellebbezett határozatot járásbíróság, kerületi bíróság, vagy törvényszék hozta, a határozatot hozó bíróság székhelye szerinti törvényszék;

ab) ha a fellebbezett határozatot ítélőtábla hozta, a határozatot hozó ítélőtábla;

b) a csatlakozó fellebbezési illetéket a fellebbezési eljárást lefolytató törvényszék vagy ítélőtábla;

c) a felülvizsgálati illetéket a felülvizsgálati kérelemmel érintett határozatot hozó elsőfokú bíróság székhelye szerinti törvényszék;

d) a csatlakozó felülvizsgálati illetéket a Kúria

illetékbevételi számlájára kell teljesíteni.[33]

Az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet (a továbbiakban: E-ügyintézési tv. vhr.) az EFER-en keresztüli kifizetés kapcsán rögzíti, hogy a csatlakozott pénzforgalmi szolgáltató a fizetési megbízás fizető fél általi jóváhagyását követően a csatlakozási megállapodásban meghatározott formai és tartalmi követelményeknek megfelelő elektronikus igazolást állít ki, amely tartalmazza:

a) fizetett összeget,

b) a fizetés jóváhagyásának időpontját,

c) a 104. § (1) bekezdés b) pontja szerinti fizetési ügyazonosítót,

d) a fizetés EFER elszámolási számlájának számát, a POS terminálon kezdeményezett bankkártyás fizetés kivételével, valamint

e) a csatlakozott fizetési megoldás szolgáltató azon nyilatkozatát, hogy az igazolásban megjelölt fizetési megbízás teljesítését elindította.[34]

[32] Itv. vhr. 6/A. § (3) bek.
[33] Itv. vhr. 6/A. § (4) bek.
[34] E-ügyintézési tv. vhr. 105. § (1) bek.

Ezek közül a fizetési módok közül az EFER-en keresztüli fizetés és a bíróság illetékbevételi számlájára történő illetékfizetés esetén érvényesül, hogy ha a beadványt elektronikus úton nyújtják be, a bíróság a keresetlevél beadásával egyidejűleg nem szerez tudomást az illeték megfizetéséről. Ebben az esetben a beadvány érkeztetését követő 3 munkanapon belül az illetékfizetéssel, illetve annak elmulasztásával kapcsolatban nincs helye hiánypótlási felhívásnak, a keresetlevél visszautasításnak, valamint fizetési meghagyásos eljárással összefüggő perben az eljárás megszüntetésének.[35]

9. Az elektronikus levélcím eljárásjogi megítélése

Úgy gondolom, hogy az elektronikus kapcsolattartás tárgykörén belül az elektronikus levélcím eljárásjogi megítélését fontos áttekinteni. Fontos leszögezni, hogy a beadvány elektronikus levélcímről bírósághoz történő benyújtása nem minősül elektronikus útnak. A Pp. pontosan rögzíti, hogy a bíróság a fél elektronikus levélcímére iratot csak e törvényben meghatározott esetben továbbíthat.[36] Hirdetményi kézbesítés esetén, ha a fél elektronikus levélcímét a bíróságnak bejelentették, a hirdetményt az elektronikus levélcímre is meg kell küldeni.[37] A bírósági irat kézbesíthetetlensége esetén, ha a fél elektronikus levélcímét a bíróságnak bejelentették, akkor a keresetlevél és az eljárást befejező érdemi határozat esetén kézbesítési fikció beállásáról értesíteni kell.[38] A fél, az ügyész és a perben részt vevő egyéb személy, valamint azok képviselője kérheti, hogy a részére kiadható iratot a bíróság az általa megadott elektronikus levélcímre továbbítsa, amennyiben az irat elektronikus formában, elektronikus okiratként vagy a papír alapú okirat elektronikus másolataként a bíróság rendelkezésére áll.[39]

III. Elektronikus hírközlő hálózat igénybevétele

1. Elektronikus hírközlő hálózat útján történő meghallgatásról általában

Elektronikus hírközlő hálózat útján a fél és más perbeli személy, a tanú, valamint a szakértő meghallgatására, valamint a szemle lefolytatására kerülhet sor, ha a szemletárgy birtokosa nem tiltakozik. A bíróság akár a fél indítványára, akár hivatalból elrendelheti az elektronikus hírközlő hálózat útján történő meghallgatást. A bíróság e döntését végzés formájában hozza

[35] Pp. 614. § (1) bek.
[36] Pp. 614. § (3) bek.
[37] Pp. 145. § (1) bek.
[38] Pp. 137. § (3) bek.
[39] Pp. 619. § (1) bek.

meg. Ilyen döntésre akkor van lehetőség, ha az célszerűnek látszik, vagy a meghallgatás a tárgyalás, illetve a személyes meghallgatás kitűzött helyszínén jelentős nehézséggel vagy aránytalanul nagy többletköltséggel járna, vagy ezt a tanú személyes védelme indokolja. Az elektronikus hírközlő hálózat útján történő meghallgatást a bíróság végzéssel rendeli el, amelyet a megidézetteknek a tárgyalásra, személyes meghallgatásra vagy szemlére szóló idézéssel együtt kézbesíti, továbbá meg kell küldenie az ily módon történő meghallgatáshoz elkülönített helyiséget biztosító bíróságnak, illetve egyéb szervnek. Elektronikus hírközlő hálózat útján történő meghallgatás során a tárgyalás, személyes meghallgatás, szemle helyszíne és az elektronikus hírközlő hálózat útján történő meghallgatás helyszíne között az összeköttetés közvetlenségét mozgóképet és hangot egyidejűleg továbbító eszköz biztosítja. Amennyiben a közvetlen összeköttetés biztosítható, lehetőség van több egyéb elektronikus hírközlő hálózat útján történő meghallgatási helyszín igénybevételére.[40]

Az elektronikus hírközlő hálózat útján meghallgatásra kerülő személynek a bíróság vagy egyéb szerv épületében található, erre a célra kialakított helyiségben kell megjelennie és a meghallgatás ideje alatt jelen lennie. A nyilvánosságot a tárgyalás kitűzött helyszínén kell biztosítani. A Pp. meghatározza, hogy kik tartózkodhatnak az elektronikus hírközlő hálózat útján történő meghallgatás helyszínén.[41]

2. A veszélyhelyzet ideje alatt bővülő jogi környezet

A veszélyhelyzet ideje alatt érvényesülő egyes eljárásjogi intézkedésekről szóló 74/2020. (III. 31.) Korm. rendelet (a továbbiakban: Veir.)[42] rögzítette, hogy a polgári peres eljárás szabályait a veszélyhelyzet ideje alatt a Pp.-ben, illetve a polgári perrendtartásról szóló 1952. évi III. törvényben (a továbbiakban: 1952-es Pp.) foglaltaktól milyen eltérésekkel kell alkalmazni. A vizsgált tárgykörhöz kapcsolódóan kimondta, hogy a Pp. hatálya alá tartozó ügyekben a perfelvételt a perfelvételi tárgyalás mellőzésével kell lefolytatni, azonban az érdemi tárgyalást és az 1952-es Pp. hatálya alá tartozó perekben a tárgyalást lehetőség szerint elektronikus hírközlő hálózat vagy más elektronikus kép és hang továbbítására alkalmas eszköz útján kell megtartani.[43] A veszélyhelyzet megszűnésével összefüggő átmeneti szabályokról és a járványügyi készültségről szóló 2020. évi LVIII. törvény a vizsgált tárgykörhöz kapcsolódóan a polgári peres és bírósági polgári nemperes eljárásokra vonatkozó az 1952-es Pp.-től, valamint a Pp.-től eltérő rendelkezések alkalmazását rögzíti, amelynek 138. § (1) bekezdése kimondja,

[40] Pp. 622-623. §
[41] Pp. 624. §
[42] Hatályban volt: 2020. III. 31-től 2020. VI. 17-ig
[43] Veir. 21. § (2) – (3) bek.

ha a járványügyi intézkedések indokolják, a tárgyalás elektronikus hírközlő hálózat vagy más elektronikus kép és hang továbbítására alkalmas eszköz útján is megtartható.[44]

A Kúria Polgári Kollégiuma a veszélyhelyzet ideje alatt az elektronikus kép és hang továbbítására alkalmas eszköz útján megtartott tárgyalás feltételeiről szóló 2/2020. (IV. 30.) PK véleményben fogalmazta meg azon álláspontját, amely az e-tárgyalásokra vonatkozó eljárásrendet tartalmazza. A kollégiumi véleményben a Kúria iránymutatást adott a bíróságok számára a veszélyhelyzet idején folytatott polgári eljárási cselekmények zavartalan foganatosításához. Más elektronikus kép és hang továbbítására alkalmas eszköz útján csak akkor tartható tárgyalás (a továbbiakban: e-tárgyalás), ha a bíróság tagjain kívül minden tárgyalásra idézendő személynek rendelkezésére áll az ehhez szükséges technikai feltétel. A bíróságnak hivatalból kell vizsgálnia a feltételeket. A használandó eszköz, illetve program fajtája a bíróság által kerül előre meghatározásra.[45] A feltételek rendelkezésre állását a tárgyalásra idézendő személyek előzetes nyilatkozata alapján lehet megállapítani. A Veir. alapján, ha rendelkezésre álltak a feltételek, e-tárgyalást kellett tartani, így biztosítható volt a célja, amely a közvetlen személyes kapcsolatok kerülése volt. Az e-tárgyalás feltétele az e-mail cím előzetes bejelentése, valamint, hogy az idézettek rendelkezzenek kép és hang egyidejű továbbítására alkalmas eszközzel és internet-kapcsolattal. Az elektronikus kapcsolattartásra kötelezetteket is fel kell hívni arra, hogy nyilatkozzanak a technikai eszközök rendelkezésükre állnak-e. A felhívásnak célszerű tartalmaznia arra vonatkozó tájékoztatást, hogy mi lesz a jogkövetkezménye, ha nincs lehetőség e-tárgyalásra. A bíróságnak tájékoztatást kell adni a felhívásban arról, hogy a nyilatkozat elmulasztása esetén a bíróság úgy tekinti, hogy nem állnak rendelkezésre a szükséges feltételek. Az idézés szabályai alkalmazandók, tehát nem mellőzhető e-tárgyalás esetén sem az idézés. Azonban a tárgyalás helye helyett a tárgyalás megtartásának pontos módját kell feltüntetni, valamint a címzettet tájékoztatni kell, hogy a „skype értekezlet”-ről külön kap egy értesítést. Az idézésnek tartalmaznia kell a távolmaradás következményeit, közreműködő esetén a velük szemben alkalmazható kényszerítő eszközök közül alkalmazható rendelkezésekről kell tájékoztatást adni (pl. pénzbírsággal sújtás, elővezetés nyilvánvalóan nem alkalmazható). Az e-tárgyalásra is a tárgyalás nyilvánosságára vonatkozó rendelkezéseket kell alkalmazni azzal, hogy a nyilvánosságot a tárgyalás „kitűzött helyszínén” kell biztosítani a veszélyhelyzeti érintkezés szabályainak betartásával. Ebben az esetben ez a bíró jelenléti helyét jelenti. Általános szabály, hogy a bírónak az e-tárgyalás során jegyzőkönyvkészítési kötelezettsége van, amely készülhet jegyzőkönyvvezető közreműködésével vagy folyamatos

[44] 2020. évi LVIII. törvény 138. § (1) bek.
[45] Megjegyzés: A bíróságok egységesen a Skype for Businesst tudják alkalmazni.

felvétel útján is. E jegyzőkönyvben a tárgyalás helye helyett az e-tárgyalás megtartásának módját kell feltüntetni. Az e-tárgyaláson is lehetőség van szembesítésre azzal, hogy ezen bizonyítási eljárásban fizikailag nem kell egy térben lenniük a feleknek, illetve tanúknak. Az e-tárgyalás során az ítélethozatal tárgyaláson kívül történik, ezért az ítélethozatal feltételeinek fennállása esetén a tárgyalás berekesztésre kerül, és nem kerül kihirdetésre az ítélet.[46]

IV. Összegzés

Az elektronikus úton történő eljárás és a papír alapú eljárás egyszerre van jelen a polgári perben a járványügyi intézkedések hatálya alatt is. Az elektronikus kapcsolattartás az E-ügyintézési tv. által meghatározott személyi kör számára kötelező. Ez alapján nem minden jogkereső köteles az elektronikus út igénybevételére. Ahogy a korábbi szabályozásban, úgy itt is lehetősége van a félnek az elektronikus kapcsolattartás választására. Az elektronikus úton történő eljárással kapcsolatban felmerülő kérdések megfelelő szabályozása szükséges, hogy az ne eredményezze a felek és közreműködők érdekeinek sérelmét. A fentebb kifejtett problémákra reagált a jogalkotó és az I. Pp. Novella a Pp. 605. §-ának és 608. §-ának módosításával választ adott az elektronikus kapcsolattartás körében felmerülő néhány kérdésre (költségek felszámítása, meghatalmazás bemutatása). A fennmaradó kérdések értelmezése során is figyelemmel kell lenni a „józan ész" kritériumára, valamint a perkoncentráció elvére, mint a polgári perjog sajátos alapelvére.

A polgári perben az elektronikus hírközlő hálózat, valamint a más kép és hang egyidejű továbbítására alkalmas eszköz útján történő meghallgatás a koronavírus járvány következtében felértékelődött, illetve előtérbe került az ily módon tartandó tárgyalás. A Veir. hatálya alatt tárgyalást csak ilyen eszköz útján lehetett lefolytatni. A Kúria pedig a zavartalan működés előmozdítása végett eljárásrendet dolgozott ki az elektronikus kép és hang egyidejű továbbítására alkalmas eszköz útján megtartott tárgyalásra vonatkozóan.

[46] 2/2020. (IV. 30.) PK vélemény veszélyhelyzet ideje alatt az elektronikus kép és hang továbbítására alkalmas eszköz útján megtartott tárgyalás feltételeiről

Tóth Dávid[*]: A közösségi média és a bűnözés összefüggései[*]

Absztrakt:

A közösségi média napjainkra az életünk alapvető részévé vált. 2020-ban csak a facebook közösségi portálnak több mint 2.6 milliárd aktív használója volt. Számos embernek az első teendője reggel, hogy ellenőrizze kapott-e értesítést, illetve üzenetet a facebookon vagy egyéb közösségi média felületeken (pl.: twitter, snapchat, instagram, stb,). Az okostelefonok fokozatos elterjedésével a közösségi média már az embereket mindenhova elkíséri. Ezek a platformok kommunikációs felületet biztosítanak embereknek, cégeknek, államoknak. A koronavírus okozta pandémiás helyzet miatt az emberek még inkább függővé váltak a kibertértől, hiszen sokan otthon végzik munkájukat az interneten keresztül.

A közösségi média, ahogy transzformálja az emberek életét, úgy változtatja meg a bűnözési formákat. A kibertér a bűnözés egyik színterévé vált, ahol sui generis deliktumok jelentek meg, mint például a cyberbullying (online zaklatás) vagy az identitáslopás.

A kutatásom célja a közösségi média és a bűnözés alapvető összefüggéseit vizsgálni, illetve áttekintést nyújtani a lehetséges bűnözési formákról.

Kulcsszavak*: kiberbűnözés, közösségi média, identitáslopás, cyberbullying*

I. Bevezetés

A közösségi média térnyerése az elmúlt évtizedben folyamatos volt, de a COVID-19 okozta pandémiás helyzet további lökést adott neki. Közösségi médiának minősül minden olyan internetes oldal (weboldal) és szoftver, amelyet közösségi hálózat építésére használnak (ún. social networking). Közösségi médiának tekinthetünk minden olyan online eszközt, amely lehetővé teszi felhasználói számára, hogy tartalmakat készíthessenek és/vagy oszthassanak meg a nyilvánossággal, vagy privát köreikkel. Egy interaktív kommunikációs színteret biztosít az embereknek a világhálón. Magát, a közösségi média kifejezést, először Darrel Berry használta 1995-ben, olyan számítógépes programok rendszerére, mint például Matissera, amely elősegítette az együttműködő közösségek felépítését, annak egyéni élményét. Ezt *social media*

[*]Dr. Tóth Dávid Ph.D., adjunktus, PTE-ÁJK Kriminológiai és Büntetés-végrehajtási Jogi Tanszék

[*] „AZ INNOVÁCIÓS ÉS TECHNOLÓGIAI MINISZTÉRIUM ÚNKP-21- 4-II-PTE-962 KÓDSZÁMÚ ÚJ NEMZETI KIVÁLÓSÁG PROGRAMJÁNAK A NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS ALAPBÓL FINANSZÍROZOTT SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.”

architecturesnek nevezte el. A közösségi média kifejezést, a mai értelemben, Chris Shipley-t használta, a Guidewire csoport társalapítója és globális kutatási vezetője.[1]

A közösségi médiának több fajtája van.

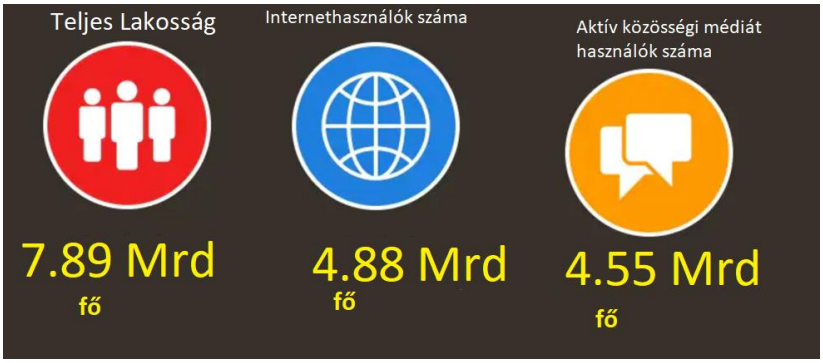
- Közösségi hálózatok. Ezeken a platformokon a felhasználók egymással kapcsolatba kerülhetnek, megoszthatják véleményüket, gondolataikat, fényképüket, egymással vagy a nyilvánossággal. Legismertebb példája a facebook, de idesorolható a twitter, vagy a szakmai közösség számára LinkedIn, illetve régebben Magyarországon az iwiw.
- Médiahálózatok. A fenti kategóriától eltérően ezeknél a hálózatoknál a központi elem a médiatartalmakon (videó, kép stb.) van. A médiahálózatok a közösségi média olyan részét képezi, ahol a felhasználók egymással médiatartalmakat oszthatnak meg, azzal kapcsolatban véleményt jegyezhetnek. A legismertebb példák közé sorolható a Google tulajdonában lévő Youtube és a Meta (korábbi Facebook tulajdonában lévő Instagram. Az elmúlt években megfigyelhetőek átfedések az előbbi kategóriával, de mégis elsősorban ezeknek a platformoknak a célja a médiaelemek megjelenítése és megosztása lesz. További különbség a közösségi hálózatokhoz képest, hogy itt a felhasználók feliratkozókat és követőket szerezhetnek nem pedig barátokat, ismerősöket.
- Véleményhálózatok. Nevéből is adódóan az ilyen hálózatoknak a fókuszában a véleménynyilvánítás áll, a felhasználóknak itt lehetőségük van különböző szolgáltatásokat, helyszíneket értékelni, és megosztani azt egymással. Erre a közösségi médium formára jó példa a TripAdvisor.
- Kibeszélőhálózatok. A kibeszélőhálózatok sok szempontból hasonlítanak a korábbi blogokra, de itt egy sokkal interaktívabb platformról van szó. A felhasználók megoszthatnak egy témát, vagy gondolatot, és az aziránt érdeklődök hozzászólhatnak, és kifejhetik véleményüket különböző alcsoportokban. Kibeszélőhálózatok egyik legismertebb példája a Reddit oldala. Közösségformáló erejét mutatja az ún. Reddit vs. Wallstreet ügyben, ami 2021 januárjában indult el. A redditezők egyik alcsoportja volt a wallstreetbets, ahol felhasználók egymást győzték meg arról, hogy a Gamestop nevezetű videójáték árusításával foglalkozó cég részvényeibe érdemes befektetni, miközben shortolták a céget azt remélve, hogy a részvények ára csökken. A részvények ára viszont elkezdett növekedni néhány hét alatt 1700%-os mértékben a redditezők befektetései miatt.

[1] Dwivedi, Y. K. – Kapoor, K. K., – Chen, H., 2015: Social media marketing and advertising. In: The Marketing Review, 3. szám pp. 289-309.

II. A közösségi média növekedése

Napjainkban szinte már közhelynek számít az a megállapítás, hogy az infokommunikációs technológiák terjedése jelentős mértékben átalakítja az emberek életét és mindennapjait. A szociális médiumok a mindennapjaink részévé váltak, nélkülözhetetlenné váltak otthonjainkban, munkahelyeken, iskolákban, vagy akár átutazóban.

A közösségi média a felhasználók számát tekintve nagy mértékű növekedésen ment keresztül az elmúlt években, amelyen a koronavírus okozta világjárvány csak tovább lendített. 2021 októberében a világ teljes lakossága körülbelül 7.89 milliárd fő. A Hootsuite felmérése szerint a világ populációjának közel 62%-a, azaz 4.88 milliárd ember internethasználó és ebből 4.55 milliárd fő használ aktívan valamilyen közösségi oldalt (ami azt jelenti, hogy legalább havonta egyszer bejelentkeznek a felhasználói fiókjukba).



1. számú ábra. A világ lakosságának lélekszáma, az internethasználók száma és az aktív közösségi média felületeket használók száma.[2]

Az elmúlt egy évben (2020 októberéhez képest) 400 millió fővel nőtt a közösségi médiát használók száma, ami 9.9%-s növekedést jelent. Globálisan naponta körülbelül több mint egymillió fővel nő a regisztráltak száma. A világ társadalmának digitalizációja köszönhető annak is, hogy általában nő a népesség, a becslések szerint a jelenlegi növekedési rátával a világ népesség 2023 közepére elérheti a 8 milliárd főt.

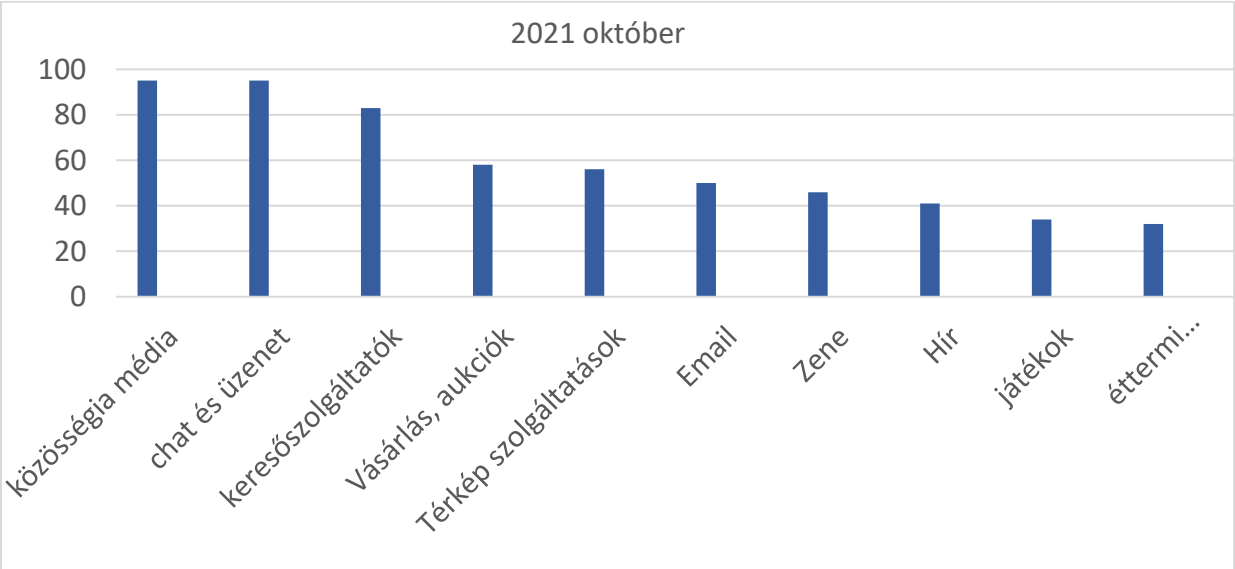
Nemcsak nő a szociális médián a regisztráltak száma, hanem a felhasználók ott eltöltött ideje is növekszik. Átlagosan jelenleg 2.27 órát töltünk egy nap a közösségi média felületeken. Az aktív használat növekedése pedig összefüggésbe hozható az okostelefonok elterjedésével[3], ami

[2] Forrás: https://datareportal.com/reports/digital-2021-october-global-statshot (2021. 11. 20.)

[3] Az okostelefonokra telepített alkalmazások is hordozhatnak biztonsági kockázatokat. Csak a Facebook alkalmazás körülbelül harminc engedélyt kér cserébe azért, hogy azt használhassuk, mint például személyes

még inkább megkönnyítette az internethez való hozzáférést, illetve a közösségi média felületekhez való bejelentkezést. Jelenleg 5.29 milliárd fő használ világszerte okostelefonokat, ami a világ népességének 67.1%-t teszi ki.

A 16 és 64 év közötti korosztály több mint 90%-a használ valamilyen közösségi oldalt és az ahhoz kapcsolódó csevegő (chat és üzenet) alkalmazásokat, mint például a Facebook messengert. Ezzel használat gyakoriságot tekintve a közösségi média már megelőzi a keresőszolgáltatásokat is, mint például a google-t azt a korosztály valamivel több mint 80%-a használja. Visszaszorulóban van az email és a hírportálok használata, ennek oka lehet, hogy ezek a funkciók, és szolgáltatások beintegrálódnak a közösségi oldalakba.



2. számú ábra. A 16-64 korosztály internethasználati szokásai.[4]

A világ vezető közösségi média szolgáltatói vagy észak-amerikaiak vagy kínaiak. A világ nagyobb szociális hálója a Facebook közel 2.9 milliárd aktív felhasználóval. Második helyen a Youtube közel 2.3 milliárd regisztrált fővel és a dobogó harmadik fokán a whatsapp áll, 2 milliárd használóval. A kínai közösségi hálók között kiemelkedik a Wechat és a Tiktok és a Weibo.

adatok, névjegyadatok, helymeghatározás stb. Lásd bővebben: Bányász, Péter, 2018, Az okos mobil eszközök biztonsága. In: Hadmérnök 2. szám pp. 360-377.
Andrea Kraut – László Kőhalmi – Dávid Tóth, 2020: Digital Dangers of Smartphones. In: Journal of Eastern-European Criminal Law 1. szám pp. 36-49.

[4] Forrás: https://datareportal.com/reports/digital-2021-october-global-statshot (2021. 11. 20.)

3. számú ábra. A vezető közösségi média felületek a világon.[5]

III. Veszélyforrások a közösségi médián

Ahogy a fenti számokból is láttuk az információtechnológiától és a közösségi médiától való függőségünk egyre inkább csak növekszik. A vezető hírek között szereptelt amikor pár órára leállt a Facebook és a hozzá kapcsolódó szolgáltatások és alkalmazások 2021 októberében.[6]

Ez a sok szempontból kényelmes, és gyors kommunikációs színtér egy Janus-arcú jelenség, mivel nem kizárólag megkönnyíti az emberek életét, hanem számos veszélyforrást hordoz magában, amelyeket e fejezetben szeretném áttekintő jelleggel elemezni.

A közösségi média veszélyforrásai[7] közé sorolhatók többek között az alábbiak:

- adathalászat (phising), identitáslopás,
- pedofília,
- terrorizmus,
- csalások,
- szervezett bűnözés, és ahhoz kapcsolódóan kábítószer-kereskedelem,
- rémhírterjesztés,
- online zaklatás (cyberbullying).

A fenti példák nem taxatívak, a jövőben a közösségi média fejlődésével (vagy esetleg devalválódásával) a fenti bűnözési formák mellett újak jelenhetnek meg.

[5] https://datareportal.com/reports/digital-2021-october-global-statshot, (2021. 11. 20.)
[6] https://hvg.hu/tudomany/20211004_leallas, (2021. 11. 20.)
[7] Lásd például: Gáspár Zsolt: Crytocurrencies & Cybercrimes: The criminal aspects of crypto assets. In: Bujtár, Zsolt; Szívós, Alexander Roland; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics, Botond (szerk.) Kriptoeszközök világa a jog és gazdaság szemszögéből : Konferenciakötet - Válogatott tanulmányok. Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, 2021. pp. 99-105.

1. Az adathalászat és az identitáslopás

Hagyományosan az adathalászat e-mailek elküldésével történik, de napjainkban egyre több phising kísérlet van a szociális hálókon is. Az egyik ilyen formája az ún. social phising (közösségi adathalászatnak) játékos applikációkon keresztül. Ezek az alkalmazások egy rövid pár perces szórakozást ígérnek a gyanútlan felhasználóknak, néhány kérdés megválaszolásáért cserébe megtudhatják, például, hogy kik voltak előző életükben, mi lenne az indián nevük, vagy mennyire minősülnek intelligensnek. Az alkalmazások használatával számos engedélyt megadunk, így hozzáférhetnek a személyes profilunkhoz és adatainkhoz, amelyekkel a jövőben visszaélést követhetnek el a bűnözők. Az ilyen jellegű applikációk veszélyessége abban is rejlik, hogy sok esetben a barátok vagy ismerősök hívják meg a felhasználót, hogy próbálja ki azt, és így az futótűzként terjedhet és gyűjthet adatok, szemben az e-mailen történő adathalászattal szemben. Növelheti az elterjedését az ún. FOMO (Fear Of Missing Out) pszichológiai jelenség is, amely a népszerű alkalmazások használatából való kimaradást jelenti e körben. Nem csak az alkalmazások, hanem a csaló, vírusos, ígéretekkel teli linkek is gyorsan terjedhetnek a közösségi médián. A csaló elkövetők akár belépési kódokat is megszerezhetik az adathalászat tevékenységükkel, ami anyagi és személyiségi károkat tud okozni a felhasználóknak.

Az adatokkal való visszaélés egyik különös formája az ún. identitáslopás. Magyar szakirodalomban többféleképpen nevezik ezt a jelenséget. Eszteri Dániel és Máté István Zsolt közös tanulmányában az identitáslopás terminust használja a virtuális valóságot szimuláló *„Second Life”* nevezetű szoftverben elkövetett deliktumok kapcsán.[8] Hámori is ezt a szakkifejezést használja, és a definíciójának középpontjában a személyes adatok jogellenes megszerzése áll: *„egy személy adatainak (név, születési év, lakcím, hitelkártya-azonosító, taj-szám és más személyes adatok, illegális eltulajdonítása azzal a céllal, hogy azokat különféle tranzakciókban anyagi előnyszerzésre használják az autóbérléstől a bankhitel felvételéig.”*[9]

Haig Zsolt a fentivel ellentétben személyiséglopás terminológiát alkalmazza. Scwhartau könyvére[10] hivatkozva a személyiséglopást az információs hadviselés, azon belül a személyes információs hadviselés kategóriájába sorolja. A bűncselekmény megvalósulása esetén az

[8] Lásd bővebben: Eszteri Dániel – Máté István Zsolt, 2017: Identitáslopás a virtuális világban. In: Belügyi Szemle 3. szám, pp. 79-107.
[9] Hámori Balázs, 2004: Bizalom, jóhírnév és identitás az elektronikus piacokon. In: Közgazdasági Szemle,9. szám, pp. 832-848.
[10] Schwartau, Winn, 2010. Information warfare. Kindle e-book edition. New York, Interpact Press Inc, Location 163.

áldozatok anyagi és emberi méltóságot érintő károkat szenvedhetnek.[11] Sorbán Kinga a személyazonosság-lopás szakkifejezést használja.[12] Szerinte ennek a bűnözési formának két mozzanata van. Az első fázisban a bűnelkövető eltulajdonítja az áldozat személyes adatait (pl.: Taj számát). A második fázis az adatok visszaélésszerű használatáról szól. Rámutat, hogy a magyar Büntető Törvénykönyv nem tartalmaz speciális tényállást, és véleménye szerint erre nincs is szükség, mert az ezzel kapcsolatos magatartások beilleszthetők már meglévő tényállásokba (pl.: személyes adattal visszaélésnek minősülhet).[13] Több angolszász államban speciális törvényi tényállásként szabályozzák az identitáslopást.[14] A közösségi médián az identitáslopás sok esetben azt jelenti a gyakorlatban, hogy a bűnelkövető vagy más személynek a felhasználói fiókjával tesz meg jogellenesen jognyilatkozatokat, vagy másnak a nevével, fotóival készítenek hamis felhasználói fiókokat akár vagyoni haszonszerzés végett, akár a másik személynek a jó hírnevének lerombolása céljából. De az identitáslopás nemcsak emberek, hanem akár jó hírnévvel rendelkező cégekkel szemben is történhet (ún. üzleti identitáslopás), amivel hamis hirdetéseket és egyéb csalásokat tudnak megvalósítani a bűnözők.

Péterfalvi Attila és Eszteri Dániel írja közös tanulmányukban, hogy Magyarországon is emelkedik az olyan bejelentések száma, ahol arra tesznek panaszt az emberek, hogy fényképeik felhasználásával a közösségi portálokon álprofilt hoznak létre bűnelkövetők. A hazai jogesetekben is az elkövetők elsődleges célja a sértett lejáratása vagy jó hírnevének rontása szokott lenni. Megállapításuk szerint az ilyen esetekben a Btk. 219. szakaszában a személyes adattal visszaélés tényállásában megfogalmazott „jelentős érdeksérelmet okozva" feltétel fennáll. A Nemzeti Adatvédelmi és Információszabadság Hatóságnak is lehetősége is van hivatalból feljelentést tenni, ha bűncselekményt észlel. Péterfalvi és Eszteri emellett még példaként emeli ki azt a jogesetet, ahol egy adatbázist hoztak létre elkövetők homoszexuális és egyéb másságú emberekről egy honlapon, ahol a nevük úgy szerepelt, hogy közvetlenül rá lehetett kattintani a személyek facebook profiljára.[15]

---

[11] Haig Zsolt, 2011: Az információs hadviselés kialakulása, katonai értelmezése. In: Hadtudomány, a Magyar Hadtudományi Társaság Folyóirata. 1-2. szám, p. 14.

[12] Sorbán Kinga, 2015: Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói. In: Themis: 1. szám, pp. 343-375.

[13] Sorbán Kinga: Az informatikai... i. m. pp. 369-370.

[14] Tóth Dávid, 2020: Személyiséglopás az interneten. In: Büntetőjogi Szemle. 1. szám pp. 113-119.
Tóth Dávid, 2020: Az identitáslopás szabályozása angolszász államokban. In: Baráth, Noémi Emőke; Mezei, József (szerk.): Rendészet-Tudomány-Aktualitások: A rendészettudomány a fiatal kutatók szemével 2020. Doktoranduszok Országos Szövetsége, Budapest 2020. pp. 228-237.

[15] Eszteri Dániel – Péterfalvi Attila 2017: A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata In: Görög, Márta; Menyhárd, Attila; Koltay, András (szerk.): A személyiség és védelme: Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül. ELTE ÁJK, Budapest, pp. 405-420.

A fenti adatvédelmi veszélyek miatt is fontos az emberek folyamatos tájékoztatása akár a közösségi média felületein is , hogy ne váljanak a jövőben áldozattá. Másik oldalról felelőssége van a szociális média szolgáltatóknak is, hogy minél hamarabb, lehetőleg már a hamis profil létrehozásakor meggátolja az ilyen incidenseket. Az állam részéről pedig fontos a büntetőjogi védelem biztosítása, így például a személyes adattal visszaélés bűncselekmény hazánkban.[16] Emellett proaktivitásra hívja fel a figyelmet, a NAIH azt javasolva, hogy a közösségi oldalakon megvalósuló személyes adattal való visszaélések kapcsán tegyenek feljelentést a sértettek.[17]

2. A pedofília

A pedofília jelensége nem elsősorban a közösségi médián, hanem pornográf tartalmakat megosztó oldalakon, illetve a sötét weben terjed. Ez a megállapítás ugyanakkor nem jelenti azt, hogy a közösségi médiát a pedofil elkövetők ne használnák arra, hogy kiskorú áldozatokat találjanak meg, illetve figyeljenek meg. A szociális hálók a pedofil elkövetők számára is tudnak segítséget nyújtani. Így tett sokáig a YouTube is, amelynek ajánlórendszer-algoritmusa tette lehetővé, hogy kiskorú gyermekek fürdőruhás videóit nézzék meg. A videómegosztó oldal így hozzájárul ahhoz, hogy pedofil vonzerőt tartalmazó képfelvételekhez hozzájussanak az elkövetők. Az oldal azóta fejlesztéseket eszközölt az algoritmuson, hogy a jövőben ilyen visszaélések ne történjenek meg. A legtöbb közösségi oldal tiltja a 14 év alatti felhasználók számára, hogy regisztráljanak az oldalon, de a regisztráció során nem kell bizonyítani az életkor, így nagyon sok gyermek is regisztrál az oldalakon, ami számukra veszélyforrást jelenthet.[18] Szintén probléma lehet, ha álprofilok segítségével próbálnak kapcsolatba lépni a kiskorú személyekkel, amelynek vége akár súlyos bűncselekmény megvalósulása (emberrablás, szexuális erőszak, emberölés) is lehet.

3. A terrorizmus és szervezett bűnözés

Bányász Péter az alábbiakat emeli ki, hogy mire használják a terroristák a közösségi hálózatokat:

- egymással történő kommunikálásra, kapcsolattartásra,

[16] Lásd bővebben: Gál Andor, 2020: A GDPR hatása a büntető anyagi jogra: a személyes adattal visszaélés tényállásának jövőjéről In: Hollán, Miklós – Mezei, Kitti (szerk.): A büntetőjog hazai rendszere megújításának koncepcionális céljai és hatásai. Társadalomtudományi Kutatóközpont Jogtudományi Intézet, Budapest. 2020. pp. 133-146.
[17] Eszteri – Péterfalvi: A személyes… i. m. p. 412.
[18] Bányász Péter: Kiberbűnözés… i. m. p. 67. o.

- információszerzésre,
- propaganda tevékenység kifejtésére,
- tagtoborzásra,
- szimpatizánsok megszerzésére,
- pszichológiai hadviselésre,
- kibertámadásokra.[19]

Utóbbiak irányulhatnak létfontosságú infrastruktúrák ellen is.[20]

Serbakov Márton ír tanulmányában arról, hogy erőszakos extrémista csoportok, elsősorban radikális fiatalok használják a közösségi média chatszobáit (Facebook, YouTube, Twitter stb.) kommunikációra. Számos terrorista szervezet, köztük az Iszlám Állam is felfedezte, hogy a közösségi média elősegítheti a tevékenységet számos módon.[21]

Szervezett bűnözői csoportok is használják a fenti hasonló célokra a közösségi médiát. Elsősorban a darkneten foglalkoznak kábítószer-kereskedelemmel és illegális vadkereskedelemmel, de a legnagyobb közösségi médián is jelentek meg már ilyen jellegű hirdetések.

4. Közösségi médián megvalósuló csalások

A nagy közösségi portálok népszerű elkövetési helynek minősülnek a kiberbűnönözők számára. A sok aktív felhasználó potenciális préda a csaló elkövetők számára, még akkor is, hogyha számos elkövetésük már kísérleti szakban megreked, a befejezett bűncselekmények nagy profitot hozhatnak.

Napjainkban számos fajta csalási módszerrel[22] élnek az elkövetők a közösségi hálókon így például:

- *adathalászat*. Hagyományosan a phising e-mailben szokott történni, de napjainkban számos elkövetők kártevő linkekkel bombázza a felhasználókat, akiknek a profilja tovább küldheti az adathalász Url-hivatkozásokat így fokozva a problémákat. Az adathalászat célja, hogy bizalmas információkat szerezzenek meg az elkövetők (pl.:

[19] Bányász Péter, 2017: Kiberbűnözés és közösségi média. In: Nemzetbiztonsági Szemle (online) 4. szám p. 71.
[20] Bányász, Péter, 2013: Dangers of social media through the example of the Arab Spring. In: Európai szellem / European Spirit. pp. 20-32. Dangers_of_social_media_through_the_exam.pdf (mtak.hu) (2021. 11. 01.)
[21] Lásd bővebben Serbakov Márton Tibor, 2020: Legújabb tendenciák a terroristák internethasználatát illetően. In: Büntetőjogi Szemle 2. szám pp. 122-139.
[22] Lásd például: Gáspár Zsolt: Piramisjátékok szervezése az online térben. In: Baráth, Noémi Emőke; Mezei, József (szerk.) Rendészet-Tudomány-Aktualitások : A rendészettudomány a fiatal kutatók szemével 2020. Budapest, Doktoranduszok Országos Szövetsége (DOSZ), 2020. pp. 78-85.

profilba történő belépés, vagy bankszámlához kapcsolódó információkat) hogy később visszaéléseket tudjanak megvalósítani.

- *Romantikus csalások.* Az ilyen jellegű elkövetési módok célja, hogy az emberek érzelmeit és naivitását kihasználva elnyerjék az áldozat bizalmát társkeresési eszközökkel (pl.: hízelgéssel). Már a facebooknak is van társkereső funkciója, ahol az elkövetők létrehozhatnak hamis profilokat és valósíthatnak meg romantikus csalásokat. Az áldozat bizalmának megszerzése után gyakran pénzt kérnek, és utána köddé válnak. A pénz kérésének hamis indoka szokott lenni, hogy segítségre van szükségük mivel megélhetési gondjaik lettek. A romantikus csalások kapcsán Gyaraki Réka végzett viktimológiai kutatást Magyarországon, amely alapján az áldozatok 93%-a nő, akiknek jelentős része az idős korosztályhoz tartozik. A bűnelkövetők orvosnak, mérnöknek vagy katonának adták ki magukat, hamis fényképekkel álcázva magukat.[23]
- *Hamis álláshirdetések.* Az álláskereső emberek kiszolgáltatott helyzetével való visszaélés is gyakori jelenség a közösségi média felületeken. A jól fizető állásajánlatokért cserébe személyes adatokat szoktak kérni az elkövetők (pl.: lakcímét, társadalombiztosítási számot, útlevél másolatot stb.).
- A fentiek mellett még ki lehet emelni az ún. „ön nyert" csalásokat, a vásárlási csalásokat, és a hamis jótékonysági csalásokat példálózó jelleggel.

5. Rémhírterjesztés

A közösségi médián megjelent az ún. *fake news j*elenség, amikor hamis híreket terjesztenek emberek különféle célokból. Ennek egyik társadalomra veszélyes formája a rémhírterjesztés. A járványhelyzet alatt szigorítottak is a rémhírterjesztés tényállásán. Ennek ellenére a bűnügyi statisztikában a járványhelyzet alatt nem nőtt a rémhírterjesztések száma, 2020-ban és 2021-ben is négy regisztrált esetet találunk.

6. Online zaklatások (cyberbullying)

[23] Gyaraki Réka, 2021: A közösségi média hatása a kiberbűncselekmények elkövetésére. In: Magyar Rendészet 2. szám, p. 77.

A virtuális térben megvalósuló online zaklatásokról már számos tanulmány, monográfia[24] jelent meg már hazánkban az elmúlt években. A cyberbullying egyik fő terepe a közösségi oldalak.
A cyberbullying egyik veszélyessége abban nyilvánul meg, hogy tartós és állandó jelleggel valósulhat meg, amely elől nem lehet könnyedén elmenekülni. A digitális eszközök a nap 24 órájában azonnali és folyamatos kommunikációt tesznek lehetővé az emberek számára, így az internetes zaklatásban szenvedő gyermekek számára nehéz lehet megoldást találni. Emellett a legtöbb elektronikusan közölt zaklató jellegű bejegyzések állandóan folyamatosan jelen lehetnek, akár a nyilvánossággal is meg lehetnek osztva.
Sokszor nehezen észrevehető, vagy amikor már észlelik az áldozatban jelentős lelki-testi traumák jelentkeznek. Szignalizáció esetén is sok esetben a szülők elbagatellizálják a probléma súlyát.

IV. Összegzés

A jelen tanulmány céljának megfelelően bemutatásra kerültek az elmúlt évtizedben a közösségi média hatására megfigyelhető változások és ezzel összefüggésben a bűnözési formák átalakulása is. A szakcikk nem kimerítő jelleggel mutatja be a közösségi médián megvalósuló bűncselekményeket, csak példálózó, illetve gondolatébresztő jelleggel sorolja fel a gyakori bűnelkövetési módokat.
A közösségi médián megvalósuló bűnözési formák egyik közös jellemzője, hogy könnyen megvalósíthatóak, szemben a hagyományos bűnelkövetésektől. Sokkal egyszerűbb egy hamis facebook profilt létrehozni, mint hamis okiratokat készíteni, majd valós térben visszaéléseket elkövetni.

[24] Lásd a témáról: Domonkos, Katalin, 2018: Az online zaklatás, mint az iskolai agresszió egyik fajtája. Takács Etel Pedagógiai Alapítvány, Budapest.
Englander E K – Donnerstein E. – Kowalski R. – Lin C. A. –Parti Katalin, 2017: Defining cyberbullying. In: Pediatrics 11. szám. pp. 148-151.
Kulcsár Gabriella, 2021: A digitális reziliencia jelentősége a cyberbullying elleni küzdelemben. In: Nagy, Melánia (szerk.): Gyerekekre fókuszálva. Konferenciakötet. Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, Pécs. pp.136-145.
Monori Zsuzsanna, 2016: Zaklatás-e a cyberbullying?: Az internetes zaklató magatartások büntetőjogi szankcionálásának dilemmái. In Medias Res: folyóirat a sajtószabadságról és a médiaszabályozásról: 2. szám, pp. 246-261.
Parti Katalin – Schmidt Andrea – Néray Bálint, 2018: Cyberbullying in Hungary. In: Anna, Kostanza Baldry – Catherine Blaya – David P. Farrington (szerk.): International perspectives on cyberbullying. Springer International Publishing, Palgrave Macmillan, Cham. pp. 205-229.
Parti Katalin, 2015: Cyberbullying, Bitcoin, Silk Road, Darknet, TOR: Az internetes bűnözés tárgyában tartott nemzetközi konferenciák kurrens témái 2014-ben. Ügyészek lapja 1. szám, pp. 71-85.
Pongó Tamás, 2021: A cyberbullying és a diákok véleménynyilvánítási szabadsága, különös tekintettel az USA jogrendszerére. Iurisperitus Kiadó, Szeged.

A közösségi médián történő bűncselekmény nagymértékű visszaszorítása csak akkor lehetséges, ha valamennyi oldal tevékenyen hozzájárul a prevencióhoz. Meglátásom szerint ebben elsődleges felelőssége a közösségi média szolgáltatóknak van, hogy a különböző bűnözési formákat (csalásokat, becsületsértéseket, rémhírterjesztéseket stb.) észleljék, és azokat jelentsék, illetve formától függően eltávolítsák. Ebben nagy segítséget jelenthet a mesterséges intelligencia technológiai fejlődése. A mérleg másik nyelve felveti természetesen azt a problémát is, hogy az ilyen szolgáltatók mekkora mértékben végezhetnek ilyen jellegű prevenciós megfigyeléseket. A nyilvános bejegyzések, hirdetések stb. esetén nem lehet kétséges a proaktív jellegű intézkedések elvárása, de vajon a privát beszélgetésben megjelenő bűnözési formákat ki lehet-e szűrni úgy, hogy az emberek magánszférához való joga ne sérüljön? Ennek megválaszolására még jövőben kutatások szükségesek.

Másik oldalon az államnak és a jogalkalmazó szerveknek felelőssége, hogy a közösségi médián megjelenő bűnözési formákról tájékoztassa, illetve oktassa az állampolgárokat, büntetni rendeljék az elkövetési magatartásokat, és érvényesítse a büntetőhatalmát a társadalomra veszélyes cselekmények ellen. Az oktató, tájékoztató tevékenységben civil szervezetek is szerepet játszhatnak.

Végezetül a prevenció oldalán fontos, hogy a közösségi médiát használók is tudatosan kezeljék profiljukat.