ELTE | ÁJK
ÁLLAM- ÉS JOGTUDOMÁNYI KAR

ELTE LAW WORKING PAPERS
2023/05

Szabályozási és túlszabályozási kérdések a digitális pénzügyi rendszerben II. – A technológiai háttérrel összefüggő kihívások

Demjén Anna Katalin

DOI: 10.58360/20231211-Demjen-2

Demjén Anna Katalin[*]

DOI: 10.58360/20231211-Demjen-2

Absztrakt

Az írás egy szemléltető jogeset bemutatásán keresztül azt vizsgálja, hogy az információs technológiai fejlődés (például a blokklánc-technológia vagy különböző biometrikus azonosító eszközök fejlesztése) milyen technológiai kihívások elé állította a digitális pénzügyi rendszert, illetve hogy e kihívásokra milyen gyakorlati és szabályozási megoldásokkal reagáltak, illetve reagálhatnak a későbbiekben a változás által leginkább érintett szereplők.

A múlt század második felétől kezdve rendkívüli gyorsasággal szaporodó információs technológiai fejlesztések eredményei mára már az átlagemberek mindennapjainak részét képezik. A legifjabb generáció tagjai számára már természetes, hogy biometrikus azonosító eszközökkel férnek hozzá a személyes adataikhoz és a bankszámlapénzükhöz is, illetve ezek segítségével bonyolítanak tranzakciókat, anélkül, hogy el kéne hagyniuk az otthon kényelmét. Természetesen róluk sem jelenthető ki, hogy átlátnák az általuk használt rendszerek működését és e rendszerek használatában rejlő kockázatot. Az informatika és a pénzügyi rendszerek mára olyan erősen összefonódtak, hogy adott esetben szakmailag képzett és kifejezetten elővigyázatos személyek sem képesek megvédeni magukat az egyre népszerűbb és praktikusabb technológiák használatával járó veszélyektől. Az írás mégis megkísérli, hogy néhány konkrét példával is illusztrálva érthetőbbé tegye a kapcsolatot a pénzügyi rendszer és a blokklánc-technológia vagy a biometrikus eljárások között. Emellett rámutat, hogy a technológiai fejlesztések nyomán átalakuló erőviszonyok miként befolyásolhatják a pénzügyi rendszer alakulását.

Az információs technológia exponenciális fejlődése következtében aligha számít túlzásnak a metaverzum említése, hiszen a párhuzamos valóságok felhasználói élményét fokozó fejlesztések sokasága valósul meg mindennapi életünkben. A metaverzumra ma már nem mint egy számítógépes játékokhoz kapcsolódó, szűk körben ismert fogalomra tekintenek, hanem mint olyan kiaknázandó vívmányra, amely a korábban sosem tapasztalt – informatikai értelemben vett – „átjárhatóság" által könnyen rekonstruálja a fizikai világot és elmossa a földrajzi határokat, ezáltal új lehetőségeket teremtve az oktatásban, a turizmusban, az egészségügyben, a társas érintkezésben, a közösségi médiában, a gazdaságban és a kommunikációban; legfőképpen azonban a biometrikus azonosítással

[*] Anna Katalin Demjén, PhD Student, Center for Theory of Law and Society, Faculty of Law, Eötvös Loránd University, Budapest. ORCID-number: 0009-0003-0757-7830.

kapcsolatban fontos említenünk a szerepét.[1] Mivel a metaverzum egy párhuzamos és független digitális gazdaságot hoz létre, a felhasználók számára fontos lehet, hogy az ott létrehozott profiljuk hozzákapcsolható legyen valamilyen módon a személyükhöz – hasonlóan ahhoz az igényhez, amely a bankszámlapénzünk távolról történő használata során jelentkezik. Bizonyos adatok, a biometrikus adatok használata lehetővé teszi az egyes személyek azonosítását a csupán egyedileg rájuk jellemző viselkedési vagy fizikai sajátosságok statisztikai elemzése alapján (arcfelismerés, retinaszkennelés, ujjlenyomat-olvasás, DNS-teszt stb.) a legfejlettebb technológiák pedig már illatok, vagy az érhálózat egyedi sajátosságai alapján is képesek különbséget tenni és egyre inkább védettek a csalások ellen az ún. élőségérzékelés fejlődésének következtében.

Azonban az élőségérzékelés sem tökéletesen kiforrott módszer, tehát korántsem arról van szó, hogy ez a technológia bármilyen hamisított felvételt ki tudna szűrni. Hatékonyan képes például észlelni azt, ha egy, az arcunk elé tartott maszk segítségével próbálunk videós azonosítást végrehajtani, de bizonyos esetekben teljesen tehetetlen, például az ún. *deepfake* technológiával létrehozott, nagyon magas minőségben megalkotott digitális anyagok még gyakran képesek kijátszani ezt a rendszert is. Az ilyen anyagok létrehozásához nagy mennyiségű adat felhasználására van szükség, amelyek megszerzése számos legális vagy illegális módszerrel történhet, ideértve az interneten valakiről elérhető felvételek felhasználásától a fizikai kényszer alkalmazásáig szinte bármit, azonban a lényeg változatlan: a személyazonosítással megbízott mesterséges intelligenciák átverhetők. A élőségészleléshez hasonló technológiák további fejlesztésének hatására a jövőben a decentralizált fizetések és a biometrikus azonosítás összekapcsolódásával talán valóban gördülékenyebben létrejöhetnek és működhetnek az egyének közti szerződések és tranzakciók, de egyelőre a technológia biztonságát és a jogi szabályozottságot tekintve is adódnak problémák, tehát ezek a rendszerek és felhasználóik továbbra is ki vannak téve a jogi rendezetlenség és a technológiai hiányosságok okozta különböző incidenseknek. Komoly kérdést jelent, hogy arányban áll-e konkrét esetben néhány másodpercnyi idő megspórolása azokkal a kockázatokkal, melyeket a kényelem érdekében a technológiának való kiszolgáltatottsággal vállalunk.

A személyiséglopás jelensége például egyes statisztikák szerint minden tizenötödik embert érinti, sőt, ez a szám egyre növekszik annak következtében, hogy egyre több és több személyes adatot osztunk meg online.[2] A koronavírus járvány és annak nyomán rohamosan terjedő elektronikus ügyintézés és általánosságban a fokozódó online jelentlét sem segítette az adatok javulását. Más kimutatások alapján az USA lakosságának 33%-a vált már személyiséglopás áldozatává, melynek legnagyobb része bankkártyákkal

[1] *The Role of Biometrics in the Metaverse*. In Cointelegraph, https://cointelegraph.com/learn/the-role-of-biometrics-in-the-metaverse (Utolsó letöltés időpontja: 2023.07.01.)
[2] Jenifer Kuadli: *15 Insane Identity Theft Statistics to Keep In Mind in 2023*. In Legaljobs, https://legaljobs.io/blog/identity-theft-statistics (Utolsó letöltés időpontja: 2023.07.01.)

DOI: 10.58360/20231211-Demjen-2

elkövetett visszaéléssel kapcsolatos.[3] A Facebook-os *stablecoin*, a Diem létrehozásának tervei is erősen összekapcsolódnak egy új metaverzum kialakításának projektjével, melyben a közösségi média felhasználói földrajzi korlátokra és eltérő anyagi lehetőségeikre tekintet nélkül lennének képesek akár globális munkavégzésre, kereskedelemre, egyéb tevékenységekre. Tekintettel arra, hogy a Facebook egyes számítások szerint már több mint 3 milliárd felhasználóval rendelkezik – azaz a 15 év feletti lakosságnak nagyjából a felét el tudja érni szolgáltatásaival – jó esélye lehet arra, hogy az egységes metaverzum létrehozását is végül a nevéhez kapcsolják, bár e tekintetben igen szoros a verseny. Nagy a nyomás ugyanis az Apple, a Google és a Microsoft oldaláról, amelyeknek az idők során talán kevésbé erodálódott a jó hírnevük az adatvédelemmel és biztonsággal kapcsolatos ügyek során. A Facebook közös szupervalutájának gondolata rögtön alkalmat adott a Cambridge Analytica adatelemző cég nevével fémjelzett adatszivárgási ügy felemlegetésére, illetve arra is, hogy általánosságban átgondoljuk azt, mennyire szerencsés az, ha egy, az adataink felhasználási jogának értékesítésére épülő platformra helyezzük át a pénzügyeink irányítását – illetve a jövőben, a metaverzum-élmény megéléséhez szükséges materiális háttér fejlesztésének előrehaladtával a „másodlagos" identitásunkat – is.

A digitális pénzügyi rendszert érintő főbb technológiai kérdések

A globális digitális pénzügyi rendszert érintő megoldandó problémák közt említhető továbbá, hogy a kriptoeszközök által használt DLT, azaz elosztott főkönyvi technológia még ma sem kikezdhetetlen, tehát nem csupán az ilyen pénzügyi eszközök rendezetlen jogi helyzete okoz fejtörést, hanem informatikai oldalról is számos veszély fenyegeti, melyeket alább részletezünk.[4] A kibertámadások célpontjai természetesen hagyományos bankok is lehetnek, ám a szabályozott keretek által biztosított tőkemegfelelési garanciák, illetve a bankok által alkalmazható, jogszabályban engedélyezett kemény biztonsági intézkedések jelentősen mérséklik az ilyen támadások által jelentett valós kockázatokat. A kriptovaluta ágazat totális ellenzői részéről persze rendszerint elhangzik, hogy óriási kockázatot vállalnak azok a bankok, amelyek kriptós befektetők számára is nyújtanak szolgáltatásokat, míg a szektor fennmaradásában érdekeltek általában a szándékos ellehetetlenítési kísérleteknek tudják be a kriptoeszközök piacán keletkező erőteljes hullámokat.[5] Az első és legismertebb kibertámadás a Bitcoint érte 2010-ben, melynek során három különböző számlán 184 milliárd Bitcoint hozott létre magának egy hacker. A hibát a fejlesztők hamar észrevették és törölték, s a technológia azóta is híres a biztonságosságáról, azonban folyamatosan érik kihívások hackerek, csalók és különböző

[3] Julija Andjelic: *Most Worrying Identity Theft Statistics for 2023*. In Fortunly, https://fortunly.com/statistics/identity-theft-statistics/#gref (Utolsó letöltés időpontja: 2023.07.01.)
[4] Joshua Esan: *Blockchain Security: Preventing Fraud on Distributed Ledger Technology*. In Cointelegraph, https://cointelegraph.com/news/blockchain-security-preventing-fraud-on-distributed-ledger-technology (Utolsó letöltés időpontja: 2023.07.01.)
[5] Nic Carter: *Operation Choke Point 2.0 Is Underway, and Crypto Is in Its Crosshairs*. In Pirate Wires, https://www.piratewires.com/p/crypto-choke-point (Utolsó letöltés időpontja: 2023.07.01.)

DOI: 10.58360/20231211-Demjen-2

célú internetes átverések formájában. A Wall Street Journal adatai szerint 2019-ben több mint 4 milliárd dollárnyi veszteséget okoztak a felhasználók számára a kriptovaluta csalások.

A blokklánc technológia biztonságosságát az egyedileg titkosított kódot használó felhasználók közötti kapcsolat közvetlensége (P2P), a bányászati technológia érvényessége és a főkönyv megváltoztathatatlansága biztosítja. A csalások tehát ezeken a pontokon próbálják kikezdeni a rendszert. Például az ún. 51% támadások arra építenek, hogy ha egy adott kriptovaluta bányászásához szükséges informatikai erőforrás több mint felét ugyanaz az érdekkör birtokolja, akkor az képes új költéseket írni a főkönyvbe valódi kiadás nélkül. Ennek következtében képes duplán költeni, ezáltal manipulálni az egész hálózatot, s akár az egész valutát bedönteni. Ez történt például 2018-ban a Bitcoin Golddal is, melyből hetvenezer dollárnyi értékben költöttek duplán, ezért törölték is arról a kriptotőzsdéről, amelyen először megjelent.

A szelfizős és nagyon sok más, biometrikus azonosításra épülő ügyfél-hitelesítés alkalmazásának tágabb értelemben vett technológiai jellegű veszélyei közé tartozik az is, hogy még a lehető legbiztonságosabb módszerrel tárolt elektronikus azonosítót is egyszerűen kiadhatja a kezéből az ügyfél anélkül, hogy komolyabb hackertámadás alá vennék az informatikai eszközeit.[6] Az adathalászat (*phishing*) ugyanúgy történik a kriptoeszközök és különböző digitális pénztárcák esetén is, mint a „hagyományos" csalásoknál: a felhasználókat az általuk igénybe vett szolgáltató által küldött e-mailhez vagy a hivatalos honlaphoz hasonló utánzattal próbálják rávenni az adataik kiadására. A Sybil támadások viszont inkább informatikai jellegűek, több hamis identitást hoznak létre a hálózaton, amely végső soron a rendszer összeomlását okozza, illetve a hackerek képesek a P2P hálózaton az internetszolgáltató felé továbbított adatok megszerzésére is, így miközben a felhasználó felé úgy tűnik, hogy rendben zajlanak a folyamatok igazából párhuzamos blokklánc jön létre. A kriptovaluták alapvető természetéhez kapcsolódik továbbá egy másik gyakorlat, az ún. *shilling* is. Ez azt jelenti, hogy különböző fórumokon, nagy nézettségű online felületeken az adott kriptoeszköz birtoklói olyan információkat osztanak meg és/vagy terjesztenek, amelyek az adott eszközre nézve kedvező piaci helyzetet vázolnak, leegyszerűsítve mindenféle gazdasági folyamat elemzését nélkülözve népszerűsítik azt. Mivel ezeknek a pénzügyi eszközöknek az értéke – ahogyan azt korábban részleteztük – erősen függ a beléjük vetett bizalomtól (vagyis a törvényes fiat valuta vagy más értékmérő mennyiségétől, amit a birtoklói adott időben belefektetnek), ezért az ilyen típusú megtévesztések sokszor hatalmas veszteségeket (egy szűkebb kör számára pedig hatalmas nyereségeket) képesek előidézni. A felelősség kizárására ezért a kriptotőzsdék üzemeltetői a DYOR rövidítést *(do your own research)* szokták bevetni és hangoztatni, amely még az internetes tévinformációk virágkorában terjedt el, és annyit jelent, hogy minden felhasználó tájékozódjon saját maga az aktuális pénzügyi vagy egyéb

[6] Tatyana Shcherbakova: *Selfie Hunting: Think Twice Before Confirming Your Identity*. In Kaspersky Daily, https://www.kaspersky.com/blog/selfie-with-id-card-scam/27926 (Utolsó letöltés időpontja: 2023.07.01.)

DOI: 10.58360/20231211-Demjen-2

hírek valóságtartalmáról, soha ne fektessen be semmibe pusztán azért, mert az interneten néhány népszerű bejegyzés ezt tanácsolja. Ez a tanács igen ambivalens érzéseket idéz elő egy olyan területen, amelynek vezető szoftverfejlesztő informatikusai sem mindig tudják kétséget kizáróan és egybehangzóan megállapítani, hogy egy adott valuta árfolyama manipulálva van-e, vagy hogy miért zuhan be egy olyan valuta, amelynek a programozása alapján ez elviekben lehetetlen lett volna. Mindenesetre a fent említetteken kívül még számos kreatív technológiai megoldást fejlesztettek és fejlesztenek a mai napig a digitális pénzügyi rendszerek támadására, és tekintve a minimális lebukási és szankcionálási kockázattal összevetett potenciális elérhető nyereséget, feltehetőleg ez a típusú „verseny" a fél-legalitásban működő kriptotőzsdék és a hackerek közt addig tart majd, ameddig a szabályozási környezet – akár a technológia módosított felhasználásával párhuzamosan – nem változik radikálisan.

Az egyik legfontosabb és leghatékonyabb intézkedés, amely technológiai oldalról bevethető az adathalászat elleni szoftverek, illetve internetkapcsolattal nem rendelkező ún. „hideg" kriptopénztárcák mellett a kétlépcsős hitelesítési rendszer (2FA), melyet számos vállalat használ már a digitális szolgáltatásnyújtáshoz. Ennek lényege, hogy a digitális eszközhöz általában használt jelszó (például internetbank bejelentkezési jelszó, e-mail fiók jelszava vagy kriptopénztárca jelszava) beírása után egy bizonyítottan hozzánk tartozó független eszközre egyszer használatos jelszót (OTP) küld a szolgáltató, melyhez elméletileg csak nekünk van hozzáférési jogosultságunk, illetve a jelszó felhasználására rendelkezésre álló időkeret is a visszaélések kivédhetőségét fokozza. Tulajdonképpen ennek a kétfaktoros azonosításnak a használatát írta elő a PSD2 az ún. erős ügyfél-hitelesítés (SCA) kötelezővé tételével. Ezt ma a 26/2020. (VIII. 25.) MNB rendelet definiálja az EU-s előírásokkal összhangban a következőképpen: „Erős ügyfél-hitelesítés: hitelesítés legalább két olyan
a) ismeret, azaz csak az ügyfél által ismert információ,
b) birtoklás, azaz csak az ügyfél által birtokolt dolog, és
c) biológiai tulajdonság, azaz az ügyfél jellemzője
kategóriába sorolható elem felhasználásával, amely kategóriák egymástól függetlenek annyiban, hogy az egyik feltörése nem befolyásolja a többi megbízhatóságát, és az eljárás kialakítása révén biztosított az azonosítási adatok bizalmassága."[7]

A biometrikus azonosítás és az erős ügyfél-hitelesítés kapcsolata

Eleinte még jellemzően SMS-ben történtek a megerősítések (a telefon, mint birtokolt dolog biztosította az ügyfél azonosságát), azonban később, ahogy a különböző mobileszközökön egyre elterjedtebb biztonsági megoldássá vált a biometrikus adatokkal (ujjlenyomat, arcfelismerés) történő azonosítás, lehetővé vált az is, hogy az okoseszközünkre telepített banki, vagy harmadik fél szolgáltató programján keresztül ujjlenyomattal vagy arcfelismeréssel indítsunk fizetéseket. Az ilyen technológiai

[7] 26/2020. (VIII. 25.) MNB rendelet 2. § 4. pont

DOI: 10.58360/20231211-Demjen-2

szolgáltatásokat nyújtó óriásvállalatok, például az Apple, a Google vagy a Microsoft – amelyek például részletfizetési és egyéb pénzügyi szolgáltatásokat is képesek magas színvonalon nyújtani az ügyfeleiknek – lehetővé teszik digitális pénztárcák létrehozását, aminek segítségével minden, az adott eszközzel párosított bankkártyával a kártyaadatok esetenkénti megadása nélkül fizethetünk.[8] Vagyis fizethet az, akinek a biometrikus adatait az adott okoseszköz arra jogosultként elfogadja. Ez pedig azért problematikus, mert ilyenkor a legtöbb bank, például a kényelmi funkciói és olcsósága miatt hazánkban is nagy népszerűségnek örvendő Revolut esetében is a biometrikus azonosítás által – tehát például Apple Pay vagy Google Pay segítségével – végrehajtott tranzakciók a bank részéről már nem esnek át biztonsági ellenőrzésen, hiszen eleve erős, kétfaktoros azonosítással indították őket. Erre a kiskapura egy teljes csalássorozat épült fel, amelyben a támadók először kinyomozták a bankkártyák adatait, majd a kártyákat más okoseszközökkel is párosították a kártyatulajdonos tudta nélkül. Ezt követően pedig – mivel az erős ügyfél-hitelesítés technológiai oldalát a harmadik fél szolgáltató biztosította – percek alatt gond nélkül el tudták költeni a világ különböző pontjain lévő fiktív üzletekben a számlatulajdonos pénzét, anélkül, hogy a bank a folyamat leállítása, a pénz visszaszerzése, a hamis tranzakciók adatainak kiadása vagy az ügyfél kárpótlása érdekében bármit is tett volna. A fentiek megtételében jogszabályok korlátozták, így az ügyfél által gyanúsnak minősített tranzakciók visszavonását is megtagadták a biometrikus azonosítás tényére hivatkozva.[9] A bank álláspontja is érthető, ugyanakkor az innovációkat övező rugalmas és támogató hozzáállásnak az ügyfelek technológiai szinten felmerülő panaszai esetén mutatkozó teljes hiánya igen fájó. A bankoknak a technológia kikezdhetősége ismeretében jóval segítőkészebben kellene hozzáállniuk a hasonló esetekhez, nem pedig teljes egészében lezárni az ügyet és legfeljebb a büntetőeljárások sikerével kecsegtetni az ügyfelet. A különböző informatikai megoldások lehetővé teszik, hogy gyanús földrajzi helyzet, gyanús kártyahasználati időpont, összeg és/vagy gyakoriság, esetleg szokatlan költési típus esetén további megerősítést kérjen a bank a felhasználótól. Az ilyen rendszerek alkalmazásának megspórolása a biometrikus hitelesítés biztonságosságára hivatkozva a Revolutot ért csalássorozat tanulságainak leszűrését követően nem valószínű, hogy lehetséges lesz a jövőben.

A biometrikus azonosításnak további buktatóit emelik ki a társadalom egy sajátos kategóriájába tartozók csoportja, az ikertestvérek is. Az ikreket a dolgokat, jelenségeket és személyeket nagy vonalakban kategóriákba sorolni törekvő társadalom és az arra épülő jogrendszer eleve nehezen tudja szétválasztani, külön személyként kezelni. Így volt ez még a biometrikus azonosítás korszaka előtt is, és ezért lehetséges, hogy az Egyesült Államokban a mai napig előfordul, hogy a hitelképességet megállapító intézmények nem tudják értelmezni a bejövő adatokat és alaptalanul megtagadják valamelyik ikertől a

[8] *2023-ban új versenytársat kaphat az Apple Pay*. In Fintechzone, https://fintechzone.hu/2023-ban-uj-versenytarsat-kaphat-az-apple-pay (Utolsó letöltés időpontja: 2023.07.01.)
[9] Fekete Emese: *Azonnal lépj, ha ilyen sms-t kapsz – folytatjuk a Revolutról ellopott 800 ezer forint történetét*. In Forbes, https://forbes.hu/penz/revolut-ugy-csalas-folytatas (Utolsó letöltés időpontja: 2023.07.01.)

DOI: 10.58360/20231211-Demjen-2

hitelfelvétel lehetőségét, vagy társadalombiztosítási díjakat számolnak fel többszörösen vagy indokolatlanul és számos egyéb módon sértik és korlátozzák az ikertestvérek alapvető jogait.[10] Az arcalapú azonosításra fejlesztett technológiáknak pedig – bár egyre kevésbé, de továbbra is – komoly kihívást jelent az egypetéjű ikrekéhez hasonló mértékben egyező arcok közötti különbségtétel. Olyannyira, hogy egyes szolgáltatók kifejezetten óva intik az egypetéjű ikreket attól, hogy az eszközeiken (illetve a banki alkalmazásokban) arcalapú azonosítási megoldásokat válasszanak[11] – holott ez a technológia egyre inkább kiszorítja az ujjlenyomat-olvasást a mobileszközök piacán. Az ilyen tévedések jelentősége a „szelfizős" ügyfél-hitelesítés esetén mutatkozik meg, amely során az ügyfél a személyi igazolványának mindkét oldalát és az arcáról készült fényképet küldi meg egy bank számára ügyfél-hitelesítéskor. A rendszer a hitelesítés során is algoritmusokat használ, így például a Binance rendszere (amikor át kellett állniuk erős ügyfél-hitelesítésre az EGT-n belüli és svájci lakóhellyel rendelkező felhasználók esetén) a hitelesítés sikertelensége esetén egy rövid SMS-ben[12] tájékoztatta a felhasználókat ennek tényéről, és arról, hogy amennyiben van ikertestvérük, kérjenek „kézi", azaz nem algoritmus által végrehajtott hitelesítést az ügyfélszolgálaton oly módon, hogy közös videót töltenek fel az ügyfélszolgálatra, melyen mindketten egyszerre tartják kézben a személyi igazolványukat. Amíg nem hitelesítik magukat így, addig az egyikük (jellemzően az, aki időben később próbálta elvégezni a hitelesítést) számlája csak kifizetésre használható (pontosabban a hitelesítésre rendelkezésre álló határidő lejárta után 10 nappal nem veheti igénybe a fiat szolgáltatásokat, a határidő lejárta után 20 nappal nem használhatja a kártyáját sem, és a legtöbb esetben 30, néhány tagállam esetén 60 nappal a határidő lejárta után csak kifizetést tud teljesíteni a kártyáról).[13] A csak kifizetés módba lépett számláknál már önmagában problematikus, hogy ki, hogyan és milyen formában tud kifizetést igényelni, ha a kártya már nem működik és a számlatulajdonos személyazonosságát nem sikerült a hatályos szabályoknak megfelelően megerősíteni. A Binance egyes ügyfeleinél viszont a „csak kiutalási" funkció is korlátozásra került, miután „valakik" – akiknek a személyes adatait a Binance biztonsági okokból nem adhatja ki annak az ügyfélnek, akinek a számláját megpróbálták hitelesíteni – sikertelenül azonosították magukat a számla tulajdonosaiként. Ezeket a „valakiket" a Binance szabályzata szerint a számlatulajdonosoknak kell ismerni és felkutatni, majd közös nyilatkozattételre rábírni a

[10] Mitchell Clark: *Credit Agencies Can't Tell My Sister and Me Apart*. In The Verge, https://www.theverge.com/22421193/credit-reporting-infrastructure-errors-experian-equifax-transunion (Utolsó letöltés időpontja: 2023.07.01.)

[11] Rachel Mortimer*: Identical Twins Told Not to Use 'Face ID' on Banking Apps*. In The Telegraph, https://www.telegraph.co.uk/personal-banking/current-accounts/identical-twins-told-not-to-use-face-id-on-banking-apps (Utolsó letöltés időpontja: 2023.07.01.)

[12] „Sorry your verification has been rejected. The reason for failure is as follows: An account with this information already exists. If you have a twin that has a Binance account, please reach out to customer support and provide a video recording of both yourself and your twin, holding up both IDs confirming that a manual verification is required. Please read the FAQs and Help section on our website and retry."

[13] *Why Do I Need to Re-verify My Binance Account (EEA Countries)*. https://www.binance.com/en/support/faq/why-do-i-need-to-re-verify-my-binance-account-eea-countries-bad81fdd4e8f404e980e6eda04eb200d (Utolsó letöltés időpontja: 2023.07.01.)

DOI: 10.58360/20231211-Demjen-2

korlátozás feloldása érdekében, amelyben a szolgáltató semmilyen segítséget nem nyújthat az érintettek személyazonosságának védelme érdekében. Amennyiben viszont nem csalók, hanem történetesen a számlatulajdonosok által ismert és beazonosított rokonaik hitelesítési próbálkozásai akadtak fent a rendszeren, abban az esetben is fennáll az informatikai rendszer hiányossága miatt elszenvedett nem csekély jogsérelem.

Az ügyet tovább árnyalja egy másik, nemcsak a Revolut-ügyek kapcsán, hanem több, hirtelen óriásira nőtt globális vállalat esetén is megfigyelt rendszerszintű probléma, amely szintén a technológiai fejlesztésekkel áll összefüggésben. Történetesen az, hogy sok más szolgáltatóhoz hasonlóan a Binance is *chatbot*-okat használ az ügyfélpanaszok kezelésére, melyeknek hatékonysága még ma is állandó kritika tárgyát képezi, tehát a vállalat által elvárt „manuális" hitelesítés a gyakorlatban majdhogynem lehetetlen. Az átlag felhasználók eleve nehezen barátkoztak meg azzal is, hogy különböző képeket és videókat kell magukról és személyes okmányaikról küldeni a világhálón keresztül, s ezt a bizalmatlanságot, ha lehet még tovább fokozza az, amikor nyilvánvalóan nem élő személy, hanem egy rendkívül makacsul és egysíkúan kommunikáló mesterséges intelligencia kezeli és értelmezi ezeket az adatokat; tőle függ tehát, hogy használhatjuk-e a pénzünket a jövőben, vagy sem. A kérdés ideális esetben természetesen rendeződhetne, ha a Binance rendelkezne megfelelő kapacitású élő ügyfélszolgálati részleggel, s még ha angol nyelven is, de sikerülne egy valós személy segítségével korrigálni a helyzetet. A kálváriát azonban tovább fokozza, hogy az élő asszisztencia kapcsolását mindaddig megtagadja a Binance, amíg a hitelesítésben minket „akadályozó" rokonunk – jellemzően, de nem kizárólag ikertestvér – hozzá nem járul egy ún. *Video Statement* során, hogy tovább használhassuk a számlánkat. A Binance külön felhívta a figyelmet, hogy nem fogad el képernyőfelvevő szoftverrel készült videókat (például olyan rokonoktól, akik egymástól több száz vagy ezer kilométerre élnek), bár felmerült, hogy elegendő lehet olyan videó, ahol nem valós időben szerepel két személy, hanem például egyikük videóhívással jelentkezik be a másik laptopján keresztül, amellett, hogy továbbra is meg kell felelni annak a követelménynek, hogy a személyi igazolványt maguk elé tartva az a teljes videó során tisztán és olvashatóan látható. Ez a remek ötlet csak azzal nem számol, hogy a Binance felületét használó különböző, egymáshoz hasonlító nevű és arcú emberek, rokonok akár érdekellentétben is állhatnak egymással, ezért még az eleve aránytalan technológiai nehézségeket nem számítva is vállalhatatlan követelményt támaszt az olyan felhasználókkal szemben, akik semmilyen módon nem tudják kikényszeríteni ezt a videós beleegyezést a rokonaiktól. Arról nem is beszélve, hogy a videó készítése során számos olyan személyes adatnak (számlaszám, e-mail cím, telefonszám, tartózkodási hely stb.) el kell hangoznia, amit az egymással esetleg érdekellentétben álló felek egyáltalán nem szívesen osztanának meg egymással, nemhogy ismeretlen, a mesterséges intelligencia által valamilyen adat alapján hozzájuk kötött idegenekkel.[14]

[14] *How to Reactivate My Account Withdrawal Function if Other People Appeared in My Face Verification Video*. https://www.binance.com/en-NZ/support/faq/how-to-reactivate-my-account-withdrawal-function-if-other-

DOI: 10.58360/20231211-Demjen-2

Hasonló problémákkal küzd az egyik legnagyobb telekommunikációs szolgáltató, a Telekom is, amelynél az ügyfelekkel történő szerződéskötést megelőzően történik algoritmus segítségével a biztonsági ellenőrzés lefolytatása. A rendszer az azonos vezetéknév, az édesanya azonos neve, az azonos születési hely és idő alapján kockázatos ügyfélnek minősítheti a szerződő felet, illetve számláját folyamatosan egy már meglévő ügyfél számlájával próbálja meg összekapcsolni, amely számlákat – ha az összekapcsolás sikerült – a technológia jelenlegi állása alapján gyakorlatilag a lehetetlennel egyenlő kísérletnek tűnik szétválasztani.[15] Egy új ügyfél regisztrációja még megoldható úgy, hogy az informatikai rendszerbe szándékosan hibásan viszik fel az adatait (például elgépelik az édesanyja nevét, vagy más, de hasonló keresztnevet írnak be, mint ami az igazolványon olvasható), esetleg azt tüntetik fel, hogy az ügyfél külföldi okmánnyal regisztrált náluk, majd miután létrejött a felhasználó és sikeresen elkerülték azt, hogy számlaadatait összekapcsolják egy már meglévő felhasználóéval, utóbb javítják a szándékos elírásokat, tévesztéseket. Az ilyen informatikai rendszerek általában automatikusan felkínálják a hasonló személyi adatokkal rendelkező ügyfelek különböző (internet, telefon stb.) számláinak összevonását, amit egy kevésbé járatos ügyintéző egy óvatlan kattintással meg is tehet, ezzel máris adatvédelmi incidenst és számos egyéb problémát előidézve. Mert legyenek bármilyen szoros kapcsolatban is egymással a rokonok, testvérek, ők törvény szerint teljesen különálló jogalanyok, akiknek semmi közük nincs egymás számlázási vagy banki adataihoz, s bár erről a szolgáltatók gyakran megfeledkeznek, egyáltalán nincs joguk azok megismeréséhez sem, nemhogy kezeléséhez (a telekommunikációs szolgáltatók által használt alkalmazásokban az ügyfélhez rendelt szolgáltatásokat és csomagokat könnyedén lehet módosítani, akár véletlenszerűen is kellemetlenséget okozva a velünk összekapcsolt felhasználónak).

Ahogyan a Telekom ügyfélregisztrációs rendszere manipulálható, úgy ez megoldható a Binance esetében is. A Binance mint pénzügyi szolgáltatást nyújtó szervezet köteles megfelelni a pénzmosás és terrorizmus finanszírozás elleni küzdelem részeként megalkotott KYC *(know your customer/client)*, azaz ügyfél átvilágítás alapvető szabályainak. Ezek a szabályzatok annyira elterjedtek, hogy mára gyakorlatilag globális minimumstandard ajánlások vonatkoznak a tartalmukra, melyet a hiteles pénzügyi szolgáltatók világszerte elfogadnak.[16] Ennek nem csupán bizonyos adózási és ügyfél-biztonsági okokból van jelentősége, hanem egy kriptotőzsde esetében például azt is hivatott szolgálni, hogy a kiemelt kockázatot jelentő ügyfelek (kiberbűnözők, oligarchák,

people-appeared-in-my-face-verification-video-634951d6973e4227ae92770a6ba59e09 (Utolsó letöltés időpontja: 2023.07.01.)

[15] Erdei Róbert: *Csúnyán összekeverte a dolgokat a Telekom az ikertestvéreknél: évek óta harcol velük Norbert, de nem oldódik meg a helyzet*. In Blikk, https://www.blikk.hu/aktualis/belfold/magyar-telekom-hiba-ikertestverek-adatok/wpf9tg3 (Utolsó letöltés időpontja: 2023.07.01.)

[16] *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF Recommendations 2012.pdf.coredownload.inline.pdf (Utolsó letöltés időpontja: 2023.07.01.)

DOI: 10.58360/20231211-Demjen-2

terroristák) egyáltalán ne férjenek hozzá a rendszer olyan pontjaihoz, melyen keresztül könnyen manipulálható az adott platform. A Binance saját állítása szerint milliárdos kiadásokat fordít a KYC elveknek és szabályoknak történő megfelelés technológiai oldalára. Jellemzően az ilyen ügyfél-átvilágításának magában kell foglalnia az ügyfél kilétének, lakóhelyének azonosítását, pénzügyi eszközeinek forrásáról való tájékozódást, és jövőbeli, pénzügyi tevékenységeire vonatkozó terveinek megismerését. Ez történhet azt megelőzően, hogy az ügyfélnek egyáltalán lehetővé tennék az adott tőzsdei felületre történő regisztrációt, de úgy is, hogy a regisztrációt követően bizonyos funkciók feloldásához, például kriptovalutákkal történő kereskedéshez szükséges elvégezni az átvilágítást. A technológiai fejlődés nyomán ahogy a bankszámla nyitása, úgy az ilyen eljárások is – a legtöbb „közönséges felhasználó" esetében legalábbis – digitális úton történnek. Ennélfogva a rendszer mind hamis dokumentumokkal, mind technikai manipulációval könnyebben kijátszható. Olyannyira valóságos ez, hogy bizonyos technológiai „kiskapuk" megtalálását és kihasználását nem egyszer maguk a Binance alkalmazottai javasolták a kínai ügyfeleknek[17] – hiszen ahogyan korábban említettük, Kína az elsők között szigorította a szabályozását és tiltotta be először a különböző kriptovalutákkal végzett pénzgyűjtést, végül 2021-ben minden más, kriptovalutákhoz köthető tevékenységet is, ami nyilván nem szolgálta a vállalat érdekeit. Még nem tisztázott, hogy a Binance vezetőségének volt-e tudomása arról, hogy a munkatársak éveken keresztül gyártottak videós segítséget különböző fórumokon keresztül a hamis igazolványok létrehozásának technikai és kapcsolati hátterének ismertetésétől a VPN (virtuális magánhálózat) használatával történő lokáció-elrejtésig. A VPN használatával az ügyfelek adatforgalma titkosításra kerül, így titokban tarthatják IP címüket (tehát például tényleges tartózkodási helyüket is) a különböző meglátogatott oldalak és az internetszolgáltató előtt is. A különböző VPN szolgáltatók nagy figyelmet fordítanak arra, hogy elérjék azokat az USA-beli felhasználókat, akiknek a Binance új, amerikai szabályozásnak megfelelni próbáló platformját kell használniuk, a Binance US-t.[18] Ezt a felületet a vállalat egy amerikai céggel közösen hozta létre, speciálisan az Egyesült Államok – kivétel Hawaii, Idaho, Louisiana, New York, Texas és Vermont – felhasználói számára, ezért például alig 70 kriptovalutával lehet csak kereskedni rajta keresztül, míg a Binance globális felületén több mint 500 féle kriptoeszköz elérhető. A Binance US 25%-os tranzakciós díjkedvezménnyel próbálja kompenzálni az amerikai felhasználókat, de sokaknak fontosabb a korlátozás nélküli kereskedelem, így VPN segítségével használják a platformot a tiltó szabályozás ellenére is.

Az ügyfél-hitelesítés szabályozási kísérletei

[17] Rohan Goswami: *Crypto Is Banned in China, but Binance Employees and Support Volunteers Tell People How to Bypass the Ban*. In CNBC,https://www.cnbc.com/2023/03/23/binance-employees-volunteers-tell-users-how-to-evade-china-crypto-ban.html (Utolsó letöltés időpontja: 2023.07.01.)

[18] Ahad Waseem: *How to Use Binance in the US (100% Safe)*. In Privacyhub, https://www.cyberghostvpn.com/en_US/privacyhub/how-to-use-binance-in-the-us (Utolsó letöltés időpontja: 2023.07.01.)

DOI: 10.58360/20231211-Demjen-2

A digitális KYC megoldások terjedésével az Egyesült Államok az ügyfél-hitelesítés technológiai hátterét nézve is szigorításra kényszerült. A *National Institute of Standards and Technology* (NIST) a digitális személyazonosság-ellenőrzés három biztonsági szintjét határozta meg (*Identity Assurance Level*, vagyis IAL, 1-től 3-ig terjedő besorolással). Az IAL1 szint a legkevésbé biztonságos, csupán a legalacsonyabb kockázatú műveletek végzésére alkalmas, mivel nem igényel sem biometrikus adatokat, sem érvényesítését és megerősítését a valódi személyazonosságnak. Az IAL2 szint a személyről készült fénykép (szelfi) és egy a személyhez kapcsolható azonosító okmány, például személyi igazolvány vagy bankszámla-kivonatok együttesét jelenti. Bizonyos erre szakosodott cégek külön kiemelik, hogy ezen a téren a technológia továbbra is bizonytalan és megbízhatatlan, ezért az IAL2 az EU-ban sem minden ügylethez megfelelő hitelesítési mód.[19] Az IAL3 szint a személyes azonosítással egyenértékűnek tekinthető, legmagasabb biztonsági szint, amely mindenképpen élő személy általi lebonyolítást és magas minőségű valós idejű folyamatos videókapcsolatot igényel, tehát a szelfizés ezen a szinten kizárt. A technológiai megoldások biztonságosabbá tételével ezen szabványok mentén rengeteg cég foglalkozik, melyek megoldásai az egyszerű szelfizős azonosítás biztonságosabbá és gyorsabbá fejlesztésétől a valós időben történő videós azonosítást kiváltó Video ID létrehozásáig számos lehetőségre kiterjednek. Az e-Személyi, a legmagasabb szintű biometrikus azonosítások, a Video ID és társainak megkövetelése és elterjedése azonban továbbra is csak akkor vezethet érdemi változásra az ügyfélbiztonság területén, ha a bankok és pénzügyi szolgáltatók hajlandók felelősséget vállalni azokban az esetekben, amikor a digitális rendszer kijátszásával lopják meg az ügyfeleiket. Hiszen a különböző digitális pénzügyi szolgáltatók és technológiai fejlesztő cégek számára hiába az az egyik legfontosabb, hogy megfeleljenek a pénzmosás és terrorizmus finanszírozása elleni szabályozás követelményeinek, vagy például az Európai Unióban a PSD2 erős, kétfaktoros ügyfél-hitelesítési követelményeinek, illetve a GDPR által megkövetelt adatvédelmi követelményeknek, hogyha a létrehozott rendszerek technológiai oldalának sérülékenységére nincsenek kellő tekintettel azok a bankok, melyeknél a felhasználók a pénzüket tartják. A Revolutot ért csalássorozat magyar áldozatairól elmondható, hogy átlagon felüli pénzügyi tudatossággal és technológiai ismeretekkel rendelkeztek, s mégis megtörténhetett velük, hogy hackerek kezébe kerültek a legérzékenyebb banki adataik. A sokkal kevésbé tudatos felhasználók, például az idősebb korosztály tagjai viszont eleve fokozottan ki vannak téve az interneten keresztül történő csalásoknak és visszaéléseknek, ám a digitalizáció rohamos mértéke, illetve az olcsóság és egyszerűség fokozatosan, de határozottan tereli őket is az elektronikus ügyintézés és pénzkezelés felé, nem is beszélve a központi digitális valutáról és a készpénzes fizetés jövőbeli megszüntetésének víziójáról.

Az Egyesült Államokban nagy fejtörést okoz még az is, hogy a digitális pénzügyi rendszerben dogmatikai szempontból elhelyezzék a különböző kriptoeszközöket; az

[19] *ID Images and Selfie Solutions Are Not KYC/AML Compliant*. In Electronic Identification, https://www.electronicid.eu/en/blog/post/selfie-based-identification-solutions-not-compliance-kyc-aml/en (Utolsó letöltés időpontja: 2023.07.01.)

DOI: 10.58360/20231211-Demjen-2

Egyesült Államok értékpapír- és tőzsdefelügyelete, a SEC *(Securities and Exchange Commission)* kitartóan érvel amellett, hogy egyes kriptovaluták nem regisztrált értékpapírnak minősülnek, például azért, mert azokat befektetésként értékesítették, és azzal fenyegeti a kibocsátókat – akik nyilván nem tekintik magukat a hatóság felügyelete alá tartozónak –, hogy eljárást indít ellenük, amennyiben nem függesztik fel az adott kriptoeszközök kibocsátását.[20] A kibocsátók természetesen ellenkeznek és készek pereskedni, de ettől függetlenül az adott kriptoeszköz kibocsátását leállítják és meghatározott ideig beváltják más pénzügyi eszközökre. Az ennek kapcsán kialakuló diskurzusban felmerült érvek és elméleti nehézségek is mutatják, hogy a tiszta és rendezett jogszabályi környezetért folytatott harc egyre keservesebb és reménytelenebb. A technológiai újításokkal napi szinten előálló kriptopiacon formálódó globális pénzügyi rendszer tulajdonképpen lekövethetetlen – emlékezzünk, hogy a MiCA, a forradalmi EU-s kriptoszabályzat már a megjelenésekor reflektálatlanul hagyott számos, a javaslat benyújtása óta virágzásnak indult eszközt, például az Ethereum 2.0 névre keresztelt rendszer által egyre szélesebb körben elterjesztett programozható kriptovalutát is, ami nem túl biztató azt tekintve, hogy ez az eszköz egyesek reményei szerint az „új internet" decentralizált bázisává válhat majd. Az Egyesült Királyság is ott tart, hogy a kriptoeszközöket – tekintettel arra, hogy nem rendelkeznek önálló értékkel – a szerencsejátékhoz hasonlóan kívánja szabályozni, míg az IOSCO *(International Organization of Securities Commissions)* a hagyományos eszközökhöz, tehát részvényekhez és kötvényekhez hasonló szabályozás kialakításának pártján áll.[21]

A közbeszéd sokszor példaként hivatkozik az élen járó EU-s szabályzatokra, a kriptovaluták és a digitális ügyfél-hitelesítés szabályozása körében az amerikaiak folyamatos „gyerekcipőben járását" és lemaradását szokás hangsúlyozni az Európai Unióhoz képest, ám félő, hogy nem sokáig tetszeleghet ebben a szerepben a térség, ha tovább enyhíti a már kialakított normákat. Az utóbbi időben ugyanis megfigyelhető, hogy a bankok a gyorsaság növelése és a kényelem fokozása érdekében próbálnak minél inkább eltávolodni az erős ügyfél-hitelesítés alkalmazásától. A PSD2 erre is tekintettel alkalmazott olyan kivételszabályt, ami például lehetővé teszi, hogy a bankok ne minden esetben kérjenek erős hitelesítést a számlainformációkat összesítő szolgáltatókon (AISP) keresztül kezdeményezett műveletekhez, hanem először 90, később 180 naponkénti hozzáférés-megerősítéssel oldják meg a folyamatos és gyors elérést bizonyos műveletek esetében. Ezt a szabályt később kötelezővé is tették annak érdekében, hogy a pénzügyi

[20] Hannah Lang – Tom Wilson – Elizabeth Howcroft*: Binance Stablecoin Backer Says U.S. SEC Has Labeled Token an Unregistered Security*. In Reuters, https://www.reuters.com/technology/binance-stablecoin-backer-ordered-stop-issuing-token-binance-ceo-2023-02-13 (Utolsó letöltés időpontja: 2023.07.01.)

[21] Dan Milmo: *'It's a Massive Ask': Is Binance Capable of Being Regulated?* In The Guardian, https://www.theguardian.com/technology/2023/may/27/is-binance-capable-of-being-regulated-crypto-exchange-uk (Utolsó letöltés időpontja: 2023.07.01.)

DOI: 10.58360/20231211-Demjen-2

szolgáltatók egységes eljárást alkalmazzanak az egész EU-ban.[22] Az ilyen típusú enyhítések megteremthetik a lehetőséget új típusú visszaélések születésére, hiszen az informatikai támadásoknak sokszor jelentős tényezője az idő. Minél több ideje van például egy előzetesen telepített kémprogramnak arra, hogy adatokat és felhasználói szokásokat gyűjtsön, később gyorsabban és hatékonyabban lesz képes végrehajtani a különböző visszaéléseket, csalásokat. A megerősítés gyakorisága pedig még ha kényelmetlen és időpazarlásnak tűnik is, jelentősen csökkenti az esélyét annak, hogy a megszerzett adatok és megfigyelt szokások alapján igazán ideális feltételrendszer alakulhasson ki a támadáshoz. A PSD2 azért megteremti a lehetőségét annak is, hogy azok a bankok, amelyek használnak valamilyen csalásmegelőző, tranzakciófigyelő rendszert a jogosulatlan hozzáférések kiszűrése érdekében, erős ügyfél-hitelesítést alkalmazhassanak, amennyiben ennek körülményeit és indokait kérés esetén megfelelően dokumentálva igazolni képesek az illetékes nemzeti hatóság felé.

Ez kifejezetten hasznos lehet a Revolut bankot ért csalássorozathoz hasonló események megelőzéséhez, de valószínűbb, hogy az adminisztratív terhek és a monitoring rendszerek anyagi és technikai hátterének megteremtésére és működtetésére „elszórt" pénz kevésbé motiválja a pénzügyi szolgáltatókat az ilyen típusú rendszerek kialakítására és fenntartására egy olyan környezetben, ahol a legfőbb cél az innováció elősegítése és az ügyfélélmény növelése. A britek szabályozása némileg eltér ettől: az Egyesült Királyság pénzügyi felügyelete, az FCA (*Financial Conduct Authority*) az erős ügyfél-hitelesítés feltételeként azt szabta meg, hogy az azonosítási eljárás az ismeret, a birtoklás és a biológiai tulajdonság fogalmi hármasa közül legalább kettőt bevonjon az ellenőrzésbe, a biológiai tulajdonság tág fogalma alatt azonban azt is értik, amikor az ügyfél kilétének és viselkedésének elemzése, azaz profilozása során például költési mintázatokat állapítanak meg, tehát – valószínűleg a korábbi negatív tapasztalatok hatására – logikailag már az ügyfél hitelesítésének körébe vonja a tranzakciók megfigyelését is, nem pedig egyfajta speciális plusz megerősítésként veti fel annak lehetőségét. Ez csupán apró fogalmi különbségnek tűnhet, de valószínűleg hozzájárul egy realisztikusabb megközelítés elterjedéséhez, amelyben a tranzakciót kezdeményező felet és a bank ügyfelét nem kezelik automatikusan egy és ugyanazon entitásként pusztán amiatt, hogy technikailag hozzáfér a fizetéshez szükséges adatokhoz.

Záró gondolatok

A digitális pénzügyi világ és azon belül is a kriptoeszközök biztonságossága a jelenlegi technológiai és szabályozási környezetben nem adott, legalábbis a legjobb minőségű szabályozás megalkotása sem garantálhatja a biztonságot, amíg nem történik szemléletváltás a különböző pénzügyi szolgáltatók és vállalatok részéről. Hiába a rengeteg

[22] Egri Szilvia: *Erre is készülniük kell a bankoknak. Változás az erős ügyfél-hitelesítés terén 2023-ban*. In Fintechzone, https://fintechzone.hu/valtozas-az-eros-ugyfel-hitelesites-teren-2023-ban (Utolsó letöltés időpontja: 2023.07.01.)

DOI: 10.58360/20231211-Demjen-2

oktató és információs anyag, a felhasználók jelentős része, ha egy kriptovalutával kapcsolatban azt ígérik neki, hogy stabil, illetve hogy mindenkor 1:1 arányban átváltható egy törvényes fiat valutára, akkor nem fogja kockázatosnak tartani az adott befektetést, a kriptotőzsde üzemeltetői pedig kizárják a felelősségüket (DYOR, mint tudjuk). A terület átláthatóságát nagy mértékben csökkentő jelentős túlszabályozás ellenére méretes hézagok mutatkoznak a szabályozásban még ma is, hiszen a globális pénzrendszer határok nélkül nyújtott szolgáltatásai fénysebességgel idézik elő az újabb és újabb társadalmi-kulturális kihívásokat a normaalkotás tempójához viszonyítva. A digitális pénzrendszer növekedése kihatással van a környezetre, a nemzeti valutákra és a nemzetek szuverenitására, a terrorizmusra, az állampolgárok adatainak, tulajdonának biztonságára és jogaik gyakorlására, miközben a jogi keretek közé terelésére tett kísérletek egyelőre nem értek el átütő sikereket. Pozitív várakozásra ad okot, hogy a kriptovaluták technológiai hátteréből fakadó bizonytalanság kiküszöbölésére a Bázeli Bankfelügyeleti Bizottság már új szabványt javasolt, amelynek érvénybe lépésére 2025. január 1-jével kezdődően lehet számítani. A megjelentetett javaslat alapján egy bank bizonyos kriptoeszközökkel szembeni kitettsége a jövőben nem haladhatná meg a 2%-ot, és általában 1%-nál alacsonyabbnak kellene lennie.[23] Ez talán védelmet jelenthet olyan esetekben, amelyet az FTX kriptotőzsde csődje okozott néhány amerikai bank számára, ám nem oldja meg azt a problémát, hogy az egyének alapvető jogai attól függenek, hogy egy rugalmasabb, évtizedes tapasztalattal rendelkező ügyintéző meg tudja-e oldani számukra bizonyos technológiai csapdák kikerülését. A realitás az, hogy az ember valódi ügyintézővel nem is találkozik, hanem már gyakorlatilag mindenhol chatbot asszisztensekkel kell kommunikálnia, akik sokszor élő munkatársnak vallják magukat, még akkor is, ha fél oldalas szövegeket küldenek el néhány milliszekundumos válaszidő alatt, illetve egy egyszerű feltételes módban megfogalmazott kérdésre sem tudnak válaszolni. Az összeadódó technológiai anomáliák hosszú hetekre nyújtják az ügyintézési folyamatot – paradox módon éppen egy az egyszerűség illúziójával nyitott online számla esetében – miközben az ügyfél folyamatosan el van zárva a saját fizetőeszközétől, tehát a jogait korlátozzák. A technológiai újítások egyfelől az egyes ember életének egyszerűsítésére és megkönnyítésére törekszenek, másfelől pedig vállalhatatlan (jog)hátrányokat képesek okozni a jogi szabályozás és az informatikai háttér, valamint egyes vállalatok merev hozzáállása következtében.[24]

[23] *Prudential Treatment of Cryptoasset Exposures*. (Basel Committee on Banking Supervision) https://www.bis.org/bcbs/publ/d545.pdf (Utolsó letöltés időpontja: 2023.07.01.)

[24] A német Volkswagen autómárka Car-Net digitális nyomkövető szolgáltatásának ügyfélszolgálata például nemrég a rendőrség kérésére sem adta ki egy ellopott jármű helyzetét (amelyben a tulajdonos kétéves gyermeke is benne ült), ameddig az ügyfél nem fizette be az adott szolgáltatásért járó díjat, ezzel mintegy fél órával késleltetve az igazságszolgáltatás eljárását egy olyan esetben, amelyben minden perc számított. Elméletileg a szolgáltatás üzemeltetői a bűnüldöző szervek megkeresésére sürgősségi eljárást kötelesek alkalmazni, amelynek elmaradása súlyos jogsértés. A cég azóta reagálva a történtekre néhány évig ingyenessé tette a távoli nyomkövetést a tulajdonosok számára. Ez egyfelől nyilván segíti a reputáció mielőbbi helyreállítását, de emellett remélhetőleg felhívja a figyelmet az ügyintézők, illetve az informatikai rendszer továbbképzésére és fejlesztésére is, hogy a közeljövőben ne állíthassanak szinte leküzdhetetlen technikai

DOI: 10.58360/20231211-Demjen-2

A fentiek alapján elmondható, hogy a jövő pénzügyi rendszerében rendkívül nagy szerepe lesz az egyének bizalmának, illetve az ennek nyomán létrejövő rendszerszintű bizalomnak, amelyért az államok és a különböző gazdasági szereplők jelenleg is intenzív harcot folytatnak. Az emberek biztonságérzete, tehát a kiszámíthatóság, a garanciák, a védelem és egyéb más, eredetileg a társadalmi szerződés gondolatához, az állam eszméjéhez kapcsolódó fogalmak egy átalakult, globális, esetleg túlnyomó részt vagy kizárólag digitális pénzügyi rendszerben teljesen átértelmeződhetnek. Ezek a fogalmak a jogi biztonság garanciáit tovább működtetni képtelen államokról a technológiai biztonságra, s az ezt garantálni képes, jó hírnevű gazdasági szereplőkre „tevődhetnek át", ezek viszont sem elszámoltathatóságuk sem felelősségük tekintetében nem hasonlíthatók az előbbiekhez.

akadályokat az egyén jogainak érvényesülése elé. Bővebben ld. Julianne McShane: *'Serious Breach' Led Volkswagen to Delay Tracking Stolen Car With 2-Year-Old Inside, Illinois Sheriff's Office Says*. In NBC News, https://www.nbcnews.com/news/crime-courts/serious-breach-led-volkswagen-delay-tracking-stolen-car-2-year-old-she-rcna72371, illetve Jess Weatherbed: *VW to Provide Five Years of Free Vehicle Tracking After Mishandled Carjacking*. In The Verge, https://www.theverge.com/2023/3/8/23630262/volkswagen-vw-carnet-free-vehicle-tracking-carjacking (Utolsó letöltés időpontja: 2023.07.01.)

DOI: 10.58360/20231211-Demjen-2