BAGÓ PÉTER

AZ AUTOMATIZÁCIÓ HATÁSA A PÉNZÜGYEKBEN – PÉNZÜGYI RENDSZEREK BIZTONSÁGA – ALGORITMIKUS KERESKEDELEM

A fintech evolúciója

A fintech fejlődése alapvetően három szakaszra bontható. A fintech 1.0 kezdete 1866 nyarára datálható, amikor lefektették az Atlanti-óceán alatt az első távírókábelt – ekkor kezdődött tulajdonképpen a pénzügyi globalizáció első korszaka, ezzel a találmánnyal vált lehetővé az információ nemcsak regionális, de interkontinentális továbbítása.[1] Ennek a korszaknak meghatározó része volt a telexgép használatának elterjedése is.[2] 1933-ban Németország vezette be a teleprinterek használatát, ami a második világháború végére egy, szinte egész Európa területén kiterjedt hálózattá alakult, 1957-re pedig már 39 országban volt jelen. A fintech 1.0 korszakának következő jelentős eseménye az első általános célokra felhasználható hitelkártya 1950-es megjelenése volt, ami a Diners Club társalapítói, Frank McNamara és Ralph Schneider neveihez kötődik.[3]

A fintech második érájának kezdetét egy áttörő újítás jelentette.[4] Az ötlet a háború utáni világ egy sajátosságából indult ki: széles körben elterjedt a csekkek használata. Ez nagyobb kényelmet jelentett, mint a készpénzes tranzakciók végrehajtása, aprópénz hordozása, számlálása. A bankok számára ellenben sok költséges könyvelési teendővel járt, ennek az oka a gazdasági fejlődésben keresendő, hisz a bérek emelkedtek, emiatt természetesen többe került nekik a dolgozóik foglalkoztatása. A magasabb fizetésnek köszönhetően nőtt a szabadidős tevékenységek iránti kereslet a hétvégi munkavégzés kárára. Emellett az ügyfelek részéről továbbra is fennállt az igény, hogy szombaton vagy akár vasárnap is készpénzhez jussanak. E tényezőket figyelembe véve igyekeztek megalkotni egy olyan rendszert, amely a könyvelési költségeket csökkenti, de egyúttal a banki szolgáltatásokat nagyobb mértékben és magasabb szinten tudják nyújtani. Erre a problémára a megoldást az ATM 1967-es bemutatása jelentette. A kezdetekben az ügyfelek utalvány ellenében vehettek fel pénzt, hat hónapon keresztül bármely nap,

[1] ARNER, Douglas W. – BARBERIS, Janos Nathan – BUCKLEY, Ross P.: The Evolution of Fintech: A New Post-Crisis Paradigm? University of Hong Kong Faculty of Law, Research Paper No. 2015/047. SSRN Electronic Journal, Volume 47, Issue 4, 2015. pp. 1271–1319. https://www.researchgate.net/publication/313365410_The_Evolution_of_Fintech_A_New_Post-Crisis_Paradigm; letöltés: 2022.10.11.

[2] ASHTA, Arvind – BIOT-PAQUEROT, Guillaume: FinTech evolution: Strategic value management issues in a fast changing industry. Strategic Change, Volume 27, Issue 4, July 2018. pp. 301–311.

[3] The Story Behind The Card. Diners Club International, 2022. https://www.dinersclubus.com/home/about/dinersclub/story; letöltés: 2023.01.04.

[4] ASHTA, Arvind – BIOT-PAQUEROT, Guillaume: FinTech evolution: Strategic value management issues in a fast changing industry.

ez a rendszer viszont megkövetelte a kézi könyvelési feladatokat. A banki feladatok hatáskörét átszervezték és a lakossági fiókok munkáját központi irodák kezdték ellátni, ezzel is csökkenteni szerették volna a költségeket, viszont ez nem a várt mértékben valósult meg.

A következő, a fintech 2.0-t meghatározó kezdeményezésnek a SWIFT-rendszer (Society for Worldwide Interbank Financial Telecommunication) 1973-as megvalósítását tekinthetjük.[5] Mint ahogy a legtöbb már említett vagy a továbbiakban említésre kerülő megoldás, ennek a kialakítása is a hatékonyabb munkavégzés és a magasabb szintű szolgáltatásnyújtás reményében indult el. A 60-as években számos nagyobb amerikai és európai bank fektetett pénzt magánhálózatok kialakításába és különböző számítógépes berendezésekbe, hogy lehetővé tegyék a határokon átívelő banki tevékenységek lebonyolítását. Ezekben a nemzetközi tranzakciókban hangsúlyos szerepe volt a közöttük lejátszódó hatékony kommunikációnak, viszont a szabad szöveges üzenetekbe sokszor kerültek kisebb-nagyobb hibák, azok sajnos akadályozták a folyamatot. Erre megoldást a belső banki eljárások standardizálása jelentett. Ezek nyomán 1973-ban az európai bankok kezdeményezésére brüsszeli székhellyel létrehozták a SWIFT-et mint nemzetközi (kezdetben 15 ország 239 bankja volt tag) pénzügyi szervezetet. Mára a nemzetközi tranzakciók elengedhetetlen részévé vált, 200 országban több mint 11 ezer pénzügyi intézmény a tagja ennek az infrastruktúrának.

Szintén említésre méltó a fintech 2.0 korszakából például az első kereskedelmi forgalomban elérhető mobiltelefon megjelenése 1983-ban, vagy az úgynevezett *program trading* 1987-es indulása, ami az értékpapír-kereskedelem algoritmizálásában katalizátorként funkcionált.[6] Ezeken kívül a 2000-es években felfutásnak induló, már emlegetett közösségi finanszírozás szintén számottevő mértékben befolyásolta a pénzügyi technológiák fejlődését.[7] Legnagyobb szerepet a pénzügyi piacon az internet elterjedése játszott.[8]

Az előző korszak végét és a jelenlegi elejét a 2008-as gazdasági válság kezdete jelentette.[9] A bankokat lekötötte a válságkezelés és a recessziót követően hozott különböző szabályozási követelményeknek való megfelelés, ez pedig teret engedett főként az újonnan belépő kis cégeknek (*start-up*ok) és a különböző innovatív megoldások megvalósításának.

---

[5] ASHTA, Arvind – BIOT-PAQUEROT, Guillaume: FinTech evolution: Strategic value management issues in a fast changing industry.

[6] ARNER, Douglas W. – BARBERIS, Janos Nathan – BUCKLEY, Ross P.: The Evolution of Fintech: A New Post-Crisis Paradigm?
MITCHELL, Cory: Program Trading: Meaning, Purpose, Example. Investopedia, 2022.05.25. https://www.investopedia.com/terms/p/programtrading.asp; letöltés: 2022.08.17.

[7] ASHTA, Arvind – BIOT-PAQUEROT, Guillaume: FinTech evolution: Strategic value management issues in a fast changing industry.

[8] LEE, In – SHIN, Yong Jae: Fintech: Ecosystem, business models, investment decisions, and challenges. Business Horizons, Volume 61, Issue 1, 2018. pp. 35–46. https://isiarticles.com/bundles/Article/pre/pdf/94413.pdf; letöltés: 2022.10.14.

[9] BUSSMANN, Oliver: The Future of Finance: FinTech, Tech Disruption, and Orchestrating Innovation. In: FRANCIONI, Reto – SCHWARTZ, Robert A. (szerk.): Equity Markets in Transition. Springer, Cham, 2017. pp. 473–486.

A Bitcoin 2009-es indulása és utána egyéb más kriptovaluták megjelenése alapjaiban rengette meg az emberek pénzről alkotott koncepcióját, ez a fintech 3.0 (eddig) egyik legjelentősebb mérföldkövének számított. A 2010-es évek elején jelentek meg tömegesen a piacon az okostelefonok, ezután gyakorlatilag bárki, bárhol és bármikor hozzáférhetett az internethez. Ez a jelenség pedig szinte azonnal magával hozta a mobilalapú fizetési megoldások széles körű elterjedését.[10]

A fintech 3.5 kezdetét ugyanúgy 2008-tól jegyzik, azzal a különbséggel, hogy ez a fejlődő világ pénzügyi technológiájára vonatkozik.[11] Ezeken a területeken nem tudott kialakulni magas szintű banki infrastruktúra (pl. Bangladesh), ami többek között annak is köszönhető, hogy az informatikai jellegű fejlesztésekre szánt pénz jelentősen elmarad az európai és az észak-amerikai szinttől, illetve az adatvédelemre vonatkozó szabályok is javarészt kevésbé szigorúak.[12] További akadályt jelent az, hogy a pénzügyi tudatosság szintje nem éri el a nyugati színvonalat, a bérek is alacsonyabbak, illetve a készpénzes tranzakciók túlnyomó többségben vannak a kártyás fizetéssel szemben, hisz sajnos sokan hozzá se férnek az Európában alapvetőnek számító pénzügyi szolgáltatásokhoz (pl. bankszámlanyitás).[13] Ezekben az elmaradott országokban jellemző az állami felügyelet alatt álló bankrendszer, viszont a beléjük vetett bizalom igen alacsony: részben sikertelenségüknek, részben pedig számos korrupciós botránynak köszönhetően.[14] Emiatt a tömegek nyitottak a különböző, nem bankok által nyújtott fintech-megoldásokra, ezzel is esélyt adva a tovább fejlődésnek és a felzárkózásnak a nyugati pénzügyi rendszerekhez.

Fintech-szektorok

A fizetés az egyik leggyakrabban használt és a legkevésbé szabályozott pénzügyi szolgáltatás.[15] Nagy fókusz helyeződik erre a témakörre, rendkívül dinamikusan fejlődik és nagy a tér az innovációnak is a szektorban. Két fő területre koncentrálódik: az egyik a lakossági, a másik pedig a kiskereskedelmi és vállalati fizetésre irányul. A lakossági fizetés területén több megoldást is kiemelnék. Az egyik ilyen a mobiltárca, erre remek példa a Barion mint magyar vállalat, de persze megemlíthetjük a Google Wallet-et, vagy az Apple Payt, ha a Big4 vállalatok fintech-szolgáltatásairól van szó. A P2P mobil fizetés (a hitelkártya-kibocsátó nagyvállalatok kikerülésével) is kiemelkedő szerepet játszik a területen, ezt a PayPal képviseli. Fontos megemlíteni továbbá a QR-kód alapú mobilos fizetési rendszert, a valós idejű fizetési megoldásokat, illetve a nemzetközi utalást különböző külföldi pénznemekben, ez utóbbira a Wise

[10] Evolution of Fintech: The 5 Key Eras. Zigurat, 2022.08.25. https://www.e-zigurat.com/innovation-school/blog/evolution-of-fintech/; letöltés: 2022.09.17.

[11] ARNER, Douglas W. – BARBERIS, Janos Nathan – BUCKLEY, Ross P.: The Evolution of Fintech: A New Post-Crisis Paradigm?

[12] Market Guide: Fintech. Energy Catalyst, June 2020. https://energycatalyst.community/developer/wp-content/uploads/2020/12/Market-Guide-Fintech.pdf; letöltés: 2022.06.27.
ARNER, Douglas W. – BARBERIS, Janos Nathan – BUCKLEY, Ross P.: The Evolution of Fintech: A New Post-Crisis Paradigm?

[13] Market Guide: Fintech.

[14] ARNER, Douglas W. – BARBERIS, Janos Nathan – BUCKLEY, Ross P.: The Evolution of Fintech: A New Post-Crisis Paradigm?

[15] LEE, In – SHIN, Yong Jae: Fintech: Ecosystem, business models, investment decisions, and challenges.

kínál kedvező lehetőségeket. A mobilról történő fizetés mind a szolgáltató, mind a felhasználó számára komoly előnyökkel jár.[16] Az ügyfelek számára a szóban forgó területen működő fintech-cégek korszerű, gyors és kényelmes fizetési élményt kínálnak, míg a vállalatok a mobilos fizetésnek köszönhetően egyre több hasznos adatot tudnak gyűjteni a felhasználókról, ami később innováció táptalaja is lehet.[17]

A következő fontos, megemlítendő terület a *crowdfunding*, vagy magyarul közösségi finanszírozás. Ahogy a nevéből is adódik, arra koncentrálódik, hogy az induló vállalkozásokat segítsék az emberek, egy-egy potenciális áttörést, forradalmi ötletet támogassanak anyagilag.[18] A rendszer három szereplőből áll: a vállalkozó, aki kezdeményezi a pénzgyűjtést; a hozzájáruló felek; valamint az az úgymond moderáló szervezet, amely közvetítő szerepet tölt be a finanszírozó és a finanszírozott között, az ő weboldalaikon keresztül lehet továbbá értesülni a különböző támogatható projektekről, illetve a támogatás fajtájáról.

A közösségi finanszírozásnak három fő típusát különböztetjük meg, ezek közül elsőként a jutalomalapú módszert ismertetném. Ez a fajta támogatás leginkább startupok és induló vállalkozók számára lehet célszerű választás, amelyek valamilyen innovatív termék vagy szolgáltatás fejlesztését tűzték ki célul maguk elé. A lényege az, hogy előre megadott időkereten belül kell hozni a „befektetők" által várt eredményt, viszont a hozzájáruló felek nem az általuk felajánlott pénzt kapják vissza, hanem lehetőség szerint a beígért terméket.[19] Népszerű vállalat a területen például a Kickstarter és a Crowdfunder. Az adományalapú finanszírozásnak ugyanaz az alapja, mint az előző *crowdfunding* formának, viszont akik segítik a vállalkozót, itt nem kapnak pénzben kifejezhető jutalmat a támogatásukért cserébe.[20] Az egyik legismertebb szervezetnek ezen a területen a GoFundMe mondható. A tőkealapú finanszírozás fő gondolata az, hogy befektetésért cserébe eladnak a cégek külső félnek egy részvényt, ez a KKV-szektorban népszerű választás lehet.[21] Ennél a támogatási formánál általában jelentősen nagyobb összegű hozzájárulásról van szó, mint az előző kettő esetén, emiatt a kockázat is természetesen nagyobb. Így tehát lényeges, hogy meggyőző üzleti terv álljon rendelkezésre, előre tisztázzák a megtérülési feltételeket, továbbá a vállalkozó legyen tisztában a részvényesek jogaival, illetve a további aspektusokkal.[22] Több vállalat foglalkozik tőkealapú finanszírozással, például a Crowdcube és az AngelList. A fintech tőkepaci szerepe nem ér véget a crowdfundingnál, számos cég (pl. Robinhood) kínál arra lehetőséget, hogy a befektetők kereskedjenek különböző részvényekkel és árukkal, illetve valós időben követhessék nyomon az esetleges kockázatokat.[23]

---

[16] LEE, In – SHIN, Yong Jae: Fintech: Ecosystem, business models, investment decisions, and challenges.
[17] BUSSMANN, Oliver: The Future of Finance: FinTech, Tech Disruption, and Orchestrating Innovation.
[18] LEE, In – SHIN, Yong Jae: Fintech: Ecosystem, business models, investment decisions, and challenges.
[19] Equity crowdfunding. European Comission, 2022. https://single-market-economy.ec.europa.eu/access-finance/guide-crowdfunding/different-types-crowdfunding/equity-crowdfunding_en; letöltés: 2022.07.01.
[20] LEE, In – SHIN, Yong Jae: Fintech: Ecosystem, business models, investment decisions, and challenges.
[21] Uo.
[22] Rewards-based crowdfunding. European Comission, 2022. https://single-market-economy.ec.europa.eu/access-finance/guide-crowdfunding/different-types-crowdfunding/rewards-based-crowdfunding_en; letöltés: 2022.07.01.
[23] LEE, In – SHIN, Yong Jae: Fintech: Ecosystem, business models, investment decisions, and challenges.

A P2P-hitelezés szintén jelentős, a fintech alapvető területe. Az ebben a szektorban létező szervezetek – mint pl. a Funding Circle – segítségével egyének és vállalatok is könnyen és hatékonyan adhatnak-vehetnek kölcsön egymástól pénzt alacsony kamat mellett.[24] Bár a bankokkal ellentétben ezek a cégek nem vesznek részt a folyamatban, hanem segítenek, hogy a hitelező és a hitelt igénylő felek egymásra találjanak, a szolgáltatásért viszont kiszámláznak bizonyos összeget. A hitelkockázat felmérése sem a bankoktól megszokott folyamaton alapul – pl. igénybe veszik a közösségi médián felgyülemlett adathalmazt is erre a célra.[25] A bankok és a hitelintézetek számára az ilyen fintech-vállalatok komoly ellenfeleknek számítanak, hiszen a tőkekövetelmény-rendeletek az utóbbiakra egyelőre nem vonatkoznak, így a kölcsönzés teljes összege se korlátozott, ami jelentős versenyelőnyt biztosít számukra a szóban forgó területen.[26]

A fintech-világ egyik leggyakrabban emlegetett területe, a blokklánc koncepciójának 2008-as megalkotása Satoshi Nakamotóhoz kötődik.[27] A kezdetekben az első kriptovaluta, a bitcoin nyilvános főkönyveként szolgált, mára már számos területen (pl. okosszerződések) használatos ez a technológia. A projekt eredeti célja az volt, hogy egy P2P-rendszert hozzanak létre, amely lehetővé teszi, hogy két fél között a hagyományos banki intézmények megkerülésével tranzakció mehessen végbe. Ezek a felek nem ismerik egymást, nincs meg köztük a kereskedelemhez szükséges bizalom, emiatt az egyik leglényegesebb a blokklánc-adatbázis megalkotásakor az volt, hogy ezt a problémát kiküszöböljék. Ehhez egy olyan technológiát dolgoztak ki, amely segítségével a könyvelési sorokat minden fél látja a blokkláncon, így ha valamilyen változás keletkezik azokban, arról mindenki értesül, ezzel elkerülhető a csalás.

Az egyik legnépszerűbb fintech-ágazat a robottanácsadás.[28] Ez olyan számítógépes algoritmusokat fed le, amelyek azonnal képesek információt szolgáltatni a befektetők és a kereskedők számára a tőkepiacot érintő hírekről, lekövetik többek között a közösségi médiában tapasztalható trendeket is, ezzel is segítve a döntéshozást.[29] Például a FutureAdvisor platformon ennek a technológiának a segítségével személyre szabottan (pl. a kockázatvállalási hajlandóságot is figyelembe véve) alakítható ki a kívánt eszközallokáció, amit a robot a folyamatos piaci változások ellenére is egyensúlyban tart.[30]

A fintech hatása a biztosítási szektorba is begyűrűzött, ahogy számos már említett terület esetén, ennek az iparágnak az üzleti modellje is a felek, jelen esetben a biztosító és az ügyfél közti közvetlen kapcsolatra és a rugalmas, korszerű szolgáltatás nyújtására épül.[31] A díjazás személyre szabott, legyen szó egészség-, baleset- vagy életbiztosításról. Járművek esetén remek példa erre a *pay-as-you-drive* biztosítás, amely az adott jármű használati adatait kéri be, és ezt elemezve állítja ki a fizetendő

[24] LEE, In – SHIN, Yong Jae: Fintech: Ecosystem, business models, investment decisions, and challenges.
[25] BUSSMANN, Oliver: The Future of Finance: FinTech, Tech Disruption, and Orchestrating Innovation.
[26] LEE, In – SHIN, Yong Jae: Fintech: Ecosystem, business models, investment decisions, and challenges.
[27] BUSSMANN, Oliver: The Future of Finance: FinTech, Tech Disruption, and Orchestrating Innovation.
[28] LEE, In – SHIN, Yong Jae: Fintech: Ecosystem, business models, investment decisions, and challenges.
[29] BUSSMANN, Oliver: The Future of Finance: FinTech, Tech Disruption, and Orchestrating Innovation.
[30] Uo.
[31] LEE, In – SHIN, Yong Jae: Fintech: Ecosystem, business models, investment decisions, and challenges.

díjat.[32] Ezen a területen jelentősebb szereplőnek mondható pl. a Clearcover és a Next Insurance.

Az azonnali fizetési rendszer (AFR) jelentősége elvitathatatlan, ezért erre is mindenképpen ki kell térni a következőkben. A TARGET Instant Payment Settlement (TIPS) a fintech-világ szintén fontos részét képezi.[33] Alapja, a TARGET2 létrehozására azért került sor, hogy támogassa az Európai Központi Bank monetáris politikáját, annak egységét. A TARGET2 olyan decentralizált fizetési rendszert takar, amelynek segítségével a központi és a kereskedelmi bankok az euróalapú fizetési tranzakciókat meg tudják valósítani. A TIPS 2018. november 30-án az eurorendszer jóvoltából indult el, mégpedig az ISO 20022 szabványok és az SCT Inst (SEPA Instant Credit Transfer) páneurópai azonnali fizetési rendszer közös szabályrendszerének figyelembevételével.[34] A TIPS egy olyan, a TARGET2 kiterjesztéseként létrehozott piaci infrastruktúraszolgáltatás, amely a PSP-k ügyfelei számára lehetővé teszi, hogy szünet nélkül (24/7) bonyolíthassanak le utalásokat, és a pénz pár másodpercen belül a fogadó fél számláján legyen. Az európai fizetési piac egységét kívánják ezzel megőrizni. A TIPS célja többek között az, hogy a tranzakciók maximum 10 másodpercen belül feldolgozásra kerüljenek – a biztonság és a folytonosság megtartásával.[35] A pénzforgalmi szolgáltatók a központi bankjuknál külön erre a célra nyitott számlán keresztül tudják ezeket az azonnali fizetéseket teljesíteni. A csatlakozás a TIPS-hez résztvevőként, elérhető félként, illetve utasító félként lehetséges.[36] A résztvevők x db számlával rendelkeznek a TIPS-ben, az elérhető felek pedig ezzel az x db résztvevői számlával jogosultak elszámolásra, de ők maguk nem rendelkeznek ilyennel. A hitelintézetek közti átutalások az úgynevezett utasító felek (pl. klíringházak) segítségével bonyolíthatók le. Magyarországon utasító félnek a GIRO Zrt. által működtetett Bankközi Klíring Rendszer mondható.[37]

Az AFR a TIPS alapján valósult meg Magyarországon. 2020. március 2-án indult el a GIRO Zrt., az MNB és 35 kereskedelmi bank részvételével – minden belföldi bank számára kötelező volt a részvétel az AFR-ben, ellentmondva a nemzetközi tapasztalatoknak.[38] Az AFR létrehozása során a SEPA-t példaként szem

[32] PUSCHMANN, Thomas: Fintech. Business and Information Systems Engineering, Volume 59, Issue 1, 2017. pp. 69–76.
https://doi.org/10.1007/s12599-017-0464-6; letöltés: 2022.05.21.

[33] Pán-európai elszámolásforgalmi rendszerek. MNB, 2022.
https://www.mnb.hu/penzforgalom/az-euro/pan-europai-elszamolasforgalmi-rendszerek; letöltés: 2022.11.23.

[34] DE JESSÉ, Marc Bayle: TARGET Instant Payment Settlement: The Eurosystem's response to an evolving payments landscape. Journal of Payments Strategy & Systems, Volume 12, Issue 4, 2018. pp. 322–327.
https://discovery.ebsco.com/c/n3fo33/viewer/pdf/h4exqdmysf; letöltés: 2022.12.15.

[35] What is TARGET Instant Payment Settlement (TIPS)? European Central Bank, 2022.
https://www.ecb.europa.eu/paym/target/tips/html/index.en.html; letöltés: 2022.06.04.

[36] DE JESSÉ, Marc Bayle: TARGET Instant Payment Settlement: The Eurosystem's response to an evolving payments landscape.

[37] GIRO. MNB, 2022.
https://www.mnb.hu/penzforgalom/a-hazai-penzforgalmi-infrastruktura/giro; letöltés: 2022.11.23.

[38] Elérhetővé vált az azonnali fizetés! MNB, 2022.
https://www.mnb.hu/azonnalifizetes; letöltés: 2022.11.23.
Az Azonnali Fizetési Rendszer (AFR). Takarékbank, 2022.
https://www.takarekbank.hu/azonnali-fizetesi-rendszer#; letöltés: 2022.03.25.

előtt tartották, épp azért, hogy ha itthon is bevezetésre kerül az euró, az átállás ne okozzon súlyos problémákat.[39] Jelenleg a rendszer egyedül belföldi, például rendszeres vagy értéknapos utalásokat támogat, illetve fizetési kérelem küldése és fogadása is lehetséges számos pénzügyi intézményben, szintén belföldi viszonylatban.[40] Ezekhez annyi követelmény tartozik, hogy ne legyen meghatározva teljesítési dátum, illetve az utalás összege ne haladja meg a 10 millió forintos felső határt. A szabály értelmében öt másodpercen belül visszavonhatatlanul a kedvezményezett számlájára kerül az átutalt összeg, a tranzakció elutasítása esetén a fizető fél arról üzenetet kap. Amennyiben öt másodperc alatt nem érkezik meg a pénz a kívánt számlára, 20 másodperc áll rendelkezésre, hogy a tranzakció végül sikeres lehessen.[41] A számlatulajdonosok a számlaszámukon kívül másodlagos azonosítót is hozzárendelhetnek a fiókjukhoz, például a telefonszámukat vagy az e-mail-címüket.[42]

Az MNB nemrég nyilvánosságra hozta az AFR fejlesztési koncepciójának tervezett elemeit, erről Bartha Lajos, az MNB pénzügyi infrastruktúrákért és bankműveletekért felelős ügyvezető igazgatója számolt be, és ezekből emelnék ki néhányat.[43] Az összes bank számára kötelező lesz a fizetési kérelmek fogadása, ahogy a QR-kódok olvasása is. A kódokat központilag hitelesített sztenderd alapján fogják megalkotni, ez a biztonság kérdésében jelentős előrelépés lesz. A QR-kód sztenderd kialakítását követően az NFC-n, illetve deeplinken keresztül történő AFR-re fogják helyezni a hangsúlyt. A tranzakciók felső értékhatárát 10 helyett 30 millió forintban állapítják meg, illetve minden átutalást követően kötelező lesz azok sikerességét igazolni egy üzenettel.

Az *open banking* és a PSD2 fogalma, célja

Az üzleti életben gyakran hangoztatják az „adat az új olaj” mondást, nem véletlenül – a vállalatoknak tudniuk kell azt, hogy a felgyülemlett adathalmazból hogyan nyerjenek ki az elemzési folyamat végére hasznos, új összefüggéseket.[44]

---

[39] AFR – the Hungarian Retail Instant Payment System. European Payments Council (EPC), 2020.04.14. https://www.europeanpaymentscouncil.eu/news-insights/insight/afr-hungarian-retail-instant-payment-system; letöltés: 2022.09.30.

[40] VRAZSOVITS Rita: Március 2-án indul az azonnali fizetési rendszer Magyarországon! Bank360.hu, 2022.01.18. https://bank360.hu/blog/azonnali-fizetesi-rendszer; letöltés: 2022.11.04.
VRAZSOVITS Rita: Fizetési kérelem: már kérni is lehet az utalást, nemcsak kapni. Bank360.hu, 2022.08.19. https://bank360.hu/fizetesi-kerelem; letöltés: 2022.10.27.

[41] VRAZSOVITS Rita: Március 2-án indul az azonnali fizetési rendszer Magyarországon!

[42] AFR – the Hungarian Retail Instant Payment System.

[43] TURZÓ Ádám Pál: Készül az AFR 2.0 – Elmondta az MNB, mit terveznek az azonnali fizetéseknél. Portfolio, 2022.12.12. https://www.portfolio.hu/bank/20220912/keszul-az-afr-20-elmondta-az-mnb-mit-terveznek-az-azonnali-fizeteseknel-564845; letöltés: 2023.01.10.

[44] AYTAŞ, Baran – ÖZTANER, Serdar Murat – ŞENER, Emrah: Open banking: Opening up the ’walled gardens’. Journal of Payments Strategy & Systems, Volume 15, Issue 4, December 2021. pp. 419–431. https://discovery.ebsco.com/c/n3fo33/viewer/pdf/pcmbonva7z; letöltés: 2022.12.04.
Belvo Team: Financial data enrichment: when data science meets open banking APIs. Belvo, 2022.02.09. https://belvo.com/blog/financial-data-enrichment-open-banking-apis/; letöltés: 2022.05.21.

A pénzügyi világot sokáig a bankok és a különböző pénzügyi intézmények uralták, az ügyfelek adataihoz egyedül ők fértek hozzá, ezzel számukra volt egyedül adott a lehetőség arra, hogy az értékes információkat felhasználva úgy és olyan irányba fejlesszék tevékenységüket, hogy abból még tekintélyesebb versenyelőnyt kovácsoljanak maguknak.

Az *open banking* (nyílt bankolás) megjelenésével viszont ez a hegemónia megszűnt, megtörtént az adatok úgymond demokratizálása.[45] Ez olyan, világszerte elterjedt, más-más fejlődési szakaszokban levő koncepció, amely végső célja egy készpénzmentes társadalom létrehozása.[46] A folyamat során az inkumbensek a harmadik feles pénzügyi szolgáltatók számára hozzáférést biztosítanak az ügyfelek bizonyos adataihoz alkalmazásprogramozási interfészeken, azaz API-kon keresztül, hogy azok az innovatív szolgáltatásaikkal további értéket biztosítsanak a felhasználók számára.[47] Az ügyfeleknek lehetőségük nyílik arra, hogy a bankjukkal kapcsolatban álló több fél szolgáltatásait is igénybe vegyék különböző célokra.[48] Területenként eltérő szabályozások érvényesek a bankokra és a pénzügyi intézményekre, vállalatokra. Európai uniós szinten a PSD2 nyújt megfelelő jogi keretet az *open banking* számára, illetve teszi lehetővé annak működését.

A PSD2 (Revised Payments Services Directive) irányelv a 2007-es PSD folytatásaként, kiegészítéseként készült. 2016 januárjában lépett hatályba, de az EU-tagállamoknak 2018 januárjáig volt idejük arra, hogy átültessék a saját jogrendszerükbe a megfogalmazott szabályokat. A szabályozástechnikai standardokat 2018 márciusában jelentették meg, ezután a pénzforgalmi szolgáltatók kaptak egy 18 hónapos átállási időt, hogy megfelelelhessenek ezeknek.[49]

A PSD2 értelmében a bankok kötelesek elősegíteni a nyílt bankolást, biztosítaniuk kell a hozzáférést az ügyfél- és a számlaadatokhoz az arra jogosult harmadik félnek (erről a későbbiekben lesz még szó).[50] Ezzel az EU-s fizetési piacot kívánták hatékonyabbá tenni, javítva a versenyt a hagyományos bankok, illetve a fintech-szolgáltatók között.[51] Sok reményt fűznek ahhoz a szabályozó hatóságok, hogy a PSD2 bevezetése serkenti az innovációra való hajlandóságot, illetve a szektorba magasabb szintű biztonságot és átláthatóságot hoz.[52]

---

[45] AYTAŞ, Baran – ÖZTANER, Serdar Murat – ŞENER, Emrah: Open banking: Opening up the 'walled gardens'.

[46] LAPLANTE, Phil – KSHETRI, Nir: Open banking: Definition and Description. Computer, Volume 54, Issue 10, October 2021. pp. 122–128.

[47] Open banking: Definition, How It Works, and Risks. Investopedia, 2022.04.04. https://www.investopedia.com/terms/o/open-banking.asp; letöltés: 2022.05.17.

[48] LAPLANTE, Phil – KSHETRI, Nir: Open banking: Definition and Description.

[49] The revised Payment Services Directive (PSD2) and the transition to stronger payments security. European Central Bank, March 2018. https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html; letöltés: 2022.06.04.

[50] ZACHARIADIS, Marcos – OZCAN, Pinar: The API Economy and Digital Transformation in Financial Services: The Case of Open Banking. SWIFT Institute Working Paper, 2016-001. http://dx.doi.org/10.2139/ssrn.2975199; letöltés: 2022.09.07.

[51] Opportunities in Open Banking. FDATA North America, 2019. ttps://fdata.global/north-america/wp-content/uploads/sites/3/2019/04/FDATA-Open-Banking-in-North-America-US-version.pdf; letöltés: 2022.04.26.

[52] ZACHARIADIS, Marcos – OZCAN, Pinar: The API Economy and Digital Transformation in Financial Services: The Case of Open Banking.

A PSD2 irányelv alappillérei és a nyíltbankolás-ökoszisztéma szereplői

A bekezdésben tárgyalt direktíva három fő pilléren alapul, az egyik az *open banking* magját képező technológiai szabványokra, azaz a fentebb már említett API-kra (alkalmazásprogramozási interfészekre) vonatkozik.[53] Ezek olyan felületeket takarnak, amelyek lehetővé teszik azt, hogy egy szoftver egy másikhoz csatlakozhasson, segítségével biztosított a harmadik fél számára a hozzáférés az ügyféladatokhoz. A PSD2-nek megfelelően az API-khoz kapcsolódó dokumentációt térítésmentesen kell a szolgáltatók rendelkezésére bocsátani.[54] Többféle API-szabvány létezik: Nagy-Britanniában az Open Banking UK vagy EU-s szinten a Berlin Group; az Unióban a bankok többségében utóbbi standard alapján alakítják ki a hozzáféréseket, de számos pénzügyi intézmény – mint a BBVA vagy az ING – saját API-t fejlesztett.[55] A másik pillér a biztonsági követelményeket vázolja fel, ez minden pénzügyi rendszer alapvető részét képezi.[56] A nyílt bankolás megjelenése pedig még nagyobb kockázati faktort rejt magában – több fél rendelkezik az érzékeny ügyféladatokkal, így nő az esélye a zsarolásoknak vagy akár a személyazonosság-lopásoknak, továbbá az adatszivárgások bekövetkezése is valószínűbb lehet.[57] A biztonság érdekében tett intézkedéseknek az adatok integritását kell elősegítenie, emellett az adott platform tulajdonosának biztosítékot kell arról adnia az ügyfélnek, hogy valóban az adatvédelmi sztenderdeknek megfelelően jár el.[58]

A PSD2 biztonsági alappillérének kulcsfontosságú része az erős ügyfél-hitelesítés (Strong Customer Authentication – SCA). Fő célja az, hogy az előző bekezdésben említett illegális tevékenységek számát visszaszorítsa. A fizetési csalások jelentős gazdasági kárt okoznak: 2019-ben csak az Egyesült Királyságban kibocsátott kártyákkal elkövetett visszaélések mértéke 621 millió fontra rúgott.[59] Kétlépcsős azonosításra van szükség a különböző banki műveletek, fizetések, illetve

[53] NANAEVA, Zhamal – AYSAN, Ahmed Farouk – SHIRAZI, Nasim Shah: Open banking in Europe: The effect of the Revised Payment Services Directive on Solarisbank and Insha. Journal of Payments Strategy & Systems, Volume 15, Issue 4, December 2021. pp. 432–444. https://discovery.ebsco.com/c/n3fo33/viewer/pdf/37bjtmjevb; letöltés: 2022.07.28.
What is API? Red Hat, 2022.06.02. https://www.redhat.com/en/topics/api/what-are-application-programming-interfaces; letöltés: 2022.08.11.

[54] LEMÁK Gábor. Itt a hazai open banking lista! 20-ból 17 magyar bank elstartolt. Fintechzone, 2019.03.18. https://fintechzone.hu/itt-a-hazai-open-banking-lista/; letöltés: 2022.03.11.

[55] BARBASURA, Dmitrii: Working with Technical Service Providers under PSD2. Finextra, 2019.07.30. https://www.finextra.com/blogposting/17686/working-with-technical-service-providers-under-psd2; letöltés: 2022.05.04.
LEMÁK Gábor. Itt a hazai open banking lista! 20-ból 17 magyar bank elstartolt.

[56] NANAEVA, Zhamal – AYSAN, Ahmed Farouk – SHIRAZI, Nasim Shah: Open banking in Europe: The effect of the Revised Payment Services Directive on Solarisbank and Insha.

[57] Open banking: Definition, How It Works, and Risks.

[58] NANAEVA, Zhamal – AYSAN, Ahmed Farouk – SHIRAZI, Nasim Shah: Open banking in Europe: The effect of the Revised Payment Services Directive on Solarisbank and Insha.

[59] What is SCA, and what is it good for? Tink, 2021.04.13. https://tink.com/blog/open-banking/strong-customer-authentication/; letöltés: 2022.09.16.

a netbankhoz történő hozzáférés esetén.[60] Ebből kiindulva két módon igazolhatja az ügyfél a személyazonosságát: lehet ez valami, amivel rendelkezik (pl. mobiltelefon segítségével), amit ismer (PIN-kód), vagy ami ő maga (pl. arcfelismerés, ujjlenyomat).[61] Számos helyzetben azonban nem szükséges alkalmazni ezt a hitelesítési formát: például 30 eurót el nem érő fizetések vagy megbízható kedvezményezettek esetén.[62]

A PSD2 irányelvtől ugyan független, de hasonlóan fontos szerepet tölt be a csalások elleni harcban a mesterséges itelligencia (MI) használata vagy az „ismerd meg az ügyfeled" (Know Your Customer – KYC) eljárás alkalmazása.[63] Ennek használata minden bank, hitelintézet, illetve a könyvelők számára is kötelező, segítségével kideríthető, hogy az ügyfél érdekelt-e korrupciós, esetleg pénzmosási ügyekben.[64]

További kihívást hozhat az *open banking* világába az adatok kezelésével, továbbá azok felhasználásával és tulajdonjogával kapcsolatos kérdések tisztázása mind a bankok, mind pedig a szabályozó hatóságok számára.[65] A PSD2 harmadik pillére, az átláthatóság itt kap jelentős szerepet. A felhasználók többféle pénzügyi adathoz engedhetnek hozzáférést biztosítani. Az ügyfél- és a számlaadatok tartoznak ide, például a számlatulajdonos neve, a számlanyitás ideje, a számla típusa, egyenlege vagy akár a devizanem. A pénzügyi mozgásokkal kapcsolatos adatok is megosztásra kerülhetnek: bemenő, kimenő tranzakciók, állandó megbízások, csoportos beszedési megbízások stb.[66] A GDPR-nak való megfelelés jegyében lényeges, hogy harmadik felek csak a felhasználó kifejezett engedélyével férhetnek hozzá azok adataihoz.[67] A hozzájárulás kérése pedig világos, minden ügyfél számára érthető legyen, hisz mindig tisztában kell lenniük azzal, hogy az általuk megosztott adatokkal mi történik. Ki milyen célra használja fel azokat, meddig engedélyezett számukra a hozzáférés, és hogy milyen módon lehet az engedélyt visszavonni.[68]

---

[60] NANAEVA, Zhamal – AYSAN, Ahmed Farouk – SHIRAZI, Nasim Shah: Open banking in Europe: The effect of the Revised Payment Services Directive on Solarisbank and Insha.

[61] GAYNOR, Brian: Payment Services Directive 2 – an overview. J.P.Morgan, 2022.05.18. https://www.jpmorgan.com/europe/merchant-services/insights/PSD2-all-you-need-to-know; letöltés: 2022.06.11.

[62] RODRIGUES, Abílio: PSD2 explained: understand the regulations and fraud monitoring. GoCardless, 2023. https://gocardless.com/guides/posts/an-introduction-to-psd2/; letöltés: 2023.04.08.

[63] SHLIAKHOUSKI, Alexey: Security In Open Banking: Concerns And Solutions. Forbes, 2021.08.19. https://www.forbes.com/sites/forbestechcouncil/2021/08/19/security-in-open-banking-concerns-and-solutions/?sh=3612304c6329; letöltés: 2022.10.01.

[64] Mit jelent a KYC? Fintech.hu, 2018.09.01. https://fintech.hu/mit-jelent-a-kyc/; letöltés: 2022.04.05.

[65] NANAEVA, Zhamal – AYSAN, Ahmed Farouk – SHIRAZI, Nasim Shah: Open banking in Europe: The effect of the Revised Payment Services Directive on Solarisbank and Insha.

[66] Open Banking and sharing your information online. MoneyHelper, 2022. https://www.moneyhelper.org.uk/en/everyday-money/banking/open-banking-and-sharing-your-online-banking-information; letöltés: 2022.10.11.
EWIN, Brad: What is open banking: Everything you need to know. GoCardless, 2023. https://gocardless.com/guides/posts/open-banking/; letöltés: 2023.04.11.

[67] LEMÁK Gábor. Itt a hazai open banking lista! 20-ból 17 magyar bank elstartolt.

[68] KEATING, ROB: Open banking data: what is it and what is it good for? GoCardless, 2023. https://gocardless.com/guides/posts/open-banking-data/; letöltés: 2023.05.24.

A nyílt bankolás koncepciója és az API-k megjelenése előtt is volt lehetőség pénzügyi adatokat összesítő oldalak szolgáltatásait igénybe venni, amelyek a 2004-ben létrehozott, úgynevezett *screen scraping* megoldást használták adatgyűjtésre.[69] A hagyományos *screen scraping* során a szolgáltató az ügyféltől mindenekelőtt igényelte a bankfiókjához tartozó hitelesítési adatokat, belépett oda, majd megszerezte a számára szükséges összes adatot.[70] Nem álltak rendelkezésre a PSD2-höz hasonló direktívák, amelyek nyomán lehetőség lett volna korlátozni a hozzáférést az adatokhoz. Ez az adatgyűjtési módszer már csak tartalékmechanizmus formában van jelen, az eredeti formája betiltásra került.[71]

A PSD2 irányelv négy fő szereplőt határoz meg. Az első a számlavezető szolgáltatók (Account Servicing Payments Service Provider – ASPSP. Idetartoznak például a bankok, a lakástakarék-pénztárak és a hitelkártya-kibocsátó intézmények.[72] Rendelkeznek banki tevékenységre feljogosító igazolvánnyal, ezek az entitások teszik elérhetővé API-kon keresztül az ügyféladatokat a harmadik feles szolgáltatók (Third Party Provider – TPP) számára, hogy a feladatuknak megfelelő szolgáltatást nyújtani tudják az ügyfél részére.[73] A TPP-k is a modell részét képezik, a PSD2 két fő pénzforgalmi szolgáltatót különböztet meg: a fizetéskezdeményezési szolgáltatókat (Payment Initiation Service Provider – PISP) és a számlainformációs szolgáltatókat (Account Information Service Provider – AISP).

A PISP-k gyakorlatilag közvetítőként funkcionálnak a pénzügyi intézmények és a kereskedő felek között, biztosítva köztük a közvetlen pénzmozgást.[74] Ha egy felhasználó feljogosít egy PISP-t egy fizetés kezdeményezésére, akkor a bank köteles lesz hozzáférést biztosítani a szolgáltatónak az API-jukhoz és a tranzakció lebonyolításához szükséges információkhoz.[75] Emellett rendkívül fontos az, hogy az ügyfél bizalmát sikerüljön megtartani, adataik integritását és biztonságát megőrizni, egy esetlegesen mégis bekövetkező incidens esetén viszont a PISP-k kötelesek a probléma mértékével arányos intézkedéseket hozni.[76]

---

[69] EWIN, Brad: What is open banking: Everything you need to know. Open banking: Definition, How It Works, and Risks.

[70] EWIN, Brad: What is open banking: Everything you need to know.

[71] VOAS, Jeffrey – LAPLANTE, Phil – LU, Steve – OSTROVSKY, Rafail – KASSAB, Mohamad – KSHETRI, Nir: Cybersecurity Considerations for Open Banking Technology and Emerging Standards. National Institute of Standards and Technology, Gaithersburg, 2022. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8389-draft.pdf; letöltés: 2023.01.17.

[72] Account Information Service Provider (AISP License). PSP Lab, 2022. https://psplab.com/services/pi-emi-authorisation/account-information-service-provider-aisp/; letöltés: 2022.09.04.

[73] FARROW, Gary S. D.: An application programming interface model for open banking ecosystems. Journal of Payments Strategy & Systems, Volume 14, Issue 1, March 2020. pp. 75–91. https://discovery.ebsco.com/c/n3fo33/viewer/pdf/jknjfoxnmz; letöltés: 2023.01.07.

[74] RODRIGUES, Abílio: PSD2 explained: understand the regulations and fraud monitoring.

[75] NANAEVA, Zhamal – AYSAN, Ahmed Farouk – SHIRAZI, Nasim Shah: Open banking in Europe: The effect of the Revised Payment Services Directive on Solarisbank and Insha.

[76] PALMIERI, Alessandro – NAZERAJ, Blerina: Open Banking and Competition: An Intricate Relationship. In: ERCEG, Aleksandar – AKŠAMOVIĆ, Dubravka: Competition Law (in Pandemic Times): Challenges and Reforms. Conference book of proceedings In Osijek, 13 May 2021. pp. 217–237. https://hrcak.srce.hr/ojs/index.php/eclic/article/view/18822/10290; letöltés: 2022.06.25.

Az AISP-k hozzáférhetnek az ügyfelek különböző számlainformációihoz, emészthető formába alakítják át őket, ennek köszönhetően pedig az ügyfél betekintést nyerhet pénzügyi helyzetének alakulásába.[77]

A nyílt bankolás előnyei, esetleges hátulütői

A következő bekezdésben szeretném kifejteni az *open banking* előnyeit, esetleges hátulütőit. A technológiai fejlődés és az Ipar 4.0 beszivárgása a pénzügyi szektorba idézte elő az *open banking* elterjedését és megvalósulását, hogy az eddig is meglévő igények – például a pénzügyi tervezés – hatékonyabban és biztonságosabb keretek között valósulhasson meg.[78] A fogyasztók az új, nyílt bankolásra épülő ökoszisztémának és a PSD2 bevezetésének az egyértelmű nyertesei. A harmadik fél által nyújtott szolgáltatások az ügyfelet helyezik előtérbe, amit a gyorsaság, a korszerűség és az intuitív kezelőfelületek is megerősítenek.

A kereskedelmi vállalatok számára is sok előnnyel járnak a harmadik felekkel történő együttműködések. A PISP-k integrálása, ezzel a fizetési folyamat gyorsaságának növelése és korszerűsítése a konverziós ráta növekedését vonhatja maga után, hiszen így kevésbé jellemző az, hogy a vásárlók a tranzakció közepén elhagyják a weboldalt és nem véglegesítik a vásárlást.[79] A francia sportáruházlánc, a Decathlon Lettországban és Litvániában integrálta a kevin. elnevezésű, fizetési szolgáltatásokat kínáló fintech-cég megoldásait, amellyel a sikertelen tranzakciók száma majdnem a felére csökkent.[80] Az is a PISP-k mellett szól, hogy a kereskedők és a bankok közti közvetlen pénzáramlásnak köszönhetően a tranzakciós költségek csökkennek, emiatt a fizetett összeg azonnal a céges számlára kerülhet.[81] Az AISP-k szolgáltatásait is ki tudják használni a vállalatok: olyan releváns ügyféladatokra tehetnek rajtuk keresztül szert, amely segítségével beazonosíthatják azokat a vásárlókat, amelyek a legnagyobb értéket jelentik számukra.[82]

A nyílt bankoláshoz köthető szabályozások meghozatala a bankok számára is jelentett változásokat. Az, hogy már nincsenek monopolhelyzetben az ügyfelekért folytatott versenyben, ráébresztette a bankokat arra, hogy szükséges bizonyos változások végrehajtása.[83] Újra kell gondolniuk az üzleti modelljüket, kapcsolatukat a kliensekkel és egy ügyfélcentrikus jövő felé kell orientálódniuk. Ez annak is köszönhető, hogy a felhasználók számára adott lehetőségek skálája a PSD2 bevezetésének következtében megugrott, így jelentős szerepet kap az eddigi ügyfelek megtartása, illetve újak bevonzása.[84] Az ő kezükben van a döntés arra vonatkozóan, hogy mely fintech-vállalatokkal lépnek együttműködésre, melyek tudják a legjobban

[77] RODRIGUES, Abílio: PSD2 explained: understand the regulations and fraud monitoring.
[78] Opportunities in Open Banking.
[79] KISKYTE, Adelina: What are account-to-account (A2A) payments? Kevin, 2022.05.30. https://www.kevin.eu/blog/what-are-account-to-account-payments/; letöltés: 2022.06.13.
[80] KISKYTE, Adelina: kevin. reduces Decathlon's abandoned carts by 50%. kevin., 2022.02.25. https://www.kevin.eu/blog/decathlon-success-story/; letöltés: 2022.05.11.
[81] KISKYTE, Adelina: What are account-to-account (A2A) payments?
[82] GAYNOR, Brian: Payment Services Directive 2 – an overview.
[83] EWIN, Brad: What is open banking: Everything you need to know.
[84] NANAEVA, Zhamal – AYSAN, Ahmed Farouk – SHIRAZI, Nasim Shah: Open banking in Europe: The effect of the Revised Payment Services Directive on Solarisbank and Insha.

kiegészíteni az általuk kínált szolgáltatások skáláját, emellett optimális ügyfélélményt garantálni a biztonsági kockázatok minimálisra csökkentésével.

Ez utóbbi azért fontos, mert lényegében az ügyfélbizalom működteti ezt a szektort, így annak elvesztése jelentős károkat okozhat a bankok számára mind presztízsvesztés, mind pedig komoly bevételkiesés veszélye is fennállhat.

Az új paradigma a felsorolt tényezőkön kívül egy igencsak ellentmondásos jelenséget hozott a szektorba. A digitális bankolás megjelenése tulajdonképpen megszüntette a humán erőforrás szükségességét a bankfiókokban, szinte minden pénzügyi teendő már otthonról intézhető.[85] Ez a bankok számára komoly kihívást jelent, hiszen hosszú időn keresztül az ügyintézők, illetve a privát bankárok kvalitásai számítottak fő differenciáló tényezőnek. Ennek hiányában az általuk kínált termékek veszik át ezt a szerepet, kizárólag azok alapján lesz lehetősége az ügyfeleknek banki szolgáltatót választani. A fintech-cégek ezzel ellenben szolgáltatásfókuszú stratégiára építenek, ez is együttműködésre és az általuk kínált szolgáltatáscsokor kiszélesítésére sarkallhatja az inkumbens pénzügyi intézményeket, de főleg a bankokat.

Az új ökoszisztéma az ügyfelek számára is ismeretlen terep. Az emberi természet velejárója, hogy rosszul reagál a gyökeres változásokra, nem hajlandó annyira befogadni az újat, ha az ráadásul a régi megszűnésével jár. Ugyan a fiatalabb generáció, amely már a technológiai vívmányokkal, a mobiltelefonnal, számítógéppel, tablettel nőtt fel, nagyobb eséllyel vonható be a nyílt bankolásba. Amely társadalmi réteg számára ez a koncepció önmagában idegen, alacsony az esélye annak, hogy őket sikerüljön mobilizálni, rábírni őket arra, hogy adataikat megosszák harmadik féllel. Mindazonáltal bármely korosztályt is sikerül elérni, elengedhetetlen a már sokat említett bizalom és a széles körű tájékozottság a lehetőségeik és esetleges kötelezettségeik terén.[86]

A bigtech cégek szerepe és létjogosultsága a nyílt bankolásban

A bigtech- vagy techfincégek olyan diverzifikált szolgáltatáskörrel bíró vállalatok, amelyek rendelkeznek három kulcsfontosságú tényezővel: az első a magas szintű technológiai fejlettség; több és sokrétűbb adatot tudnak összegyűjteni a bigtechek intenzív online jelenléte és a lehetséges versenytársak adataihoz való hozzáférés miatt, mint bármely pénzügyi intézmény vagy fintech-startup; széles a felhasználói körük.[87] Az amerikai székhelyű multik közül a Google, az Amazon, a Facebook (vagy mai nevén Meta) és az Apple sorolható a bigtechek közé. A legnagyobb bigtechek székhelye többnyire az EU-n kívül található, túlnyomórészt Kínában és az Amerikai Egyesült Államokban. Ennek lehetséges magyarázata több tényező figyelembevételével függhet össze, mint amilyenek a különböző európai kormányzati rendszerek, a társasági jog, a kockázati tőke korlátozott elérhetősége és az új technológiához való társadalmi attitűdök, amelyek vélelmezhetően gyengébbek

[85] EWIN, Brad: What is open banking: Everything you need to know.
[86] NANAEVA, Zhamal – AYSAN, Ahmed Farouk – SHIRAZI, Nasim Shah: Open banking in Europe: The effect of the Revised Payment Services Directive on Solarisbank and Insha.
[87] TANDA, Alessandra – SCHENA, Cristiana-Maria: FinTech, BigTech and Banks. Digitalisation and Its Impact on Banking Business Models. Palgrave Macmillan, London, 2019.

Európában. A kínai techfindominancia és gyors fejlődés egyik lehetséges oka lehet, hogy az EU-ban és az Amerikai Egyesült Államokban a meglévő pénzügyi szolgáltatások infrastruktúrái fejlettebbek, így a délkelet-ázsiai régió technológiai innovációjának kedvezhet a helyzet. A techfinek tevékenységüket a fentebb felsorolt előnyökre építették a saját területükön, és csak utána kezdték el fontolóra venni azt, hogy belépnek a pénzügyi szektorba.[88] E vállalatok jelenléte a pénzügyi piacon ugyan fokozhatja a versenyt és az innovációs képességet, de emellett komoly fenyegetést jelentenek az inkumbens bankok és a fintech-cégek számára is, hiszen a techóriások kifinomultabb MI- és gépi tanulási módszereket alkalmaznak az adatok valós idejű feldolgozására.[89] A bankok is kihasználják ugyan az MI adta lehetőségeket, de nagy volumenű adatgyűjtésre és -feldolgozásra nem képesek annyira, mint a bigtechek. Mindez azzal is magyarázható, hogy a bigtechcégeket nem érintik a pénzintézetekre vonatkozó különféle szabályozások, így például több pénzt képesek fordítani a K+F-tevékenységekre.[90]

Szabályzói környezet

Fontos, hogy a szabályzói környezet lépést tudjon tartani a rohamosan fejlődő technológiai vívmányokkal és a pénzügyi szektorban folyamatosan megjelenő innovációkkal, ugyanis számos kockázattal járhat felhasználói, befektetői vagy akár versenyjogi szempontból egy nem megfelelően kezelt újítás. Befektetői és felhasználói oldalról a legnagyobb rizikót az adatvédelem jelentheti. Bármilyen szintű személyes adatkiszivárgás alapjaiban rengetheti meg az adott innovációba vetett bizalmat. Mivel a fintech-megoldások terén az adatvédelmi kockázat sokkal komplexebb formában kezelendő, így erre kiemelt figyelmet szükséges fordítani. Versenyjogi szempontból is kardinális kérdés, hogy hogyan kezeljük a megjelenő fintech-cégek rendszerszinten jelentős innovációit, ugyanis az ilyen szervezeteknél könnyedén koncentrálódhat a piaci részesedés. E kérdésben említendő a klasszikus fintech-innovációkkal kapcsolatos szabályzói dilemma, miszerint a megoldás a két véglet között keresendő, amelyek a *laissez-faire* és a túlzott szigor.

A *laissez-faire* felfogás szerint a szabályzói oldalnak csak a lehető legkisebb mértékben szabadna kontrollálnia a gazdasági innovációs folyamatokat. Ez a szemlélet semmiféle gátat nem szabna a fejlődésnek, kontroll nélkül azonban könnyedén sérülhetnének a fentebb említett jogok. A másik végletet tekintve a túlzott szigor is működésképtelen, hiszen a fintech-irányzat központi elemét, az innovativitást korlátozná. Ez emellett a megjelenő innovációk és fintech-cégek magyar piactól történő teljes elfordulásához is vezetne, aminek hatására hazánkban nagymértékű pénzügyi-technológiai lemaradást tapasztalhatnánk. Ekkor számos hazai felhasználó nyithatna a külföldi piac felé, amelynek hatására a szolgáltatások díja növekedne.

---

[88] OMARINI, Anna Eugenia: Banks and Fintechs: How to Develop a Digital Open Banking Approach for the Bank's Future. International Business Research, Volume 11, Issue 9, 2018. http://www.ccsenet.org/journal/index.php/ibr/article/download/76769/42646; letöltés: 2022.08.01.

[89] PALMIERI, Alessandro – NAZERAJ, Blerina: Open Banking and Competition: An Intricate Relationship.

[90] TANDA, Alessandra – SCHENA, Cristiana-Maria: FinTech, BigTech and Banks. Digitalisation and Its Impact on Banking Business Models.

A fintech-szervezetek jelentős része összetett IT-struktúrával és -szoftverekkel rendelkezik. Ennek okán kiberkockázati szempontból is nehezen azonosíthatók egyes hiányosságok. Ilyen esetekben fontos a rendszer átláthatósága, kritikus pontjainak felmérése és a krízishelyzetek megelőzése vagy azoknak gyors felismerése, majd megfelelő akciótervvel a kár minimalizálása. Abban az esetben, ha egy harmadik feles szolgáltatónak együttműködés során nagy volumenű megosztott adat kerül a birtokába, annak kezelése igen nagy körültekintést kíván. Esetleges hibánál közvetlenül a felhasználót érheti kár, ami bekövetkezhet adatvesztéstől, adatminőség-romlástól vagy nem megfelelően megírt automatizálástól, elemzéstől. Ilyen esetekben felmerülhetnek a károkozáson kívül megtévesztéssel kapcsolatos vádak is, hiszen a nem megfelelő elemzések nem megalapozott döntésekre vehetik rá a felhasználót.

Makroprudenciális kockázatok szempontból érdemes mérlegelni azoknak a vállalatoknak a versenyelőnyét, amelyek a versenytársaiknál korábban integráltak bizonyos funkciót vagy technológiát. Ilyen esetben természetes a versenyelőny kialakulása, de rendszerszinten jelentős működésnél, ha a versenyelőnyt élvező vállalat olyan szinten képes piaci részesedést szerezni, hogy mellette nem képesek potenciális versenytársak felzárkózni, úgy egy vállalati sokk hatására rendszerszinten jelenhet meg krízishelyzet. Más gazdasági ágazatok számára is lehetséges veszélyforrást jelenthet egy ilyen krízis, ugyanis a piaci szereplők közötti összeköttetés növekedésével közös kockázati pontok is megjelennek.[91]

Az API-technológia

Az alkalmazásprogramozási interfész (Application Programming Inteface – API) technológiája kulcsfontosságú szerepet tölt be az nyílt bankolásban, hiszen ez biztosítja a szoftverek közti adatcseréhez szükséges ki- és bemeneteket. „*Az API-hozzáférés szolgáltatók, adatbázisok, funkcionalitások között teremt gyors, dokumentálható, menedzselhető kapcsolatot.*”[92]

Az API-gazdaság mint trend a 2000-es évek elején kezdődött, amikor a technológiai cégek az elsők között kezdték el a fejlesztési folyamataikba történő beintegrálását. Ezzel a megoldással rendszereik hibatűrésének és a fejlesztések gyorsaságának növelését kívánták elérni. Évekkel később a hatékony működésüknek köszönhetően a pénzügyi szektor is felismerte az API-technológia kiaknázhatóságát, és az EU-szabályozásnak (PSD2) köszönhetően ez meg is valósulhatott, így kezdetét vehette a nyílt pénzügyek (*open finance*) kialakítása.[93]

[91] FÁYKISS Péter – PAPP Dániel – SAJTOS Péter – TŐRÖS Ágnes: A FinTech-innovációk ösztönzésének szabályozói eszközei: Innovation Hub és Regulatory Sandbox a nemzetközi gyakorlatban. Hitelintézeti Szemle, 17. évfolyam 2. szám, 2018. augusztus. pp. 43– 67. https://hitelintezetiszemle.mnb.hu/letoltes/hsz-17-2-t2-faykiss-papp-sajtos-toros.pdf; letöltés: 2022.10.16.

[92] LEMÁK Gábor: Vizsgálja az MNB a fizetési kérelem kötelező bevezetését. Jön az AFR 2.0! FinTechZone, 2021.12.15. https://fintechzone.hu/vizsgalja-az-mnb-a-fizetesi-kerelem-kotelezo-bevezeteset-jon-az-afr-2-0/; letöltés: 2022.03.18.

[93] Uo.

Az API biztonságkozkázati tényezői

Az API-biztonság a kritikus eleme magának a technológiának, hiszen az adatbázisok és a központi rendszerek megnyitásával és más rendszerekkel való összekapcsolásával növekszik a támadható felület és nő a biztonsági kockázat. A pénzügyi szektorban ez még nagyobb problémát okozhat, hiszen nagy mennyiségű érzékeny információ folyik keresztül ezeken a csatornákon. Ilyenek közé sorolhatjuk többek között a személyes és a pénzügyi adatokat, a vállalati titkokat és egyéb privát információkat.[94] A harmadik feles szolgáltatók belépésével új adatszivárgási forrás keletkezhet, és ha sérül a felhasználó adata, az a folyószámlájára is hatással lehet. Bár a GDPR a TPP-k számára is előírja az adatok megfelelő és biztonságos kezelését, esetleges fejlesztői biztonsági hibákon keresztül vagy szándékos emberi tevékenységből (szivárogtatás) feltételezhetők támadások.

Az ilyenhez hasonló biztonsági rések kiküszöbölését több módon érdemes megközelíteni. A bank oldaláról a tranzakciók és a felhasználói viselkedés folyamatos monitorozása és a kockázatelemzés jelenthet megoldást. Ezek mellett helyet kapott 2021. január 1-jétől a fokozott ügyfélazonosítás is, amelyet többlépcsős PIN-kódmegadással vagy biometrikus adatellenőrzéssel hajtanak végre. A harmadik feles szolgáltatóval való együttműködés során a legfontosabb biztonsági intézkedések a kommunikációs csatorna védelme, valamint a független biztonsági ellenőrzések eredményeinek folyamatos ismertetése a másik féllel. Ezen biztonsági intézkedések mellett említhetünk még néhány alapszabályt, amelyek mind a bankok, mind a külső érdekelteknek iránymutatásul szolgálhat. Az első és legfontosabb, hogy „*a külső szolgáltatónak meg kell győződnie arról, hogy az API által használt adatformátumtól függetlenül az alkalmazásprogramozási felület adatstruktúrákat feldolgozó szoftveres komponense ellenálló a kibertámadásoknak.*” Ennek érdekében minden API-t és minden érintett eszközt le kell tesztelni és biztonsági elemzést kell végrehajtani rajtuk. Az API-struktúrába elengedhetetlen lépés egy biztonsági *gateway* integrálása, amely a jogtalan hozzáféréseket kiszűri, így csak az azonosított féltől érkező kérések jutnak el az adatbázisig. A *gateway* továbbá validálja ezeket a kéréseket, az azokra adott válaszokat, titkosít és tartalmat szűr. A kockázatcsökkentés és a folyamatos tanulás fontos része a naplózás is, amelynek segítségével folyamatosan monitorozhatjuk az esetleges adatbiztonsági incidenseket.[95]

Pénzmosás és a fintech

Valószínűleg a kifejezés nem újszerű senkinek, valamilyen formában mindenki találkozott már a kifejezéssel. De hogyan is lehetne legkönnyebben megfogalmazni, hogy mit is jelent a pénzmosás? Ez egy folyamat, amely során az illegálisan szerzett pénz forrását próbálják megváltoztatni, és ezáltal legális forrásból származóként feltűntetni.[96] A folyamat lényege minden esetben az, hogy ne látszódjon, honnan is

[94] Miért van szükség API-biztonságra? Computerworld, 2019.09.25. https://computerworld.hu/biztonsag/miert-van-szukseg-api-biztonsagra-268739.html; letöltés: 2022.10.01.

[95] IT-biztonsági katasztrófa, ha a jobbról várt pofont balról kapjuk. Bitport, 2020.09.07. https://bitport.hu/it-biztonsagi-katasztrofa-ha-a-jobbrol-vart-pofont-balrol-kapjuk-api-security-balasys-open-api; letöltés: 2022.06.21.

[96] Képesített pénzmosás és terrorizmus finanszírozása elleni szakértő képzés. Jegyzet. Bankárképző, Budapest, 2018.

származik az összeg, valamint könnyű szerrel a pénz útja is nehezen lekövethető legyen. Más forrás szerint úgy lehet meghatározni, hogy a pénzmosási folyamat az illegális tevékenységből származó haszon eredetének leplezését jelenti.[97]

A pénzmosás folyamatát – vagyis a pénz legalizálásának útját – egy háromfázisú modellel tudjuk szemléltetni. Ez a modell az Amerikai Egyesült Államokból származtatott. A folyamat lépései:

- elhelyezés;
- rétegzés;
- integrálás.[98]

Az első lépésben a tisztára mosni kívánt pénz – ami jellemzően készpénz – elhelyezése történik a pénzügyi rendszerben valamilyen formában. Jellemzően a cél a bankrendszer. Manapság erre a lépésre már világszerte felkészült a pénzügyi szektor. Mindig a legnagyobb indikátor és veszélyjelző a nagy összegű készpénz megjelenése. Ekkor a legfontosabb a pénz forrásáról valahogy meggyőződni, amely hitelesen igazolja, hogy milyen eredetű összeg fog a bankrendszerbe bekerülni. Sok esetben láthatunk adás-vételi szerződést, végkielégítést, vagy akár családi örökséget is.

A folyamat második része a rétegzés. Ennek lényege, hogy bonyolult, több számlán, több érintett ügyfélen keresztüli tranzakciókat végeznek. Jellemzően több különböző banknál vezetett számlákon, akár különböző devizákban, több országot érintve, amelyeknél az sem baj, ha olyan országot is érintenek a tranzakciók, ahonnan nehezebb banki információkat szerezni. Ez a folyamat azért is fontos, mert bárki szeretné az átutalásokat visszakeresni, rengeteg erőfeszítésbe kerül és sokszor közel lehetetlen az eredetét megtalálni. Egy-egy tranzakcióra lehet bekérni információt az ügyfelektől, de a teljes lánc visszafejtéséhez akár nemzetközi együttműködés is szükséges lehet. Viszont ha az utalások csak egy kis szeletét nézzük, csak annyit látunk, hogy egy ügyfél egy másiknak utalást teljesít, akár átlagos mértékűt, és ha bekérek információt az utalás hátteréről, készségesen válaszolnak és akár még számlákat, szerződést is be tudnak mutatni. Ezen a ponton már nehéz helyzetben van a pénzmosás megelőzése.

A harmadik lépés – az elhelyezés és a rétegzés után – az integrálás. A második pontban sokáig forgatott összegek felvétele vagy befektetése. Ez valójában már az a lépés, amikor tiszta bevételként kerül feltüntetésre, vagy az ügyfél épp egy nagyobb értékű beruházást végez ebből a pénzből. Forrása tisztának mondható, hiszen az ellenkezőjére sincs bizonyíték. Ez az a lépés, amikor a könyvelő plusz-, vagyis megnövekedett bevételként könyveli szét egy-két hónapra a hozzárakott pénzt. Nagyon sok esetben a folyamat készpénzfelvétellel zárul, adófizetéssel színezett, ezzel méginkább a legalitásának látszatát keltve. Jellemző napjainkra is, hogy az ügyfelek az ATM maximális kapacitásának megfelelően több részletben felveszik a kívánt összeget, csak a fiókba vagy pénztárba ne kelljen bemenni, mert ott van egy számukra veszélyes tényező: a banki dolgozó, aki elsődleges pénzmosásmegelőzési

[97] Adó-kódex. XXVII. évfolyam, 6. szám. Wolters Kluwer, 2018.
[98] GÁL István László: A pénzmosás hatályos büntetőjogi szabályozása Magyarországon. Pécs, 2007. https://www.mnb.hu/letoltes/pszafhu-rtfkonf-gali.pdf; letöltés: 2022.07.26.

védelmi vonalként bizony érdeklődni fog az összeggel kapcsolatban. A befizető automaták népszerűsége is jelentősnek mondható hasonló okokból kifolyólag. Erre természetesen a bankoknak fel kell készülniük, és eljárásrendben foglaltaknak megfelelően valamilyen szűrés alapján figyelniük szükséges.

A fenti folyamatból is jól látható néhány figyelmeztető jel. A legelső lépésben a készpénz elhelyezésénél van a legnagyobb lehetőség megakadályozni a folyamatot, a folyamat vége szintén az esetek többségében egy készpénzfelvétel lesz, vagy nagy értékű beruházás. A pénzmosásmegelőzési folyamat nagyon nagy részét a tranzakciók eredetének és azok céljainak a vizsgálata kell, hogy kitöltse.

Összességében kijelenthetjük, hogy a legnagyobb indikátor a pénzmosás jelenlétére a kiemelkedő készpénzforgalom.

Monitoring vagy filtering?

A fenti folyamatokból látható, hogy minél több, minél nagyobb számban szükséges az ügyfelek folyamatos figyelemmel kísérése, a tranzakciók vizsgálata. A 26/2020. (VIII. 25.) MNB rendelet (a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló törvény végrehajtásának az MNB által felügyelt szolgáltatókra vonatkozó, valamint az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvény szerinti szűrőrendszer kidolgozásának és működtetése minimumkövetelményeinek részletes szabályairól) 33. §-a szerint:

„*Automatikus szűrőrendszer: az ügyfél és az ügylet pénzmosás és terrorizmus finanszírozása szempontjából előzetes paraméterezés alapján történő, emberi beavatkozást nem igénylő leválogatására alkalmas informatikai rendszer.*”

A fent idézett jogszabály szerint a szolgáltatónak kötelessége szűrőrendszert alkalmaznia, amely támogatja a pénzmosásmegelőzési tevékenységét, és az alkalmas emberi beavatkozás nélkül jelzések generálására. Nagyon fontos ezzel kapcsolatban meghatároznunk, hogy mi a különbség a monitoring- és a filteringrendszer között.

A monitoringrendszer utólagos, úgynevezett posztmonitoring tevékenységre alkalmas. A rendszer a megtörtént tranzakciókat utólagosan vizsgálja előre beállított szabályok, szcenáriók alapján. Ez a gyakorlatban úgy kivitelezhető, hogy a monitoringrendszerbe folyamatosan betöltésre kerülnek az ügyfelek tranzakciói, amely megszűri azokat, és a beállított szabályoknak megfelelően jelzéseket, riasztásokat generál. Természetesen önmagában a rendszer még nem egy MI, hogy egyértelműen meg tudja mondani számunkra mi pénzmosás és mi nem az, de minél pontosabb beállításaink és szabálymeghatározásaink vannak, annál pontosabb szűrési eredményeket kapunk, és annál valószínűbb, hogy egy ilyen riasztás valós. Ennek egyetlen hátránya, hogy ilyen mélységű szabályrendszert valós időben lehetetlen működtetni, amikor néhány másodperc van egy utalás teljesítésére. Ahogy a fenti példánkban is láthattuk, a problémát az generálja ebben az esetben, hogy a tranzakció már messze több számlán és országon túl lehet, mire a vizsgálat megvalósul. A riasztások kivizsgálására az MNB által meghatározottan 30 vagy 20 munkanap áll rendelkezésre.

A filtering, vagyis szűrőrendszer némileg másképp működik. Az kifejezetten a forgalom valós idejű szűrését hivatott elvégezni. A valós idejű szűrésnél elvárt a szankciós érintettség vizsgálata nemzetközi forgalom esetén. Ezek az utalások naponta több ciklusban kerülnek kiengedésre. Bármilyen hasonlóságot fedez fel a rendszer egy szankciós entitással, szintén egy riasztás generálódik, és a vizsgálat függvényében folytatódik a tranzakció vagy elutasításra kerül. Így szűrni lehet a bejövő és kimenő utalásokat is.

A filteringrendszer jellemzően karakteregyezőséget vizsgál a szankciós listákkal összevetve, miközben az előző, a monitoring pedig előre meghatározott paramétereket. A filteringrendszernél a program nemcsak gyanús tranzakciókat keres, hanem gyanús ügyfeleket is. A monitoringrendszer a beállított szabály szerint gyanús tranzakciókat detektál részünkre. Egy táblázatba összefoglalva jól összehasonlítható a két rendszer működése, feladata:

	Jogszabály	
	Kit. 2017. évi LII. törvény	Pmt. 2017. évi LIII. törvény
Feladat	Szankciók alá eső ügyfelek és tranzakciók kiszűrése és megakadályozása	Pénzmosási szokatlanság felismerése
Adatforrás	Szankciós listák	Letárolt historikus adatok
Módszer	Összevetés (karakteregyezőség)	Szokatlanságok keresése előre meghatározott paraméterek alapján
Intézkedés	Gyanús ügyfelek és tranzakcióik megállítása, intézkedés megtétele	Gyanús tranzakciók kiszűrése és ellenőrzése, intézkedés megtétele
Időpont	Valós időben, folyamatba építve	Utólagosan, nem valós időben

1. táblázat. Szűrőrendszerek csoportosítása[99]

A hazai és az egyéb nemzetközi szabályozások természetesen messze bővebbek, mint amire a jelen tanulmány lehetőséget ad, de azok bemutatása nem feladat. A tanulmány fő témájához szükséges jogi háttér és fogalmak ismertetésére hagyatkoztam. Talán így is látható, hogy szükséges lesz valamilyen szabály megalkotására a monitoringrendszerben, hogy a kriptovaluták forgalma is látható legyen.

[99] LUKÁCS Zsolt: Prezentáció. Budapest Institute of Banking, 2022.

Hatósági bejelentés

A 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról az alábbi tevékenységet várja el a szolgáltatóktól, jelen tanulmányban a banktól:

„*30. § (1) A szolgáltató vezetője, foglalkoztatottja és segítő családtagja*

a) pénzmosásra,

b) terrorizmus finanszírozására, vagy

c) dolog büntetendő cselekményből való származására

utaló adat, tény, körülmény (a továbbiakban együtt: bejelentés alapjául szolgáló adat, tény, körülmény) felmerülése esetén köteles a 31. § (1) bekezdésében megjelölt személynek haladéktalanul írásban bejelentést (a továbbiakban: bejelentés) tenni.

(2) Az (1) bekezdésben meghatározott bejelentésnek tartalmaznia kell

a) a szolgáltató által a 7-14/A. § alapján rögzített adatokat,

b) a bejelentés alapjául szolgáló adat, tény, körülmény részletes ismertetését és

c) a bejelentés alapjául szolgáló adatot, tényt, körülményt alátámasztó dokumentumokat, amennyiben azok rendelkezésre állnak.

(3) A szolgáltató vezetője, foglalkoztatottja és segítő családtagja pénzmosásra, terrorizmus finanszírozására vagy dolog büntetendő cselekményből való származására utaló adat, tény, körülmény felmerülését a végrehajtott vagy végrehajtandó ügylet és az ügyfél által kezdeményezett, de végre nem hajtott ügylet esetében, valamint a 13. § (8) bekezdésében meghatározott esetben is köteles vizsgálni.”

Elsősorban a fenti törvényi részlet határozza meg, hogy mi is pontosan egy hatósági bejelentés. Amennyiben a fentebb említett szűrőrendszerek esetében a szolgáltató valamilyen gyanús körülményt vél felfedezni, akkor a c) pont értelmében kötelessége haladéktalanul írásos bejelentést tenni. Ebből az idézetből az nem derül ki, hogy valójában ki részére szükséges ez. Minden bejelentést a Nemzeti Adó- és Vámhivatal Pénzmosás és Terrorizmusfinanszírozás Elleni Iroda (NAV PEI) részére kell megküldeni. A jogszabályi részletből látszik, hogy egy teljes, a szolgáltatók által elérhető összes információt tartalmazó vizsgálati anyagot kell megküldeni a riasztás és a gyanús tevékenység tudomásunkra jutását követően azonnal, vagyis haladéktalanul. Mindig kérdés, hogy ezekkel a bejelentésekkel a NAV oldalán valójában mi történik, hiszen a bejelentett esetek többségéről nincs visszajelzés a szolgáltató felé. A NAV néha küldd egy levelet, amelyben a bejelentés azonosítójára hivatkozva tájékoztatja a szolgáltatót, hogy a bejelentését a hatóság „sikeresen felhasználta”, jelentsen ez bármit is. A NAV-nak a nemzetközi pénzmosás elleni hatóságokkal is van kapcsolata, így képes nemcsak országon belüli mélyebb vizsgálatokra, de nemzetközi együttműködésre is. Ez természetesen a másik oldalról is igaz, a hazai NAV PEI-hez is érkeznek nemzetközi hatósági megkeresések, amelyek megválaszolásában, vagy akár folyamatban lévő nyomozásban is részt kell vennie.

Egy ilyen bejelentésben magánszemélyek, egyéni vállalkozók, illetve céges ügyfelek is szerepelhetnek, akár külön bejelentésben, vagy teljes cégláncolatok egyben küldésével is teljesíthető ez a bejelentési kötelezettség. ilyen hatósági bejelentéseket. A bejelentésnek van egy elvárt minimális adattartalma, de optimális esetben több információt tartalmaz, mintsem kevesebbet. Az esettől függ, hogy mi áll rendelkezésre, de törekedni kell ezek meglétére:

- a tranzakció ténye;
- a gyanút adó tényállás kifejtve;
- a kapcsolódó partnerek;
- nyilvános céginformációk;
- társbanki jelzés, ha volt;
- a tranzakció visszahívását kísérő üzenet, ha volt;
- a tranzakció forrását igazoló dokumentum.

Összességében a hatósági bejelentések kulcsfontosságúak. Ezzel a tevékenységgel ajánljuk a számunkra gyanús tevékenységet folytató ügyfeleket a hatóság számára is megvizsgálandónak. Minél kifinomultabb szűréseket és munkafolyamatokat alakít ki egy szolgáltató, annál nehezebb lesz nála pénzmosást megvalósítani. Minél inkább szofisztikáltabb kockázatérzékenységgel rendelkezik az adott szolgáltató, annál mélyebb elemzéseket tud elvégezni optimális esetben már a saját szűrőrendszerében, vagy kiegészítő riportok és információk segítségével. A kapott információkat pedig haladéktalanul továbbítja a NAV PEI részére, ahol vagy egyetértenek a gyanúval és eljárást kezdeményeznek, vagy megköszönik figyelmeztetésünket és a vizsgálatot lezárják. A szolgáltatók kizárólag egy gyanút jelentenek be, a cselekedet törvénytelenségének kimondására nem ők hivatottak.[100]

Fenyegetettségek az Európai Unióban

Az EU-ban, ezen belül Magyarországon is az alábbi fenyegetettségekkel kell szembenéznie a pénzügyi szektornak, amelyet az Európai Unió Kiberbiztonsági Ügynöksége (ENISA)[101] tesz közzé éves riportjaiban:

1. *ransomware* (zsarolóvírusok);
2. *malware* (rosszindulatú programok);
3. *social engineering threats* (pszichológiai manipuláció);
4. *threats against data* (adatokkal való visszaélés);

[100] Nemzeti Adó- és Vámhivatal Pénzmosás és Terrorizmusfinanszírozás Elleni Iroda. NAV, 2022. https://pei.nav.gov.hu/penzmosas-es-terrorizmusfinanszirozas-elleni-iroda/penzmosas-es-terrorizmusfinanszirozas-elleni-iroda; letöltés: 2022.12.11.

[101] ENISA Threat Landscape 2022. ENISA, 2022.11.03. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022; letöltés: 2022.12.11.

5. *threats against availability*: *Denial of Service* (túlterheléses támadás);
6. *threats against availability*: *Internet threats* (általános internetes támadások);
7. *disinformation – misinformation* (dezinformáció);
8. *supply-chain attacks* (ellátási láncok támadása).

Az első, amit a 2022-es listát átolvasva érdemes észrevenni, hogy a harmadik helyre „katapultált" a pszichológiai visszaélések réges-régi technikája, ez az ENISA 2021-es listáján még nem volt megtalálható. Még pontosabban azt lehetne mondani, a *cryptojacking* helyet cserélt a *social engineering threats*-szel; ebben kettős tartalom található: az első, hogy a kriptovaluták árfolyama lassan egy éve a töredékére esett vissza, ezért az érdeklődés is ugyanígy csökkent. A másik tartalom pedig a világjárvány lehet, hogy megváltozott az emberek hozzáállása, és újra előjött a *social engineering* lehetősége. Az ESET vírusírtó gyártója szerint a két legfőbb *social engineering* módszer a *spam* és az adathalászat.[102] A *social engineering* ennél sokkal több technikát is magában foglal. Van olyan, amelynek alig van köze az informatikához, például a *baiting* (csalogatás, beetetés), amikor a bűnöző jutalmat ajánl az információkért cserébe.[103] Érdekesség kedvéért érdemes megjegyezni, hogy a világ egyik leghíresebb hackere, Kevin Mitnick a 90-es években a *social engineering* technikáival, pontosabban rábeszéléses technikákkal jutott be számítógépes rendszerekbe.[104]

A pénzügyi intézmények, szolgáltatások ellen irányuló támadások egyre szofisztikáltabban működnek és egyre szélesebb körű megoldásokkal rendelkeznek, Magyarországon az NBSZ-NKI monitorozza és kezeli a támadásokat, de sajnos nem osztanak meg a nyilvánossággal részletes információkat, a heti hírlevelükben is csak olyan információ olvasható, hogy mekkora az adott fenyegetettségi fok, vagyis pl. 2022 50. hetében a zsarolóvírusok fenyegetettségi szintje közepes.[105] Ugyanakkor az MNB közölt ennél pontosabb, az NBSZ-NKI-tól származó adatokat, így számosítva olvashatjuk, hogy pl. 2022. február 1. – július 31. között összesen 21 fenyegetettséget követtek nyomon. Ennél részletesebb információt azonban ott sem kapunk, így azt sem tudjuk meg, hogyan sikerültek ezek a támadások és hogy mely intézettel szemben történt támadás. Gondolok itt arra, hogy bank, pénzügyi intézmény elleni vagy fintech-támadásról beszélhetünk.[106] Mindez azt jelzi, hogy Magyarországon is jelen vannak ezek a támadások. Az előbbi statisztika azt mutatja, hogy a hatóság havonta 4-5 ilyen támadásról szerez tudomást, a fenti jelentés a védelemben részt vevő összes hatóságtól is kapott információt. Az MNB az említett öt hónap alatt 765 incidensről tud, ami már egy aggasztóan magas mértékű tevékenységeket feltételez.

---

[102] Social engineering: Hogyan veszélyezteti ez a támadási forma vállalkozását? ESET, 2022. https://www.eset.com/hu/it-biztonsagi-temak-cegeknek/social-engineering/; letöltés: 2022.12.07.

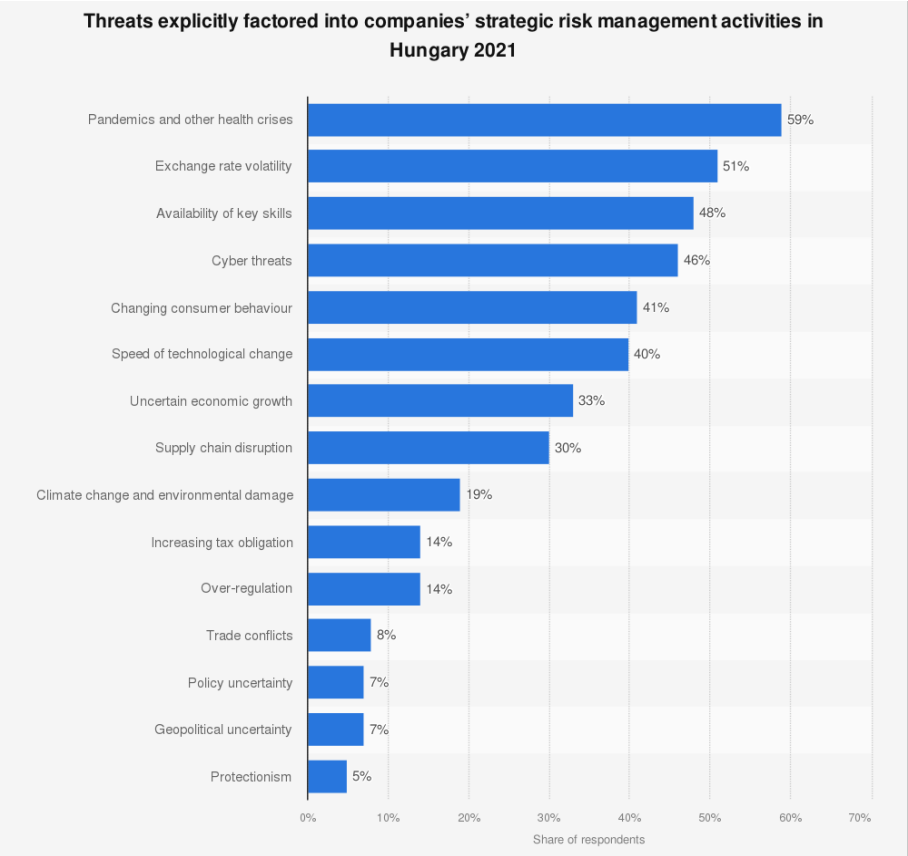
[103] 9 Examples of Social Engineering Attacks. Terranova Security, 2022.04.19. https://terranovasecurity.com/examples-of-social-engineering-attacks/; letöltés: 2022.12.08.

[104] MITNICK, Kevin: The History of Social Engineering & How to Stay Safe Today. Mitnick Security, 2022. https://www.mitnicksecurity.com/the-history-of-social-engineering; letöltés: 2022.06.17.

[105] Nemzetközi IT-biztonsági sajtószemle. 2022. 50. hét. NBSZ–NKI, 2022. https://nki.gov.hu/wp-content/uploads/2022/12/Sajtoszemle_50.-het.pdf; letöltés: 2023.02.13.

[106] A magyar pénzügyi szektor kiberfenyegetettségi térképe. MNB, 2022. https://www.mnb.hu/letoltes/kiberfenyegetettsegi-terkep-2022.pdf; letöltés: 2023.01.23.

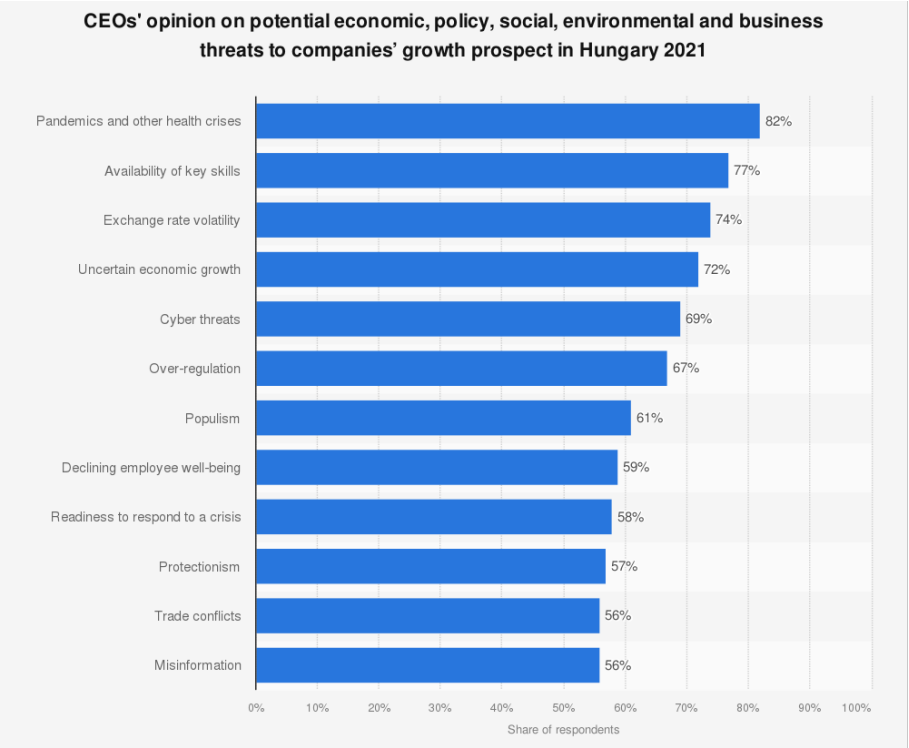
Érdemes megnézni, hogy a vállalatok hogyan vélekednek ebben a témában. A következő ábra a vállalatok alaptevékenységébe beépített veszélyeket mutatja. Mint látható, majdnem minden második vállalat számol az online fenyegetéssel.



1. ábra. A vállalatok stratégiai kockázatkezelési tevékenységébe beépített veszélyek Magyarországon 2021-ben[107]

A következő ábra még inkább hangsúlyozza a fenyegetések kezelésének fontosságát, mivel a vállalatvezetők közel kétharmada szerint ez a fenyegetettségi módszer hatással lehet a növekedésre:

[107] Threats explicitly factored into companies' strategic risk management activities in Hungary 2021. Statista, 2022. https://www.statista.com/statistics/1239649/hungary-threats-factored-into-companies-strategic-risk-management/; letöltés: 2022.07.15.



2. ábra. A vállalatvezetők véleménye a magyarországi vállalatok növekedési kilátásait érintő lehetséges gazdasági, politikai, társadalmi, környezeti és üzleti veszélyekről 2021-ben[108]

Mesterséges intelligencia a pénzügyekben

Nagyon fontos újra megemlékezni a Pmt. 2017. évi LIII. törvény részleteiről, röviden:

- pénzmosási szokatlanság felismerése;
- letárolt historikus adatok;
- szokatlanságok keresése előre meghatározott paraméterek alapján;
- gyanús tranzakciók kiszűrése és ellenőrzése, intézkedés megtétele;
- utólagosan, nem valós időben.

[108] CEOs' opinion on potential economic, policy, social, environmental and business threats to companies' growth prospect in Hungary 2021. Statista, 2022. https://www.statista.com/statistics/1234133/hungary-potential-threats-to-companies-growth/; letöltés: 2022.07.15.8

Ha ezeket gyorsan áttekintjük, akkor láthatjuk, hogy egyből olyan fogalom jut eszünkbe, mint a BigData, ami magában fogalja az összes olyan rendszert, amelyek a rendszeresen keletkező nagy mennyiségű adatot strukturált vagy strukturálatlan formában kezelik, tárolják, létrehozzák vagy kategorizálják. Az adatok tekintetében beszélhetünk szigorúan csak az elektronikus úton képződő adatokról, de a témával kapcsolatban tulajdonképpen minden olyan dolgot figyelembe kell vennünk, aminek információs értéke van. Ebből adódóan az emberek között zajló információcserét is számításba kellene vennünk, ami írásos és/vagy digitalizált forma hiányában nem túl hatékony. A Belényesi által leírt elvek szerint: „*A Big Data a nagy mennyiségű strukturálatlan adat, amely megjelenése az utóbbi évek felgyorsult technikai fejlődésének eredménye.*”[109] Tehát amikor a BigDatáról beszélünk, olyan állományra gondolunk, amely egy nyers információforrás, és amit szabad szemmel és kézzel szinte lehetetlen megfogni és elemezni, vagy kiolvasni belőle valós lényegi döntést támogató információkat.

Ugyanakkor be kell látnunk, hogy ezeknek az eszközöknek a lehetőségeit tárgyalva számításba kell vennünk az olyan rendszereket és technológiai vívmányokat is, amelyek képesek ezeket az adatokat megfelelően rendszerezni, csoportosítani, majd a végén könnyen átlátható, strukturált és vizualizált formában prezentálni.[110] A felhasználás előfeltétele, hogy a nyers adatokat már rendszerezett formában tároljuk a megfelelő metaadat-címkékkel és -tulajdonságokkal ellátve. Az előzetes munkát a legtöbb komplex rendszernél okosan megírt matematika algoritmusok végzik. Programtervezési és megoldási megvalósítási szempontból fontos megjegyezni, hogy a kezdeti fázisban ugyan sok hasonlóság lehet egy okos algoritmus és az MI adta lehetőségekre épülő szoftverek között, de lényegében nem hasonlíthatók össze. Míg az MI-t nem használó algoritmust szabványosított bejáratott módszerekkel erre szakosodott emberek írják és építik ki, addig egy MI megírásánál fontos, hogy szimulációk és próbálkozások révén, az úgynevezett mély tanulás módszerével hozzunk létre egy szoftvert, amely utána minimális hibaszázalékkal dolgozva önállóan is képes elvégezni feladatát. E kódok struktúrája és tartalma az ember számára általában átláthatatlan.[111] Egy algoritmus létrehozásánál van lehetőség egy kész MI-t használni (például tesztelések, szimulációk), de a végső termék nem tükrözi egy komoly MI-re épülő szoftver komplexitását. Mindezek ellenére az MI és az okos algoritmusok a köznyelvben sokszor hasonló tekintélyt és rangot kapnak, ezért nehéz a kettőt jól elválasztani egymástól, amikor ezeket az eszközöket tárgyaljuk. A strukturálatlan adatokat feldolgozás és rendszerezés után lényegesen egyszerűbb felhasználni. Ezek a BigData-algoritmusok képesek az adatokat rendszerezni és egységes formában tárolni különböző adattárházakban, ahonnan a különböző felhasználók igényük szerint további programokkal feldolgozhatják azokat.

---

[109] BELÉNYESI Pál: Digitális Platformok és a Big Data. In: VALENTINY Pál – KISS Ferenc László – NAGY Csongor István (szerk.): Verseny és Szabályozás – 2016. MTA KRTK Közgazdaság-tudományi Intézet, Budapest, 2016. pp. 127–162. http://real.mtak.hu/48669/1/teljes.pdf; letöltés: 2022.11.04.

[110] Uo.

[111] CHEN, Hsinchun – CHIANG, Roger H. L. – STOREY, Veda C.: Business Intelligence and Analytics: From Big Data to Big Impact. MIS Quarterly, Volume 36, Issue 4, December 2012. pp. 1165–1188. https://www.jstor.org/stable/41703503; letöltés: 2022.09.07.

Az adattárházakból kinyert adat az információtartalma és az olvashatósága szempontjából még nem érte el a teljes potenciálját, de szakemberek, szoftverek, algoritmusok és MI-k segítségével könnyen és gyorsan mindenki számára értelmezhető és vizualizált egységgé állnak össze. Ezek különböző diagramokban, táblázatokban kerülnek a döntéshozókhoz, akik az értelmezhető információ feldolgozása után képesek lesznek dönteni.[112] A rendelkezésre álló strukturált adat a cégek működésében jelentős szerepet tölthet be, mint például a vállalati működés optimalizálásánál, az értékesítés folyamat különböző lépéseinek fejlesztésénél, vagy akár vállalati stratégia tervezésénél, annak döntéshozatalánál is.

A mai világban a termékekkel és a szolgáltatásokkal foglalkozó szervezetek számára a legfontosabb dolog, hogy megtartsák ügyfeleiket és fogyasztóikat, ehhez azonban pontos adatokra van szükségük a felhasználóktól és a vásárlóktól. Nagyon sok módszer van már arra és implementálva a hétköznapi termékekbe, hogy hogyan mérjék a fogyasztók viselkedését a fogyasztott termékkel kapcsolatban.

A keletkező adatmennyiség nagyobb hányadáért természetesen a vállalatok felelnek, ez alól nem lehetnek kivételek a pénzügyi szektorba tartozó szervezetek sem vagyonkezelőkként, sem a kereskedelmi és a befektetői bankok, sem az egyszerű kereskedők. A megszámlálhatatlan tranzakciók során keletkező adatmennyiség egy jó részét a tranzakciós adatok köré épített védelmi protokollok és fordítási csomagok teszik ki. Bár az adatbiztonság és a személyes adatok kérdése sok helyen vitatott és tárgyalt, ebben a tanulmányban nem részletezem, de nem hagyható figyelmen kívül a BigData és az MI-k szempontjából sem.[113] A fentiekben tárgyaltak alapján már tudjuk, hogy a rendszerezett adatok nagy segítséget nyújthatnak egy jól kiépített rendszer szakszerű használóinak.

Az MI által nyújtott előnyök megértéséhez fontos, hogy először meghatározzuk azokat a tulajdonságokat és lehetőségeket, amelyekben az eltér egy lehetőségekben gazdag algoritmus működésétől. Fel kell térképeznünk, hogy mikortól is hívhatunk egy programot MI-nek, illetve mi az a különbség, ami a tudomány állásfoglalása és a köznyelv között eltérhet és félreértésre adhat okot. Több szempont alapján kell megvizsgálnunk egy ilyen szoftvert, hogy szakmai tekintetben is MI-minősítést kaphasson.

Összegezve, a mesterséges intelligencia a pénzügyekben az egész iparágat modernizálja a hagyományosan manuális banki folyamatok racionalizálásával és a generált adatokból mélyebb betekintést engedve, ami segít meghatározni, hogyan és hol történjenek a befektetések. Az MI megváltoztatja az ügyfélélményt is a gyorsabb, érintkezés nélküli interakciók létrehozásával, amelyek magukban foglalják a valós idejű hitelengedélyezést, a hatékonyabb csalásvédelmet és kiberbiztonságot.

---

[112] BENGIO, Yoshua – LECUN, Yann André: Scaling Learning Algorithms towards AI. In: BOTTOU, Léon – CHAPELLE, Olivier – DECOSTE, Dennis – WESTON, Jason (szerk.): Large-Scale Kernel Machines. The MIT Press, Cambridge, 2007. http://yann.lecun.com/exdb/publis/pdf/bengio-lecun-07.pdf; letöltés: 2023.01.07.

[113] HALASKA Gábor: Mire jó a Big Data? – interjú Huszics Györggyel. DigitalHungary, 2016.07.29. https://www.digitalhungary.hu/marketing/Mire-jo-a-Big-Data-interju-Huszics-Gyorggyel/2586/; letöltés: 2022.05.04.

A mesterséges intelligencia nagyban befolyásolja a pénzügyi szervezetek kockázatkezelésének módját, ami magában foglalja a biztonságot, a szabályozói megfelelést, a csalás, a pénzmosás elleni (AML) és a *know-your-customer* (KYC) irányelveket. A bankok, a befektetési cégek és a biztosítótársaságok azzal, hogy az MI az infrastruktúrájuk része, valós idejű számításokat végezhetnek a teljesítmény előrejelzésére, az anomális költési magatartás észlelésére és a megfelelés fenntartására – számos más alkalmazás mellett.

A pénzintézetek számára az MI lehetővé teszi, hogy felgyorsítsák és automatizálják a történelmileg manuális és időigényes feladatokat, például a piackutatást. Az MI gyorsan képes nagy mennyiségű adatot elemezni a trendek azonosítása és a jövőbeli teljesítmény előrejelzésének segítése érdekében, lehetővé téve a befektetők számára a befektetések növekedésének feltérképezését és a potenciális kockázatok értékelését. Az értékelés a biztosítások esetében is alkalmazható, ahol a személyes adatok összegyűjthetők és felhasználhatók a biztosítási fedezet és a díjak meghatározásához. Az MI kiberbiztonsági célokra is használható, különösen a csalárd tranzakciók azonosítására. A vásárlási viselkedés szoros figyelemmel kísérésével és a korábbi adatokkal történő összevetésével az MI képes jelezni a rendellenes tevékenységet, figyelmeztetni az intézményt és az ügyfelet is, hogy valós időben ellenőrizze a vásárlást vagy átutalást, és ha szükséges, lépéseket tegyen a probléma megoldására.

A banki ügyfelek számára az MI és a gépi tanulás (*machine learning* – ML) javíthatja az általános ügyfélélményt. Az online bankolás (azaz az érintésmentes bankolás) térhódítása minimalizálja a személyes interakciók szükségességét, de a virtuálisra történő áttérés több végponton (pl. okostelefonok, asztali számítógépek és mobileszközök) jelenthet sérülékenységet. Az MI számos alapvető banki tevékenységet, például a fizetéseket, befizetéseket, átutalásokat és ügyfélszolgálati kéréseket automatizálhatja, valamint képes kezelni a hitelkártyák és a hitelek kérelmezési folyamatait is, beleértve az elfogadást és az elutasítást is, szinte azonnali válaszokat adva. Bár a legtöbb intézmény úgy véli, hogy az MI és az ML javíthatja az üzletmenetet és versenyelőnyt biztosíthat számukra (a Forrester egyik felmérése szerint 98%), az ML-projektek 80–85%-a nem indul el különböző logisztikai és irányítási problémák vagy „utolsó mérföld" problémák miatt. Ez arra utal, hogy az intézményeknek az IT és az MI hálózati szakemberei segítségére van szükségük az MI-projektek befejezéséhez.

A logisztikán túl a pénzügyi szervezeteknek számos biztonsági és megfelelőségi előírással is szembe kell nézniük, mivel folyamatosan érzékeny és személyes adatokat használnak. Bármely MI-megoldásnak képesnek kell lennie arra, hogy megvédje ezeket az adatokat, és be kell tartania az iparág- és régióspecifikus irányelveket – mivel a pénzügyek globális jelentőségűek, és a vállalatok nagy részét lefedik. Az adatok puszta mennyisége önmagában is összetett kihívást jelent. Ahhoz, hogy bármilyen MI-megoldás hatékonyan működjön, az intézményeknek az összes adatot rendezett csővezetékekben és silókban kell tárolniuk, lehetővé téve az ML számára, hogy a piaci mozgásokat pontosan megjósolja és előrejelezze a konkrét üzleti céloknak megfelelően.

Fel kell tenni a kérdést, vajon a gépi tanulás-e a hatékony pénzügyi műveletek kulcsa? Az ML-alkalmazások a kockázatértékeléstől az eszközgazdálkodásig mindenre használhatók, az adatok felhasználásával kritikus betekintést nyerhetnek,

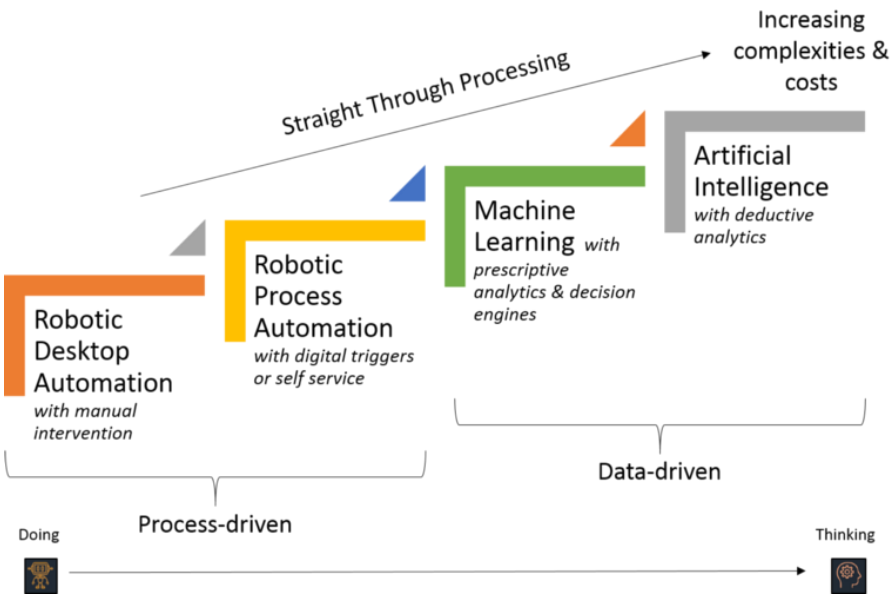
és az eredmények optimalizálásán túl racionalizálhatják a különböző folyamatokat. Az ML alkalmazása a pénzügyi folyamatokban egy fejlődő gyakorlat, amelyet az iparágban többféleképpen alkalmaznak. Annak változatos alkalmazásai a pénzügyekben számos új, az ML-lel kapcsolatos pénzügyi állást is megnyitottak. De először is segít megérteni az ML-t a pénzügyekben, és azt, hogy hogyan használható a karrierépítésben. Az ML az MI fogalomkörébe tartozik. Olyan algoritmusok tervezésével és fejlesztésével foglalkozik, amelyek képesek adatokból tanulni és előrejelzéseket készíteni az adatok alapján. Az ML-modellek a kognitív feladatok automatizálásának technológiáját biztosítják. A gépi tanulási technológiát különböző pénzügyi feladatokban használják, ilyenek a hitelpontozás, a befektetések nyomon követése és ajánlása, a csalásfelismerés és az algoritmikus kereskedés. Az ML segíthet a pénzügyi vállalatoknak abban, hogy jobb árképzési, kockázati és ügyfélmagatartási döntéseket hozzanak. Ez a technológia képes olyan modelleket építeni, amelyek javítják a nagy adathalmazok megértését, és olyan mintákat tárnak fel, amelyek megkönnyítik az új üzleti rendszerek és folyamatok kialakítását. A pénzügyi területen dolgozva számos előnnyel jár a különböző folyamatok ML-lel történő racionalizálása és automatizálása. A pénzügyi vállalatok e technológiákat olyan feladatok automatizálására használhatják, mint a papírmunka, a számítások, az adatfigyelés és a követelések feldolgozása. Így az alkalmazottak felszabadulhatnak, hogy több értékteremtő tevékenységre összpontosíthassanak. Egy másik kritikus terület Az ügyfelek elkötelezettsége, ahol a gépi tanulás és az MI felhasználható. Az IoT-eszközök jelentős mennyiségű adatot generálhatnak, amelyek segítik az ügyfelek viselkedésének és preferenciáinak a megértését. Az adatok ezután személyre szabott marketingkampányok létrehozására és az ügyfélszolgálat javítására is felhasználhatók. Összességében a jobb ügyfélkiszolgálás és a jobb ügyfélélmény jellemzően több eladást és magasabb ügyfél-elégedettségi arányt eredményez. Ezért mindenképpen érdemes nem összekeverni a mesterséges intelligencia, a gépi tanulás és az automatizálás fogalmakat.

A robotizált folyamatautomatizálás (Robotic Process Automation – RPA) olyan előre konfigurált szoftver használatára utal, amely üzleti szabályokat és előre meghatározott tevékenységkoreográfiát használ a folyamatok, tevékenységek, tranzakciók és feladatok kombinációjának autonóm végrehajtására egy vagy több, egymástól független szoftverrendszerben, hogy emberi kivételkezeléssel eredményt vagy szolgáltatást nyújtson.

Az MI[114] a kognitív automatizálás, a ML[115] az érvelés, a hipotézisgenerálás és -elemzés, a természetes nyelvi feldolgozás és a szándékos algoritmusmutáció kombinációja, az emberi képességek szintjén vagy azok felett meglátásokat és elemzést eredményez.

[114] Példa az MI-alkalmazásokra: SCHROER, Alyssa: 29 Examples of AI in Finance. Builtin, 2023.03.21. https://builtin.com/artificial-intelligence/ai-finance-banking-applications-companies; letöltés: 2023.04.05.

[115] Példa az ML-alkalmazásokra: 15 Projects on Machine Learning Applications in Finance. ProjectPro, 2021. https://www.projectpro.io/article/projects-on-machine-learning-applications-in-finance/510; letöltés: 2023.04.05.



3. ábra. A folyamatvezérléstől az adatvezérlésig[116]

Az egyszerűség kedvéért az RPA-ra szoftverrobotként is gondolhatunk, amely emberi tevékenységeket utánoz, míg az MI az emberi intelligencia gépek általi szimulációjával foglalkozik. A legalapvetőbb szinten az RPA a „csinálással" kapcsolatos, míg az MI és az ML a „gondolkodással", illetve a „tanulással" foglalkozik, vagy ha úgy tetszik: izom kontra agy.

Például a beszállítók elektronikus számlákat küldenek e-mailben, letöltjük a számlákat egy mappába, kiszedjük a releváns információkat a számlákból, és végül létrehozzuk a számlákat a könyvelőszoftverben. Ebben a forgatókönyvben az RPA alkalmas az e-mailek lekérdezésének (az egyszerűség kedvéért a lekérdezés az e-mail tárgya alapján történik), a mellékletek (azaz a számlák) letöltésének automatizálására egy meghatározott mappába, és a számlák létrehozására a könyvelőszoftverben (főként másolási és beillesztési műveletekkel). Másrészt MI-re van szükség a számlák intelligens „olvasásához", és az olyan lényeges információk kinyeréséhez, mint a számlaszám, a szállító neve, a számla esedékességi dátuma, a termékleírás, az esedékes összegek és még sok más. A számlák lényegében strukturálatlan, vagy legjobb esetben is félig strukturált adatok. A különböző beszállítóknak például különböző számlasablonjaik és formátumaik vannak. A különböző számlákon különböző számú sorszámozott tételek is szerepelnek. Mivel az RPA-ban minden tevékenységet kifejezetten programozni vagy szkriptelni kell, gyakorlatilag lehetetlen

[116] BIRNBAUM, Brad: Should You Be Using RDA For More Efficient Service? Forbes, 2018.09.07. https://www.forbes.com/sites/bradbirnbaum/2018/09/07/rda-rpa-service/?sh=a42c955b8e2b; letöltés: 2022.09.07.

megtanítani a robotot arra, hogy pontosan honnan vegye ki a releváns információkat minden egyes számlázott fogadáshoz. Ezért van szükség arra, hogy a mesterséges intelligencia intelligensen megfejtse a számlát, ahogyan egy ember tenné. Az biztos, hogy a számlafeldolgozást kizárólag RPA segítségével is lehet kezelni. Ebben az esetben azt fogjuk bevetni, amit általánosságban jelenlévő automatizálásnak nevezünk.

A robotizált desktopautomatizáció (Robotic Desktop Automation – RDA) olyan, mint egy virtuális asszisztens, amely kéz a kézben dolgozik az emberi alkalmazottakkal. Visszatérve a példánkhoz, a számlák letöltése után átmennek egy optikai karakterfelismerő (OCR) szoftveren, amely megpróbálja kinyerni a szükséges információkat. Ezt követően egy emberi alkalmazott hitelesíti ezeket az információkat, mielőtt visszaadja a munkát az RPA-robotnak, hogy létrehozza a számlákat a rendszerben. Az RPA- és az MI-megoldás használatának fő előnye tehát az, hogy (minimális emberi beavatkozással) egyenes feldolgozás érhető el. Hátránya a megnövekedett költség és a projekt összetettsége.

Az RPA erősen folyamatorientált – az ismétlődő, szabályalapú folyamatok automatizálásáról szól, amelyek jellemzően több, eltérő IT-rendszerrel való együttműködést igényelnek. Az RPA bevezetésénél általában előfeltétel a folyamatfeltáró workshopok megtartása, amelyek célja a meglévő „jelenlegi" folyamatok feltérképezése és dokumentálása a folyamatdefiníciós dokumentumban (PDD). A számlafeldolgozással kapcsolatos példánk esetében többek között azzal foglalkozunk, hogy elegendő mintaszámlát találjunk az ML-algoritmusok betanításához, biztosítsuk, hogy a mintáink jó minőségűek legyenek (különösen, ha a számlákat beszkennelik), és hogy a számlák reprezentatívak legyenek az adathalmazra nézve. Ezt követően a feladat a megfelelő ML-algoritmus kiválasztása, majd az algoritmus megfelelő képzése, hogy az képes legyen más új számlákat az embernél gyorsabban és pontosabban felismerni. Végső soron az RPA és az MI nem más, mint értékes eszköztár, amellyel segítheti szervezetének digitális átalakulását. Az RPA vagy az MI (vagy mindkettő) bevezetése a konkrét felhasználás esetétől függ, és a „célnak való megfelelés" biztosítása a legfontosabb. Az RPA esetében sok szervezet olyan okokra hivatkozik, mint például az „alacsonyan lógó gyümölcsök" megragadása, a gyors megvalósítás és piacra kerülés (általában hetek vagy hónapok alatt), az alacsony költségek és komplexitás, valamint egyéb okok. Sokan pedig okosan fogadnak arra, hogy az RPA-t az intelligens automatizáláshoz vezető digitális lépcső első lépcsőfokaként használják.

Összegzés

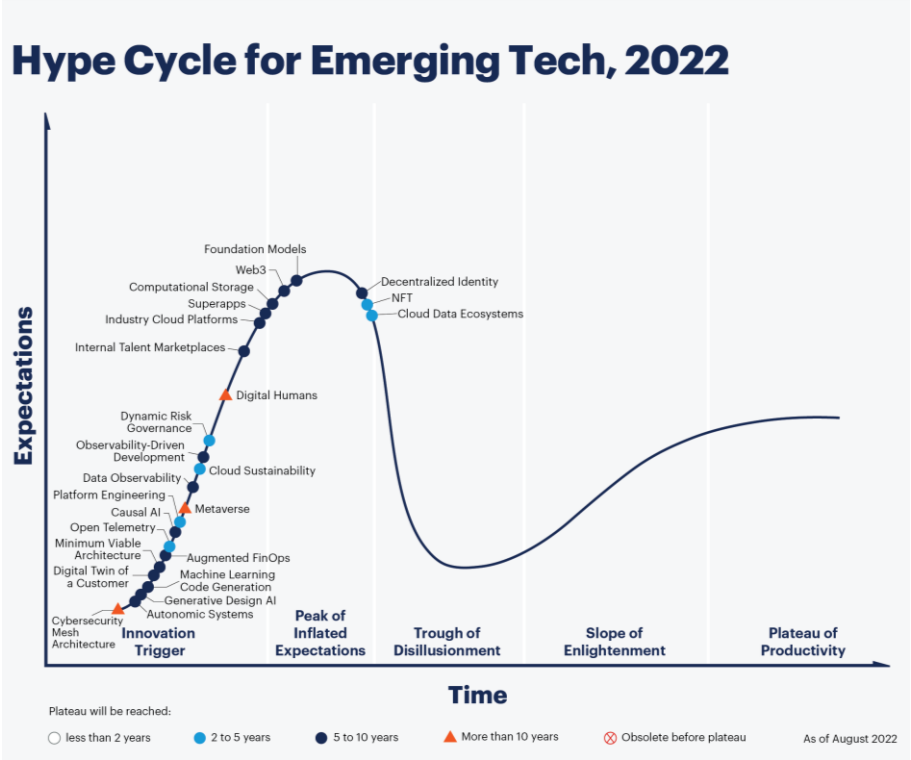
A pénzügyi technológiák, a fintech, a *financial technology* határozzák meg a mostani pénzügyi világunkat. A fintech három olyan korszakon lépdelt előre, amelyek elhozták számunkra az MI korszakát, ahol a számítógépek kereskednek egymással, és az ügyfelek interakcióit sem manuálisan végezzük. A fintech fejlődése együtt járt az informatika fejlődésével, a fintech 1.0-ás korszakot a távíró hozta el, a mostani, 3.5-ös korszakot meg olyan technológiák, mint a mobiltelefónia, a BigData, az internet, de még a számítási teljesítmény növekedése is hozzájárult ehhez a fejlődéshez.

Ezért nyugodtan kijelenthetjük, hogy a fintech fejlődése együtt mozog az informatika fejlődésével. Lehetne ezt evolúciós informatikának is hívni, mert a lépeseket vissza tudjuk követni az első számítógépig, ugyanakkor a „mutációk" tudatosan vitték előre a fejlődést, és szinte napról-napra hozzáadtak valamit a pénzügyi világhoz. Gondoljunk itt az első internetes banktól mekkora fejlődés a mobilbank megjelenése és a hozzá kapcsolható technológiák megléte. A pénzügyi megoldások digitalizációja az evolúciós informatikának köszönhető, egyszerű logikával kikövetkeztethető, hogy mihelyst a mobiltelefonok alkalmassá váltak mobilbankolásra, azonnal megjelentek a mobilbankok. De ugyanezt lehet elmondani az internetes bankolásra is, maga az internetes protokollok vagy azok titkosítása is akkor történt meg, amikor a technológia képessé vált rá. Külön tanulmányt lenne érdemes írni arról, hogy az internet az IPV4-es technológiával milyen régi, és erre a régi technológiára ültették rá a mostani alkalmazásokat, ez meg milyen biztonsági problémákkal jár a mai napig.

A pénzügyi technológiák felnőttek az informatika jelenlegi szintjére, első lépés a digitalizáció volt, utána az RDA, robotizált desktopautomatizáció, és igazából ez volt az, amikor a digitalizáció után rájöttek, hogy nem lehet mindent manuálisan feldolgozni. Utána jött az RPA, a robotizált folyamatautomatizálás, ami előre konfigurált szoftver használatára utal, amely üzleti szabályokat és előre meghatározott tevékenység-koreográfiát használ a folyamatok, tevékenységek, tranzakciók és feladatok kombinációjának autonóm végrehajtására egy vagy több, egymástól független szoftverrendszerben, hogy emberi kivételkezeléssel eredményt vagy szolgáltatást nyújtson.

Érdemes megnézni a Gartner-féle *hype cycle* ábrát (lásd 4. ábra), hogy milyen új technológiák fogják meghatározni a jövőnket. Ez azért is fontos, mert az olyan technológiák, mint az NFT (*non-fungible token*) vagy a *cloud-data* ökoszisztéma, már leszálló ágban vannak. Természetesen ezzel a nézettel lehet egyet nem érteni, de a Gartner már elég régóta foglalkozik a „*hype cycle*" módszertannal, ezért bízzunk abban, hogy az ábrán található MI-technológiák valóban felívelőben vannak.

Olyan kifejezések jelennek meg a jövőbeli irányok között, mint a *casual AI*, ami az MI olyan ága, amely leginkább hasonlít az emberi választásokra és döntésekre. De olyan kifejezéseket is lehet említeni, mint a fenntartható felhő vagy az *open telemetry*. A decentralizált identitás a magyarban némileg másképp hangzik, itt inkább a külön álló adatok felhasználhatóságáról beszélhetünk, vagyis az egészségügyi, adózási, oktatási és közlekedési adatok mind-mind különállóan szerepelnek, de egy központi rendszerből érhetők el. Ez a decentralizált identitás valójában a BigData-ról szól, ami leginkább az egyén személyes adatait tartalmazza. Azért van leszálló ágban, mert ez csak egyszerű adatkapcsolatról szól, míg az MI ennél sokkal többre képes. Az MI nemcsak mintázatokat keres, hanem ennél sokkal többre képes, olyan összefüggéseket tár fel, amelyeket manuális úton már nem vagyunk képesek kimutatni. A legfontosabb, hogy a háttérben lévő adatok, adatbázisok és strukturált erőforrások mind-mind rendelkezésre álljanak és stabilan, megbízhatóan működjenek.



4. ábra. A Gartner-féle *hype-cycle* 2022-es változata[117]

A pénzügyi adatok esetében nem szabad nem helyesen tárolni az adatokat, nincs lehetőség arra, hogy azt mondjuk az ügyfélnek, körülbelül megvan a fizetése vagy a befektetése. Ha az alapinfrastruktúra megbízhatóan működik, akkor jöhet a gépi tanulás vagy a mesterséges intelligencia. A pénzügyi termékek esetén a törvényi szabályozást mindenképpen kiemelném, hogy megfelelő tájékoztatást adjanak a pénzügyi szektor szereplőinek. A bizalomról is szól ez a kérdés, ugyanis a klasszikus pénzintézetekbe vetett bizalom a 2008-as válság körül megingott, onnan indultak a finech megoldások, ők alapvető bizalomra alapoztak, onnan kellett tovább építkezni. 14 év elteltével már komplett megoldások születtek, érdemes a Revolutra, Wise-ra gondolni. A digitalizáció, az evolúciós informatika az, ami elhozta ezt a korszakot, a továbblépés viszont kérdéses, méghozzá az, hogy milyen irányba. Ennek egyik lehetséges forgatókönyve a mesterséges intelligencia, a gépi tanulás és az, hogy minél jobban automatizáljuk azt, amit már nem lehetséges manuális módon elvégezni.

[117] PERRI, Lori: What's New in the 2022 Gartner Hype Cycle for Emerging Technologies. Gartner, 2022.08.10. https://www.gartner.com/en/articles/what-s-new-in-the-2022-gartner-hype-cycle-for-emerging-technologies; letöltés: 2022.08.15.

IRODALOMJEGYZÉK

9 Examples of Social Engineering Attacks. Terranova Security, 2022.04.19. https://terranovasecurity.com/examples-of-social-engineering-attacks/; letöltés: 2022.12.08.

A magyar pénzügyi szektor kiberfenyegetettségi térképe. MNB, 2022. https://www.mnb.hu/letoltes/kiberfenyegetettsegi-terkep-2022.pdf; letöltés: 2023.01.23.

Account Information Service Provider (AISP License). PSP Lab, 2022. https://psplab.com/services/pi-emi-authorisation/account-information-service-provider-aisp/; letöltés: 2022.09.04.

Adó-kódex. XXVII. évfolyam, 6. szám. Wolters Kluwer, 2018.

AFR – the Hungarian Retail Instant Payment System. European Payments Council (EPC), 2020.04.14. https://www.europeanpaymentscouncil.eu/news-insights/insight/afr-hungarian-retail-instant-payment-system; letöltés: 2022.09.30.

ARNER, Douglas W. – BARBERIS, Janos Nathan – BUCKLEY, Ross P.: The Evolution of Fintech: A New Post-Crisis Paradigm? University of Hong Kong Faculty of Law, Research Paper No. 2015/047. SSRN Electronic Journal, Volume 47, Issue 4, 2015. pp. 1271–1319. https://www.researchgate.net/publication/313365410_The_Evolution_of_Fintech_A_New_Post-Crisis_Paradigm; letöltés: 2022.10.11.

ASHTA, Arvind – BIOT-PAQUEROT, Guillaume: FinTech evolution: Strategic value management issues in a fast changing industry. Strategic Change, Volume 27, Issue 4, July 2018. pp. 301–311.

AYTAŞ, Baran – ÖZTANER, Serdar Murat – ŞENER, Emrah: Open banking: Opening up the 'walled gardens'. Journal of Payments Strategy & Systems, Volume 15, Issue 4, December 2021. pp. 419–431. https://discovery.ebsco.com/c/n3fo33/viewer/pdf/pcmbonva7z; letöltés: 2022.12.04.

Az Azonnali Fizetési Rendszer (AFR). Takarékbank, 2022. https://www.takarekbank.hu/azonnali-fizetesi-rendszer#; letöltés: 2022.03.25.

BARBASURA, Dmitrii: Working with Technical Service Providers under PSD2. Finextra, 2019.07.30. https://www.finextra.com/blogposting/17686/working-with-technical-service-providers-under-psd2; letöltés: 2022.05.04.

BELÉNYESI Pál: Digitális Platformok és a Big Data. In: VALENTINY Pál – KISS Ferenc László – NAGY Csongor István (szerk.): Verseny és Szabályozás – 2016. MTA KRTK Közgazdaságtudományi Intézet, Budapest, 2016. pp. 127–162. http://real.mtak.hu/48669/1/teljes.pdf; letöltés: 2022.11.04.

Belvo Team: Financial data enrichment: when data science meets open banking APIs. Belvo, 2022.02.09. https://belvo.com/blog/financial-data-enrichment-open-banking-apis/; letöltés: 2022.05.21.

BENGIO, Yoshua – LECUN, Yann André: Scaling Learning Algorithms towards AI. In: BOTTOU, Léon – CHAPELLE, Olivier – DECOSTE, Dennis – WESTON, Jason (szerk.): Large-Scale Kernel Machines. The MIT Press, Cambridge, 2007. http://yann.lecun.com/exdb/publis/pdf/bengio-lecun-07.pdf; letöltés: 2023.01.07.

BIRNBAUM, Brad: Should You Be Using RDA For More Efficient Service? Forbes, 2018.09.07. https://www.forbes.com/sites/bradbirnbaum/2018/09/07/rda-rpa-service/?sh=a42c955b8e2b; letöltés: 2022.09.07.

BUSSMANN, Oliver: The Future of Finance: FinTech, Tech Disruption, and Orchestrating Innovation. In: FRANCIONI, Reto – SCHWARTZ, Robert A. (szerk.): Equity Markets in Transition. Springer, Cham, 2017. pp. 473–486.

CEOs' opinion on potential economic, policy, social, environmental and business threats to companies' growth prospect in Hungary 2021. Statista, 2022. https://www.statista.com/statistics/1234133/hungary-potential-threats-to-companies-growth/; letöltés: 2022.07.15.

CHEN, Hsinchun – CHIANG, Roger H. L. – STOREY, Veda C.: Business Intelligence and Analytics: From Big Data to Big Impact. MIS Quarterly, Volume 36, Issue 4, December 2012. pp. 1165–1188. https://www.jstor.org/stable/41703503; letöltés: 2022.09.07.

DE JESSÉ, Marc Bayle: TARGET Instant Payment Settlement: The Eurosystem's response to an evolving payments landscape. Journal of Payments Strategy & Systems, Volume 12, Issue 4, 2018. pp. 322–327. https://discovery.ebsco.com/c/n3fo33/viewer/pdf/h4exqdmysf; letöltés: 2022.12.15.

Elérhetővé vált az azonnali fizetés! MNB, 2022. https://www.mnb.hu/azonnalifizetes; letöltés: 2022.08.25.

ENISA Threat Landscape 2022. ENISA, 2022.11.03. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022; letöltés: 2022.12.11.

Equity crowdfunding. European Comission, 2022. https://single-market-economy.ec.europa.eu/access-finance/guide-crowdfunding/different-types-crowdfunding/equity-crowdfunding_en; letöltés: 2022.07.01.

Evolution of Fintech: The 5 Key Eras. Zigurat, 2022.08.25. https://www.e-zigurat.com/innovation-school/blog/evolution-of-fintech/; letöltés: 2022.09.17.

EWIN, Brad: What is open banking: Everything you need to know. GoCardless, 2023. https://gocardless.com/guides/posts/open-banking/; letöltés: 2023.04.11.

FARROW, Gary S. D.: An application programming interface model for open banking ecosystems. Journal of Payments Strategy & Systems, Volume 14, Issue 1, March 2020. pp. 75–91. https://discovery.ebsco.com/c/n3fo33/viewer/pdf/jknjfoxnmz; letöltés: 2023.01.07.

FÁYKISS Péter – PAPP Dániel – SAJTOS Péter – TŐRÖS Ágnes: A FinTech-innovációk ösztönzésének szabályozói eszközei: Innovation Hub és Regulatory Sandbox a nemzetközi gyakorlatban. Hitelintézeti Szemle, 17. évfolyam 2. szám, 2018. augusztus. pp. 43– 67. https://hitelintezetiszemle.mnb.hu/letoltes/hsz-17-2-t2-faykiss-papp-sajtos-toros.pdf; letöltés: 2022.10.16.

GÁL István László: A pénzmosás hatályos büntetőjogi szabályozása Magyarországon. Pécs, 2007. https://www.mnb.hu/letoltes/pszafhu-rtfkonf-gali.pdf; letöltés: 2022.07.26.

GAYNOR, Brian: Payment Services Directive 2 – an overview. J.P.Morgan, 2022.05.18. https://www.jpmorgan.com/europe/merchant-services/insights/PSD2-all-you-need-to-know; letöltés: 2022.06.11.

GIRO. MNB, 2022. https://www.mnb.hu/penzforgalom/a-hazai-penzforgalmi-infrastruktura/giro; letöltés: 2022.11.23.

HALASKA Gábor: Mire jó a Big Data? – interjú Huszics Györggyel. DigitalHungary, 2016.07.29. https://www.digitalhungary.hu/marketing/Mire-jo-a-Big-Data-interju-Huszics-Gyorggyel/2586/; letöltés: 2022.05.04.

IT-biztonsági katasztrófa, ha a jobbról várt pofont balról kapjuk. Bitport, 2020.09.07. https://bitport.hu/it-biztonsagi-katasztrofa-ha-a-jobbrol-vart-pofont-balrol-kapjuk-api-security-balasys-open-api; letöltés: 2022.06.21.

KEATING, ROB: Open banking data: what is it and what is it good for? GoCardless, 2023. https://gocardless.com/guides/posts/open-banking-data/; letöltés: 2023.05.24.

Képesített pénzmosás és terrorizmus finanszírozása elleni szakértő képzés. Jegyzet. Bankárképző, Budapest, 2018.

KISKYTE, Adelina: kevin. reduces Decathlon's abandoned carts by 50%. Kevin, 2022.02.25. https://www.kevin.eu/blog/decathlon-success-story/; letöltés: 2022.05.11.

KISKYTE, Adelina: What are account-to-account (A2A) payments? Kevin, 2022.05.30. https://www.kevin.eu/blog/what-are-account-to-account-payments/; letöltés: 2022.06.13.

LAPLANTE, Phil – KSHETRI, Nir: Open banking: Definition and Description. Computer, Volume 54, Issue 10, October 2021. pp. 122–128.

LEE, In – SHIN, Yong Jae: Fintech: Ecosystem, business models, investment decisions, and challenges. Business Horizons, Volume 61, Issue 1, 2018. pp. 35–46. https://isiarticles.com/bundles/Article/pre/pdf/94413.pdf; letöltés: 2022.10.14.

LEMÁK Gábor. Itt a hazai open banking lista! 20-ból 17 magyar bank elstartolt. Fintechzone, 2019.03.18. https://fintechzone.hu/itt-a-hazai-open-banking-lista/; letöltés: 2022.03.11.

LEMÁK Gábor: Vizsgálja az MNB a fizetési kérelem kötelező bevezetését. Jön az AFR 2.0! FinTechZone, 2021.12.15. https://fintechzone.hu/vizsgalja-az-mnb-a-fizetesi-kerelem-kotelezo-bevezeteset-jon-az-afr-2-0/; letöltés: 2022.03.18.

LUKÁCS Zsolt: Prezentáció. Budapest Institute of Banking, 2022.

Market Guide: Fintech. Energy Catalyst, June 2020. https://energycatalyst.community/developer/wp-content/uploads/2020/12/Market-Guide-Fintech.pdf; letöltés: 2022.06.27.

Miért van szükség API-biztonságra? Computerworld, 2019.09.25. https://computerworld.hu/biztonsag/miert-van-szukseg-api-biztonsagra-268739.html; letöltés: 2022.10.01.

Mit jelent a KYC? Fintech.hu, 2018.09.01. https://fintech.hu/mit-jelent-a-kyc/; letöltés: 2022.04.05.

MITCHELL, Cory: Program Trading: Meaning, Purpose, Example. Investopedia, 2022.05.25. https://www.investopedia.com/terms/p/programtrading.asp; letöltés: 2022.08.17.

MITNICK, Kevin: The History of Social Engineering & How to Stay Safe Today. Mitnick Security, 2022. https://www.mitnicksecurity.com/the-history-of-social-engineering; letöltés: 2022.06.17.

NANAEVA, Zhamal – AYSAN, Ahmed Farouk – SHIRAZI, Nasim Shah: Open banking in Europe: The effect of the Revised Payment Services Directive on Solarisbank and Insha. Journal of Payments Strategy & Systems, Volume 15, Issue 4, December 2021. pp. 432–444. https://discovery.ebsco.com/c/n3fo33/viewer/pdf/37bjtmjevb; letöltés: 2022.07.28.

Nemzeti Adó- és Vámhivatal Pénzmosás és Terrorizmusfinanszírozás Elleni Iroda. NAV, 2022. https://pei.nav.gov.hu/penzmosas-es-terrorizmusfinanszirozas-elleni-iroda/penzmosas-es-terrorizmusfinanszirozas-elleni-iroda; letöltés: 2022.12.11.

Nemzetközi IT-biztonsági sajtószemle. 2022. 50. hét. NBSZ–NKI, 2022. https://nki.gov.hu/wp-content/uploads/2022/12/Sajtoszemle_50.-het.pdf; letöltés: 2023.02.13.

OMARINI, Anna Eugenia: Banks and Fintechs: How to Develop a Digital Open Banking Approach for the Bank's Future. International Business Research, Volume 11, Issue 9, 2018. http://www.ccsenet.org/journal/index.php/ibr/article/download/76769/42646; letöltés: 2022.08.01.

Open Banking and sharing your information online. MoneyHelper, 2022. https://www.moneyhelper.org.uk/en/everyday-money/banking/open-banking-and-sharing-your-online-banking-information; letöltés: 2022.10.11.

Open banking: Definition, How It Works, and Risks. Investopedia, 2022.04.04. https://www.investopedia.com/terms/o/open-banking.asp; letöltés: 2022.05.17.

Opportunities in Open Banking. FDATA North America, 2019. https://fdata.global/north-america/wp-content/uploads/sites/3/2019/04/FDATA-Open-Banking-in-North-America-US-version.pdf; letöltés: 2022.04.26.

PALMIERI, Alessandro – NAZERAJ, Blerina: Open Banking and Competition: An Intricate Relationship. In: ERCEG, Aleksandar – AKŠAMOVIĆ, Dubravka: Competition Law (in Pandemic Times): Challenges and Reforms. Conference book of proceedings In Osijek, 13 May 2021. pp. 217–237. https://hrcak.srce.hr/ojs/index.php/eclic/article/view/18822/10290; letöltés: 2022.06.25.

Pán-európai elszámolásforgalmi rendszerek. MNB, 2022. https://www.mnb.hu/penzforgalom/az-euro/pan-europai-elszamolasforgalmi-rendszerek; letöltés: 2022.11.23.

PERRI, Lori: What's New in the 2022 Gartner Hype Cycle for Emerging Technologies. Gartner, 2022.08.10. https://www.gartner.com/en/articles/what-s-new-in-the-2022-gartner-hype-cycle-for-emerging-technologies; letöltés: 2022.08.15.

PUSCHMANN, Thomas: Fintech. Business and Information Systems Engineering, Volume 59, Issue 1, 2017. pp. 69–76. https://doi.org/10.1007/s12599-017-0464-6; letöltés: 2022.05.21.

Rewards-based crowdfunding. European Comission, 2022. https://single-market-economy.ec.europa.eu/access-finance/guide-crowdfunding/different-types-crowdfunding/rewards-based-crowdfunding_en; letöltés: 2022.07.01.

RODRIGUES, Abílio: PSD2 explained: understand the regulations and fraud monitoring. GoCardless, 2023. https://gocardless.com/guides/posts/an-introduction-to-psd2/; letöltés: 2023.04.08.

SHLIAKHOUSKI, Alexey: Security In Open Banking: Concerns And Solutions. Forbes, 2021.08.19. https://www.forbes.com/sites/forbestechcouncil/2021/08/19/security-in-open-banking-concerns-and-solutions/?sh=3612304c6329; letöltés: 2022.10.01.

Social engineering: Hogyan veszélyezteti ez a támadási forma vállalkozását? ESET, 2022. https://www.eset.com/hu/it-biztonsagi-temak-cegeknek/social-engineering/; letöltés: 2022.12.07.

TANDA, Alessandra – SCHENA, Cristiana-Maria: FinTech, BigTech and Banks. Digitalisation and Its Impact on Banking Business Models. Palgrave Macmillan, London, 2019.

The revised Payment Services Directive (PSD2) and the transition to stronger payments security. European Central Bank, March 2018. https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html; letöltés: 2022.06.04.

The Story Behind The Card. Diners Club International, 2022. https://www.dinersclubus.com/home/about/dinersclub/story; letöltés: 2023.01.04.

Threats explicitly factored into companies' strategic risk management activities in Hungary 2021. Statista, 2022. https://www.statista.com/statistics/1239649/hungary-threats-factored-into-companies-strategic-risk-management/; letöltés: 2022.07.15.

TURZÓ Ádám Pál: Készül az AFR 2.0 – Elmondta az MNB, mit terveznek az azonnali fizetéseknél. Portfolio, 2022.12.12. https://www.portfolio.hu/bank/20220912/keszul-az-afr-20-elmondta-az-mnb-mit-terveznek-az-azonnali-fizeteseknel-564845; letöltés: 2023.01.10.

VOAS, Jeffrey – LAPLANTE, Phil – LU, Steve – OSTROVSKY, Rafail – KASSAB, Mohamad – KSHETRI, Nir: Cybersecurity Considerations for Open Banking Technology and Emerging Standards. National Institute of Standards and Technology, Gaithersburg, 2022. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8389-draft.pdf; letöltés: 2023.01.17.

VRAZSOVITS Rita: Fizetési kérelem: már kérni is lehet az utalást, nemcsak kapni. Bank360.hu, 2022.08.19. https://bank360.hu/fizetesi-kerelem; letöltés: 2022.10.27.

VRAZSOVITS Rita: Március 2-án indul az azonnali fizetési rendszer Magyarországon! Bank360.hu, 2022.01.18. https://bank360.hu/blog/azonnali-fizetesi-rendszer; letöltés: 2022.11.04.

What is API? Red Hat, 2022.06.02. https://www.redhat.com/en/topics/api/what-are-application-programming-interfaces; letöltés: 2022.08.11.

What is SCA, and what is it good for? Tink, 2021.04.13. https://tink.com/blog/open-banking/strong-customer-authentication/; letöltés: 2022.09.16.

What is TARGET Instant Payment Settlement (TIPS)? European Central Bank, 2022. https://www.ecb.europa.eu/paym/target/tips/html/index.en.html; letöltés: 2022.06.04.

ZACHARIADIS, Marcos – OZCAN, Pinar: The API Economy and Digital Transformation in Financial Services: The Case of Open Banking. SWIFT Institute Working Paper, 2016-001. http://dx.doi.org/10.2139/ssrn.2975199; letöltés: 2022.09.07.