A megfelelőségbiztosítási funkció szerepe a digitalizáció, mesterséges intelligencia és robotizáció idején a pénzügyi szektorban*

Harkácsi Gábor József – Szegfű László Péter

Elemzésünket hiánypótlónak szánjuk abban a vonatkozásban, hogy vizsgálódásunk fókuszában a megfelelésbiztosítási funkció előtt álló kihívások és a rájuk adandó válaszok állnak, komplex megvilágításba helyezve a nemzetközi és nemzeti jogszabályi környezet minősége, valamint az etikai, gondossági keretek szerepe közötti kényes egyensúly megteremtésének hiányát és igényét. A digitalizáció eredményeként a FinTech-vállalkozások megkerülhetetlenné váltak a pénzügyi szolgáltatások világában, és ennek hatására az inkumbens szereplők üzleti és kockázati modellje átalakult, ami erőteljes hatással van a szabályozási környezetre és ezzel párhuzamosan a bizalom, a megbízhatóság, valamint az etikus, prudens magatartás alakulására, változására. A szabályozás szükségszerűen mindig elmaradásban lesz az új igényekhez és a megjelenő új technológiákhoz képest, mivel ezek működését és kockázatait teljeskörűen meg kell ismerni ahhoz, hogy megfelelő szabályozást lehessen rájuk kialakítani. Ebben a változó környezetben kell a megfelelőségbiztosítási funkciónak megtalálnia a helyét és szerepét ahhoz, hogy hathatós támogatást tudjon nyújtani a pénzügyi szektor szereplőinek a szabályok betartásában, valamint a tisztességes és etikus magatartás biztosításában.

Journal of Economic Literature (JEL) kódok: D18, D53, E58, G01, G21, O33, O52

Kulcsszavak: digitalizáció, mesterséges intelligencia, etika, compliance, bizalom, bankok, FinTech, PSD2

1. Bevezetés

Számos tanulmány és cikk jelent meg a nemzetközi, valamint a hazai szakirodalomban, vizsgálva a bizalom és az etika újkori szerepét és arra keresve a választ, hogy a bizalom, a megbízhatóság, az etikai normák és etikus magatartás hogyan alakul a FinTech világában. Ezek az írások, ahogy jelen cikkünk is, mind azt erősítik, hogy

* A jelen kiadványban megjelenő írások a szerzők nézeteit tartalmazzák, ami nem feltétlenül egyezik a Magyar Nemzeti Bank hivatalos álláspontjával.

Harkácsi Gábor József a Magyar Nemzeti Bank senior compliance szakértője. E-mail: harkacsig@mnb.hu
Szegfű László Péter a Magyar Nemzeti Bank osztályvezetője. E-mail: szegful@mnb.hu

A magyar nyelvű kézirat első változata 2020. szeptember 14-én érkezett szerkesztőségünkbe.

DOI: http://doi.org/10.25201/HSZ.20.1.152170

szerepük fontos, hiszen megteremtik az ellenőrzés és felelősségre vonás lehetőségét akkor is, amikor a FinTech-világ átfogó szabályozása még nem zárult le. Azt is előrevetítik, hogy a jelenleg alkalmazott etikai, magatartási normák és a hiányos nemzetközi szabályozás megmérettetésre kerülnek, amikor gazdasági lassulás, recesszió következik be. A bizalom alapvetően a problémamentes együttműködésen, a feladatok közös megoldásának élményén, az etikus viselkedésen és a kölcsönös morális elkötelezettségen alapul. Az üzleti kapcsolatokban a bizalom bizalmat szül, és a megszerzett bizalom megteremti a megbízhatóság vélelmét. A bizalom hiánya azonban romboló hatással van, az együttműködési hajlandóság gyengüléséhez, végső soron az üzleti kapcsolat sérüléséhez vezet. A megfelelőségi terület (compliance) szerepe és felelőssége a megfelelőség, valamint az etikus viselkedés biztosításában, így a bizalom és megbízhatóság megteremtésében és fenntartásában rendkívül komplex. Egyfelől a szervezet belsőkontroll-rendszerének részeként felel a megfelelőségi kockázatok[1] szervezeti szintű azonosításáért és kezeléséért. Másfelől a megfelelőségi terület nemcsak egy szervezeti egység vagy funkció, hanem egy komplex rendszer is egyben, egy olyan szemléletbeli megközelítés, aminek a gyakorlatban és az egész szervezetben kell érvényesülnie. Ez utóbbihoz szervezeti és funkcionális függetlenség, határozott felsővezetői támogatás és a szervezet egészét tekintve erős kapcsolati hálózat megléte szükséges.

A pénzügyi ágazat, különösen a bankszektor már a kezdetektől bizalmi alapokon működik, így széleskörű tapasztalattal rendelkezik arról, hogy hogyan kell etikusan működni, hogyan kell felépíteni és megtartani az ügyfelek és a piac bizalmát, ismerve, hogy mindez milyen gyorsan elveszíthető. A bizalom és a megbízhatóság ismételt felépítése és visszaszerzése pedig, ahogy ez a gazdasági válságokat követően már többször bebizonyosodott, lassú és nehéz folyamat. A bizalom, a megbízhatóság, az etika, az üzleti jó hírnév értéket jelent, és egyben a sikeres működés és profitabilitás eszköze (*Müller – Kerényi 2019*).

Felmerül azonban a kérdés, hogy az etikai elvárások, szakmai követelmények, vonatkozó szabályozások hogyan változnak, alakulnak át, amikor a pénzügyi szektor FinTech[2]-szereplői (továbbiakban: FinTech) mint pénzügyi innovációs megoldásokat

[1] A megfelelőségi kockázatok alatt annak veszélyét értjük, hogy törvényi vagy felügyeleti szankciók, jelentős pénzügyi veszteség vagy hírnévvesztés éri a szervezetet amiatt, hogy nem tartott be a tevékenységére vonatkozó valamely törvényt, előírást, szabályt, önszabályozó testületi előírást vagy viselkedési normát.

[2] A financial technology (a továbbiakban: FinTech) olyan, digitális környezetben létrehozott és digitális eszközökön működtetett innovatív termékek és szolgáltatások összefoglaló elnevezése, amelyek a pénzügyi szektor intézményei (hitelintézetek, biztosítók, befektetési szolgáltatók, pénztárak, egyéb pénzforgalmi intézmények stb.) által nyújtott pénzügyi szolgáltatások korszerű versenytársaként a szolgáltatási kínálat kibővítésére jönnek létre abból a célból, hogy az adott szolgáltatás igénybevétele kényelmesebb, gyorsabb és/vagy olcsóbb legyen, vagy az innováció jegyében új ügyféligényeket generáljon. Ugyanakkor a FinTech egy olyan új iparág megnevezése is, amely innovatív technológiát alkalmaz a pénzügyi tevékenységek fejlesztésére.

kínáló vállalkozások[3] belépnek a pénzügyi szolgáltatások világába, kikényszerítve a hagyományos hitelintézetek, bankok, biztosítók és más pénzügyi intézmények üzleti modelljének átalakítását, nem beszélve arról, hogy olyan előttünk álló kihívásokra is reagálni kell, mint az új koronavírus-járvány digitalizációt érintő következményei. A digitális technológiák megváltoztatják életünket: a mesterséges intelligencia, a big data-elemzés, a blokklánc és a felhő alapú technológiák számtalan módon javítják világunkat, de az új lehetőségek mellett új sebezhetőségeket, hibalehetőségeket – ezáltal eddig ismeretlen kockázatokat is hoznak. A szabályozó környezet azonban mindig hátrányban lesz a megjelenő új technológiák gyors fejlődésével szemben, mivel a szabályozóknak először meg kell ismerniük a technológiák gyakorlati működését és kockázatait, hogy megfelelő, de nem túlzóan korlátozó szabályokat alkothassanak. Mivel a digitális pénzügyi infrastruktúra akadálymentes építéséhez szükséges egységes követelményeknek még csak részben sikerült eleget tenni, ezért áthidaló megoldásként egyre inkább előtérbe kerültek az etikai, bizalmi elvárások, üzletviteli magatartási kódexek.

2. Veszélyek és válaszok

Az új technológiák világszerte jelentős előnyöket hoztak, de veszélyeket is jelentenek. Lényeges előnyök a gyors ügyfélszerzés, az ügyfélélmény növelése, a költségek csökkentése, a hatékonyságnövekedés és a nagyobb fokú átláthatóság. Ezenkívül az innováció hatékony eszköz a pénzügyi kirekesztés felszámolására azáltal, hogy magas szintű szolgáltatásokat kínál azoknak is, akik korábban ezeket nem engedhették meg maguknak. A digitális technológiák egyik legnagyobb felhasználójaként a pénzügyi szektor jelentős szerepet játszik a gazdaság és a társadalom digitalizálódásában. A pénzügyi szolgáltatásokat nyújtó FinTech-vállalkozások megtörik a klasszikus banki, pénzügyi szolgáltatások évszázados egyeduralmát, új csatornákat nyitva az ügyfelek számára. Piacra lépésük fokozza a versenyt, de veszélyeket, illetve a már ismert működési és biztonsági kockázatok súlyosbodása mellett új kockázatokat is hordoznak, miközben működésük alapvető szabályozási és társadalmi kérdéseket is felvet. A feltárt kockázatok több okból is súlyosbodhatnak. A legfőbb okok, hogy az elmúlt években az új technológiák tömeges megjelenése, valamint a pénzügyi szolgáltatások nyílt igénybevétele (például a nyílt bankolás) eredményeként az új, ügyfélélmény-fókuszú szolgáltatások megjelenése gyorsan megváltoztatta a verseny dinamikáját, és az üzleti modellek változása is gyorsabban következett be. A FinTech-vállalkozások aktívan és sikeresebben hatolnak be a hagyományos pénzügyi szolgáltatások területére, és a szolgáltatásuk nyújtása során alkalmazott digitális technológiák – különösen, amikor szorosan integrálódva a pénzügyi intézmények

[3] FinTech-vállalkozások azok a szereplők, amelyek a klasszikus pénzügyi intézmények, hitelintézetek, biztosítók, brókerek stb. számára, vagy tőlük független, önálló szolgáltatás nyújtása céljából készítenek FinTech-alkalmazásokat, beleértve a PSD2 szerinti számlainformációs (AISP), valamint fizetéskezdeményezési szolgáltatást (PISP) nyújtó szolgáltatókat, melyeket a köznyelv harmadik fél szolgáltatóknak (TPP) nevez.

működésébe hozzáférnek az ügyfelek érzékeny adataihoz – a működési kockázatok új dimenzióját nyitották meg. Az ügyféladatokhoz való hozzáférés általában az interneten keresztül, interfészek közötti kommunikáció útján, kezelésük, feldolgozásuk, tárolásuk pedig jellemzően felhőszolgáltatások igénybevételével történik, így az alkalmazott technológiai megoldások az internet jellegéből, illetve az internetet használó számos, a szolgáltatásba bevont alvállalkozó különféle biztonságú megoldásaiból fakadóan jelentenek kockázatot.

Mindezeket a kockázatokat figyelembe véve, különösen, hogy a FinTech-vállalkozások jellemzően határon átívelő, internet alapú szolgáltatások keretében nyújtják szolgáltatásaikat, a felhasználók biztonsága érdekében elengedhetetlen lépés volt az Európai Unió egészében egységes biztonsági követelmények szigorítása és a magas színvonalú fogyasztóvédelem biztosítása ezen szolgáltatások igénybevételéhez is.

2.1. A pénzforgalmi szolgáltatásokra vonatkozó előírások szigorítása

Az európai jogalkotó, az Európai Bankhatóság (EBA) az Európai Központi Bank (EKB) közreműködésével kialakította a pénzforgalmi szolgáltatások nyújtásához szükséges szigorúbb szabályozási keretrendszert, így 2016. január 12-én lépett hatályba a PSD2[4], amelyet 2018. január 13-i határidővel kellett a tagállamoknak a saját jogrendjükbe implementálni. A PSD2 az ügyfelek – és kiemelten a fogyasztók – hatékony védelme mellett azzal a céllal jött létre, hogy szabályozott környezetet teremtsen a digitális pénzügyi szolgáltatások fejlődéséhez, és támogassa az új, nem csupán hitelintézeti hátterű szolgáltatók belépését a pénzügyi szolgáltatások piacára, továbbá növelje a fizetések biztonságát, tekintettel az online fizetések egyre nagyobb térnyerésére. Ugyanakkor a PSD2 hatalmas lehetőségeket nyit meg a harmadik fél szolgáltatóknak nevezett FinTech-szereplők előtt azzal, hogy engedélyezi számukra a hozzáférést az ügyfél fizetési számlájához. Az ügyfél személyes adatainak védelmének biztosítása az általános adatvédelmi rendelet (GDPR[5]) és a vonatkozó nemzeti törvényi szabályozás szerepekörébe tartozik. A pénzügyi ágazati titokkörbe sorolt adatok védelmére a vonatkozó pénzügyi ágazati törvények, az érzékeny fizetési adatokra pedig a pénzforgalmi szolgáltatás nyújtásáról szóló törvény[6] (Pft.) tartalmaz további előírásokat[7]. A PSD2, illetve az azt a hazai jogrendbe átültető pénzforgalmi jogszabályok szerint a harmadik fél szolgáltatók a szolgáltatásuk nyújtása során kizárólag az ügyfél hozzájárulása alapján és olyan mértékben férhetnek

[4] A belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről szóló 2015. november 25-i (EU) 2015/2366 európai parlamenti és tanácsi irányelv

[5] A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet

[6] A pénzforgalmi szolgáltatás nyújtásáról szóló 2009. évi LXXXV. törvény

[7] A Pft. 2. § 5a alpontja alapján érzékeny fizetési adatnak minősül minden olyan adat, amely csalás elkövetésére alkalmazható, ideértve a személyes hitelesítési adatokat is, azzal, hogy a fizetés-kezdeményezési szolgáltatás vagy számlainformációs szolgáltatás tekintetében nem érzékeny fizetési adat a számlatulajdonos neve és a fizetési számlájának száma.

hozzá az ügyfeleik fizetéseihez kapcsolódó adataihoz, amilyen mértékben a szolgáltatás nyújtásához feltétlenül szükséges.

2.2. Az adatok védelmének megerősítése

Az ügyféladatok megfelelő védelmének biztosítása a vonatkozó törvények előírásai szerint jellemzően a szolgáltatók felelőssége. A GDPR megjelenése a beígért súlyos szankciók miatt még jobban szigorította a pénzügyi intézmények egyébként is szigorú adatvédelmi és adatbiztonsági szemléletét. Sajnos a GDPR csak a személyes adatok védelméről szól, így a szolgáltatók igyekeztek az adatvédelmi és adatbiztonsági szabályaikat és megoldásaikat az ügyfeleik személyes adataira fókuszálni, nem törődve azzal, hogy a szolgáltatóknál más szenzitív adatok is megjelenhetnek, amelyeknek csak egy része tartozik a személyes adatok körébe.

Az adatbiztonság megfelelő kialakításához nélkülözhetetlen, hogy a piaci szereplők teljeskörűen felmérjék az általuk kezelt adatvagyont, beleértve a személyes adatokon felül a különféle pénzügyi ágazati törvények által titok körbe sorolt adatokat, az üzleti titkokat, a nyilvános, de védendő adatokat, valamint az olyan szenzitív adatokat, amelyekre nincs ugyan jogszabályi előírás, de befolyásolhatják az intézmény megfelelő működését, biztonságát vagy akár a piaci helyzetét. Az adatokat, valamint az adatokat kezelő rendszereket biztonsági osztályokba kell sorolni, az információbiztonság három fő alappilére, a bizalmasságuk, a sértetlenségük és a rendelkezésre állásuk szerint. Az információbiztonsági osztályokra vonatkozó kockázatokat fel kell mérni, és a megfelelő intézkedésekkel kezelni kell, figyelembe véve a vonatkozó jogszabályi előírásokat, valamint a vonatkozó etikai és társadalmi elvárásokat, normákat is.

2.3. Ügyfél-átvilágítás, a távoli szerződéskötés új lehetősségeinek megnyitása és szabályozása

Az EU egyre szigorúbb AML-direktívái és -rendeletei[8], illetve az azokat a hazai jogrendbe átültető Pmt., valamint a végrehajtására kiadott Magyar Nemzeti Bank (MNB) rendelet[9] alapvető biztosítékokkal szolgál az uniós pénzügyi rendszer integritásának a pénzmosással és terrorizmusfinanszírozással szembeni védelméhez. A Pmt. és a vonatkozó MNB-rendelet ezenfelül új lehetőségeket nyitott a pénzügyi innovációs technológiák térnyerésében. Egyes esetekben, így különösen akkor, ha a törvény hatálya alá tartozó intézmények[10] új ügyfelekkel létesítenek üzleti kapcsolatot[11], ún. ügyfél-átvilágítást kell végezniük. E törvény már a 2017-es hatályba

[8] A vonatkozó normákat az MNB honlapján összegyűjtve hivatkozza: https://www.mnb.hu/felugyelet/szabalyozas/penzmosas-ellen/kotelezo-es-iranyado-szabalyok/eu-jogszabalyok

[9] 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 szóló 26/2020 (VIII.25.) MNB-rendelet

[10] Pmt. 1. § (1) bekezdés

[11] Pmt. 6. § (1) bekezdés

lépésekor lehetőséget nyitott a távoli, elektronikus formában végzett ügyfél-átvilágításra az ún. auditált elektronikus hírközlő eszköz útján, amelynek technológiai részletszabályainak megalkotására a Magyar Nemzeti Bankot hatalmazta fel. Az MNB-rendelet az első időkben a személyes megjelenéshez leginkább hasonlító videó-chat alapú ügyfél-átvilágítást preferálta, később különféle selfie-készítést alapul vevő technológiákat is engedélyezett. A rendelet legújabb módosításával lehetővé vált az elektronikus tárolóelemet is tartalmazó személyi igazolványok, illetve a biometrikus chipet tartalmazó úti okmányok alkalmazásával a pénzmosás-megelőzési célú ügyfél-átvilágításhoz kapcsolódó azonosítás, mely lényegesen megkönnyítheti a távoliügyfél-akvirációt. Mivel időközben a Ptk. írásbeli alakisági követelményei is egyszerűsödtek, az MNB úgy ítélte meg, hogy amennyiben az ügyfél a pénzmosás-megelőzés céljából az auditált elektronikus hírközlő eszközön keresztül végzett ügyfél-átvilágítás során jognyilatkozatot is tesz, és a jognyilatkozat változatlan visszaidézését a szolgáltató lehetővé teszi, akkor az egyúttal megfelel a szerződéskötésre vonatkozó írásbeli alakisági követelményeknek is. Így a távoli ügyfél-akvirációs folyamat már azokban az esetekben is megszakítás nélkül, online végigvihető, amelyekben a vonatkozó törvény a szerződéskötésre írásbeli alakiságot ír elő, jelentősen támogatva ezzel a FinTech-szereplők ügyfélszerzését.

3. A szabályozó szereplők felelőssége

A szabályozó szereplők felelőssége kettős: egyrészt támogató jellegű, másrészt figyelemmel kell lenniük a biztonsági és egyéb kockázatokra. Biztosítaniuk kell, hogy az új technológiák, üzleti innovációk elterjedése előtt a jogszabályi korlátok ne képezzenek akadályt, másrészt meg kell könnyíteniük az új szereplők piacra lépését, biztosítva a tisztességes versenyt úgy, hogy az új szereplők ne kerüljenek versenyhátrányba, de a hagyományos pénzügyi intézmények érdekei se sérüljenek, természetesen mindezt a biztonsági kockázatok szem előtt tartásával. Szabályozási szempontból fontos figyelembe venni továbbá, hogy az egyes innovációk használhatósága és biztonsága között fordított arányosság áll fenn. A szabályozóknak meg kell teremteniük azt az egyensúlyt, ami még nem akadályozza az új megoldások használhatóságát, de még kellően nagy biztonságot nyújt a pénzügyi intézmények, ügyfeleik és a tagállamok pénzügyi stabilitásának megőrzéséhez. A jogalkotóknak azonban nagy kihívást jelent, hogy a technológia gyors fejlődését a kapcsolódó jogszabályok módosításával, megalkotásával követni tudják, így ebben a helyzetben az etikai normák betartása és betartatása kulcsfontosságú szerephez jut.

4. Bizalom, megbízhatóság, megfelelőség és etika a digitális világban

4.1. Gyors fejlődés

A technológia rendkívül gyors fejlődésen ment keresztül, amely a mindennapjainkra is jelentős hatást gyakorolt, és melynek követése a jogalkotók számára is nagy kihívást jelent. A változás a pénzügyi szektort is rendkívüli módon érintette: a bankok sokszor élenjáróként alkalmazták az új technológiákat, amelyek számukra a költségeik csökkenésével jártak, miközben az ügyfelek elégedettsége is nőtt. A FinTech típusú pénzügyi szolgáltatásokat a felhasználók meghatározó többsége pozitívan fogadja, hiszen a szolgáltatás gyors és jóval olcsóbb is, mint a hagyományos, főleg a személyes jelenlétet igénylő pénzintézeti szolgáltatások; gyanakvásuk, kockázatérzékenységük pedig a szolgáltatással kapcsolatban – főként a fiatalok körében, leginkább a tájékozatlanságuk okán – meglehetősen alacsony. A fő motiváció a kényelem, a gyorsaság és a költségmegtakarítás. A bankok is folyamatosan alkalmazkodnak a modern technikai lehetőségekhez, így ügyfélkiszolgálásuk egyre nagyobb részben tolódik az elektronikus, elsősorban az internet alapú kommunikáció irányába, és igyekeznek felvenni a versenyt a FinTech-vállalkozásokkal hasonló hozzáadott értékű, ügyfélélmény fókuszú szolgáltatások nyújtásával. Ráadásul új motivációként megjelent a koronavírus-járvány, és az emiatt hozott intézkedések kifejezetten felgyorsították a digitalizációt. Rövid idő alatt a pénzügyi szektor átállt a szinte teljes digitális működésre, melynek keretében bővült a netbankon és mobilbankon keresztül elérhető funkciók és szolgáltatások köre. Ezzel együtt nagymértékben nőtt azoknak az ügyfeleknek a száma – beleértve minden korosztályt, de leginkább az idősebbeket –, akik ezeket a szolgáltatásokat azért veszik igénybe, hogy ne kelljen személyesen bemenniük a bankfiókba. A digitalizáció által nyújtott előnyök biztosításához és megtartásához a digitális pénzügyi szolgáltatók működésük során szolgáltatásaik nyújtásához igénybe veszik a digitális technológia minden elérhető elemét, így az interfész-kapcsolódást (API), a mesterséges intelligenciát, az adatelemző módszereket, a robottechnikát, valamint a gyűjtött és hátrahagyott adatok felhasználását. Ezeket az adatokat algoritmusok, programozott alkalmazások gyűjtik és rögzítik, a szolgáltatók pedig szolgáltatásaikat vagy azok egy részét ezekért az adatokért cserébe nyújtják. Az adatokat eladják, vagy egyéb, pénzért árult szolgáltatásuk nyújtásához használják fel, amiből bevételük származik. Mindez rendkívül gyors fejlődéshez vezetett, amelynek során az egyre gyarapodó FinTech-vállalkozások az általuk nyújtott szolgáltatások változatosságával már a pénzügyi szolgáltatások olyan széles körét képviselik, illetve fedik le, melyet a jogalkotóknak a jelenleg hatályos és alkalmazandó jogszabályok módosításaival vagy új jogszabályok megalkotásával meglehetősen nehéz követniük. Ezért kiemelten fontos, hogy legyenek stabil etikai normák, legyen stabil a fejlesztések, innovációk értékalapozottsága az ügyfelek számára, miközben tisztességesen és etikusan kezelik őket.

4.2. Megfelelő szabályozási környezet

A fejlődéshez elengedhetetlen egy olyan nemzetközi és nemzeti szabályozási környezet kialakítása és fenntartása, amely egyszerre ad teret a hasznos és értékes újításoknak, de emellett hatékonyan és szigorúan lép fel a túlzottan kockázatos, az etikátlan vagy káros magatartással szemben (*MNB 2019*). A jogszabályoknak, szabályozásnak és felügyeleti szerveknek alkalmazkodniuk kell az innovációhoz, és meg kell találniuk a helyes egyensúlyt az innováció támogatása és szabályozása között. A pénzügyi technológia kiegyensúlyozott szemléletet követel meg az intézmény szabályozása és a tevékenység szabályozása között. Erre azért van szükség, mert a technológia és a szabályozás közötti összetett kölcsönhatás eredményeként ellentmondások alakulhatnak ki. Előfordulhat ugyanis, hogy egyes vállalatokat és szolgáltatókat eltérően szabályoznak még akkor is, ha alapvetően azonos tevékenységeket folytatnak. Emellett egyes tevékenységeket a jelenlegi szabályozás a fogalommeghatározás és/vagy a tevékenységi körök tekintetében rosszul közelít meg. A jelenlegi uniós szabályozás igen összetett, ahol a pénzügyi technológia innovációira vonatkozóan több, egymást átfedő jogszabály is érvényben van. Hogy az európai FinTech-szereplők ne kerüljenek versenyhátrányba, de a hagyományos hitelintézetek érdekei se sérüljenek, biztosítani kell a közös európai szabályozási környezetet. A szabályozás azonban még nem teljes körű, a kialakítás továbbra is folyamatban van. A következőkben bemutatjuk azokat a fontos területeket, ahol a hatályos szabályozás még alakításra, kiegészítésre szorul.

4.2.1. Az új technológiákra vonatkozó felelősségi szabályok

A jogi felelősség kérdése továbbra is tisztázásra váró terület. Az olyan fejlesztések, mint a mesterséges intelligenciát (MI) is alkalmazó ügyfélkockázat-elemzés, csalásfigyelés, robottanácsadás vagy a big data-elemzés során a technológiában rejlő hibák és torzulások akár rendszerszintű kockázathoz is vezethetnek, és kárt okozhatnak az ügyfeleknek. Nem egyértelmű azonban, hogy az ilyen esetekben ki viseli a jogi felelősséget. A megbízható mesterséges intelligenciának meg kell felelnie a hatályos törvényeknek és rendelkezéseknek. A felelősség megállapítása azért is komoly kérdés, mert a technológia működése nem evidens, nem kizárólag emberek által megírt algoritmusok működésén alapul, összetett, kiszámíthatatlan és átláthatatlan, ezért a rábízott döntéshozatal esetén nem minden esetben azonosítható, hogy pontosan hol, hogyan és miért történhetett egy esetlegesen előforduló tévedés vagy hiba. Ezért a technológiával szemben komoly ellenérzések fogalmazódnak meg. A jogi keretek meghatározása során fontos, hogy az MI kockázatait lehetőség szerint úgy minimalizálja a jogalkotó, hogy figyelemmel legyen az ágazati specifikumokra, így az ágazati törvényekben foglaltakra. A szabályozás preferálja az emberközpontú megközelítést, védje az egyént az automatikus döntéshozatal esetleges aszimmetriáitól, segítse az MI-technológiát fejlesztő és használó vállalkozásokat a jogbiztonság biztosításával, ne okozzon versenyhátrányt, túlzott adminisztratív terhet, ne gátolja a technológia megfelelő fejlődését, ugyanakkor legyen technológiasemleges, és

legyen figyelemmel a nemzetközi előírásokra és szabályozási keretekre is. Az EU felismerte, hogy a közös európai értékek érvényesülése szempontjából fontos, hogy uniós szinten kerüljenek meghatározásra a szabályozási és etikai elvek, és lefektetésre került az Európai Unió mesterséges intelligenciára vonatkozó magas szintű stratégiája[12], illetve az elveket kifejtő Fehér könyv a mesterséges intelligenciáról (*Európai Bizottság 2020*) is. Az MI magyarországi nemzeti szabályozására 2018. október 9-én alakult meg a Magyarországi MI Koalíció, 78 nemzetközi és hazai cég, illetve egyetemek, tudományos műhelyek, szakmai és közigazgatási szervezetek részvételével[13].

Az MI szabályozásán felül a PSD2, az AML-irányelvek, a NIS-irányelv[14], valamint a GDPR hatályba lépésével és alkalmazásával kezdetét vette a szükséges, közös európai szabályozási környezet megteremtése, melynek keretében egyes témákhoz kapcsolódóan, így a felhő alapú szolgáltatások igénybevételére, továbbá a mesterséges intelligencia alkalmazására vonatkozóan európai iránymutatások kerültek és jelenleg is kerülnek kidolgozásra. Ez azért is fontos, mert az ügyfelek és partnerek érzékeny adatainak kezelése és feldolgozása – mind a FinTech, mind az inkumbens szereplők esetén – egyre inkább felhőszolgáltatás keretében igénybe vett, illetve MI-megoldásokra támaszkodó rendszerekben történik. A hitelintézetek és FinTech-vállalkozások tárolják, illetve felhasználják ügyfeleik azonosító adatait, fizetési számlájuk számát, fizetési műveleteihez kapcsolódó és egyéb személyes adatait annak érdekében, hogy az ügyfeleknek személyre szabott szolgáltatásokat nyújtsanak. Az adatok megfelelő védelméhez azonban egyértelműen meg kell határozni az adatgazdai feladatokat és felelősségeket a folyamat teljes egészére. Az adatgazda által meghatározott védelmi elveket a folyamat egészében technológiailag vagy jogi garanciák alkalmazásával ki kell kényszeríteni, függetlenül attól, hogy az adatkezelés vagy -feldolgozás más-más szereplőnél történik-e. Az adatok igénybevételét, hasznosítását vagy az adatokkal kapcsolatos, adatokból származtatott döntések meghozatalát segítő mesterséges intelligencia, a gépi adatelemző módszerek, valamint a robottechnika már jelenleg is a digitális pénzügyi szolgáltatások elválaszthatatlan eszközei, és – ahogy korábban tárgyaltuk – az ezzel kapcsolatos kockázatok és előítéletek miatt vetődik a legtöbb árnyék a FinTech-megoldásokra. Itt nyilvánul meg leginkább a bizalom és az etika követelménye, ugyanis a szabályozók leginkább arra törekednek, hogy magukat a FinTech-szolgáltatásokat szabályozzák, ugyanakkor az ezen szolgáltatások által használt vagy igénybe vett technológiákat és eszközöket már nehezebb azonosítani és működésüket megfelelően szabályozni. Így a PSD2 szerint is a FinTech-vállalkozások által nyújtott egyes pénzügyi szolgáltatások a jogalkotói szándék szerint addig tartanak, ameddig például egy számlainformációs szolgáltatást nyújtó FinTech-vál-

[12] Artificial Intelligence for Europe, COM/2018/237 final
[13] https://digitalisjoletprogram.hu/hu/tartalom/mesterseges-intelligencia-koalicio
[14] https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive

lalkozás az ügyfél által kért adatokat az ügyfél számára eljuttatja, vagy elérhetővé teszi. Természetesen ezt követően az ügyfél a szolgáltatás keretében rendelkezésére bocsátott adatokkal szabadon rendelkezik, így például elfogadva a szolgáltató azon feltételeit, hogy a szolgáltatás ingyenes használata érdekében a FinTech-vállalkozás a gyűjtött adatokat átadhatja egy harmadik félnek (pl. könyvelőnek, marketingcégnek célzott reklámok nyújtásához, vagy egy hitelt nyújtó pénzügyi intézménynek személyre szabott hitelajánlatok, illetve -konstrukciók nyújtásához) az adatok további sorsa, feldolgozási és felhasználási módja a harmadik félnél már kevésbé szabályozott, így kevésbé átlátható és ellenőrizhető. Ez az adatátadás már nem tekinthető például törvényben[15] meghatározott számlainformációs szolgáltatás keretében nyújtott szolgáltatásnak, így a PSD2 szabályai nem alkalmazhatók. Ezért a szolgáltatáson kívüli adatátadás során az adatvédelmi jogszabályokon, így különösen GDPR szabályain túlmenően figyelemmel kell lennie a FinTech-vállalkozásnak – többek között – a pénzügyi ágazati törvények által titok körébe sorolt adatok (így például a Hpt. szerinti banktitok vagy az Fszt.[16] szerinti fizetési titok) átadására vonatkozó törvényi előírásokra. Ezenfelül meg kell vizsgálni a kiszervezésre vonatkozó szabályok, valamint a jelenlegi jogszabályi hézagok miatt az etikai, viselkedési, magatartási, gondossági normák alkalmazását is**.**

4.2.2 Azonos tevékenység, azonos szabályozás

A piaci visszajelzések alapján az egyenlő versenyfeltételek nem biztosítottak még teljeskörűen, hiszen a PSD2 a banki szektor számára jelentős adat- és piacvesztést eredményez, amennyiben nem indítanak maguk is jelentős költséggel járó digitális fejlesztéseket. A harmadik fél szolgáltatók szintén a versenyfeltételek torzulását érzékelik több szempontból is. Bár a csatlakozás nyílt szabványokon alapuló interfészen keresztül történik, mind a harmadik fél szolgáltatóknak, mind az ilyen szolgáltatásokat nyújtó bankoknak minden csatlakozás megteremtéséhez jelentős költséggel járó fejlesztéseket kell elvégezniük. A fejlesztési idő- és költségigény, az eltérő paraméterekkel rendelkező banki interfészekhez, azaz az egységes, egyetlen szabvány helyett több szabvány szerinti[17] és az egyes országokra specifikus elemeket is tartalmazó[18] interfészekhez való csatlakozás szükségessége emeli a belépési küszöböt, lassítja az új harmadik fél szolgáltatók, valamint a banki szektor által nyújtandó PSD2 szerinti új szolgáltatások megjelenését. Mindemellett egyes hitelintézetek a vélt vagy valós piacvesztést elkerülendő igyekeznek megnehezíteni, akadályozni a harmadik fél szolgáltatókat a csatlakozási folyamat során, leginkább etikátlan, de egyes esetekben jogszabályellenes feltételek támasztásával és tesztelési körülményekkel, vagy az esetlegesen bekövetkezett incidensek ürügyén történő eljárásokkal. Ezért az „akadályozás" egységes értelmezését, illetve a vitás helyezetekre vonatkozó

[15] a Hpt. 6. § (1) bekezdés 101a. pontjában
[16] az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény
[17] a két legnagyobb a Berlin Group és Open Banking
[18] pl. Magyarországon az azonnali fizetési szolgáltatás biztosításához szükséges speciális mezők

jogalkalmazást segítendő, az EBA kiadta az SCAr.[19] 32 cikk (3) bekezdésben szereplő akadályozás fogalmának és eseteinek pontosítására irányuló véleményét[20] és az MNB is kiadta a harmadik fél szolgáltatók által nyújtott szolgáltatásokhoz kapcsolódó biztonságos kommunikációról szóló felügyeleti szabályozó eszközét is[21].

A pénzügyi FinTech-vállalkozások, beleértve a harmadik fél szolgáltatók működését is – tekintettel a szolgáltatások kockázatára — minden esetben engedély- vagy regisztrációkötelesek. Az azonos elvek kikényszerítése érdekében a szolgáltatók szigorú engedélyezési procedúrán esnek át, ez azonban nem jelenti azt, hogy a megfelelő garanciákkal működni kívánó szolgáltatók piacra lépését nehezítené vagy gátolná a hatóság. A magyarországi engedélyek kiadásánál az MNB a szigorú feltételek betartása érdekében számos lehetőséget biztosít az engedélyezés megkönnyítésére, ezért részletes útmutatót[22], valamint a vonatkozó gyakori kérdésekre összefoglaló tájékoztatót[23] bocsátott ki, az új pénzügyi megoldások piacra lépését pedig további felügyeleti innovációkkal is segíti.

4.2.3. Erős ügyfél-hitelesítés

A harmadik fél szolgáltatóknak az is jelentős versenyhátrányt jelentett, hogy az EBA által nyújtott lehetőség szerint az egyes tagállamok nemzeti felügyeleti hatóságai a bankok és más pénzforgalmi szolgáltatók számára 2020. december 31. napjáig meghosszabbították az erős ügyfél-hitelesítésről szóló jogszabályi rendelkezéseknek a fizetési kártyával végzett internetes fizetési műveletek esetében történő megfelelés határidejét, azonban ezzel párhuzamosan a harmadik fél szolgáltatók számára nem biztosítottak lehetőséget az erős ügyfél-hitelesítés alkalmazásának mellőzésére a szolgáltatásaik nyújtása során. A PSD2 2019. szeptember 14-ét határozta meg, amikortól a bankoknak és más pénzforgalmi szolgáltatóknak – ahhoz, hogy az ügyfelek online hozzáférjenek a fizetési számláikhoz vagy elektronikus fizetési műveletet kezdeményezzenek – alkalmazni kell az erős, legalább két hitelesítési faktort (például PIN-kód és ujjlenyomat, vagy jelszó és SMS-kód stb.) alkalmazó ügyfél-hitelesítés előírásait. Figyelembe véve azonban a szabályozás komplexitását, valamint a kártyakibocsátók és kártyaelfogadók kérését, lobbitevékenységét, a nemzeti felügyeleti hatóságok munkáját koordináló EBA lehetővé tette a tagállamok felügyeleti hatóságainak, hogy további, 2020. december 31-ig tartó időt biztosítsanak az informatikai

[19] Az (EU) 2015/2366 európai parlamenti és tanácsi irányelvnek az erős ügyfél-hitelesítésre, valamint a közös és biztonságos nyílt kommunikációs standardokra vonatkozó szabályozástechnikai standardok tekintetében történő kiegészítéséről szóló 2017. november 27-i (EU) 2018/389 felhatalmazáson alapuló bizottsági rendelet

[20] https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2020/884569/EBA%20Opinion%20on%20obstacles%20under%20Art.%2032%283%29%20RTS%20on%20SCA%26CSC.pdf

[21] https://www.mnb.hu/letoltes/vezetoi-korlevel-a-fizetes-kezdemenyezesi-es-szamlainformacios-szolgaltatasokhoz-kapcsolodo-biztonsagos-kommunikacioval-2020-07-13.pdf

[22] https://www.mnb.hu/felugyelet/engedelyezes-es-intezmenyfelugyeles/engedelyezes/szektorok/penzpiac/penzforgalmi-intezmeny/kizarolag-szamlainformacios-szolgaltatast-vegzo-penzforgalmi-intezmeny-bejelentese, https://www.mnb.hu/letoltes/penzforgalmi-intezmenyek-tevekenysegenek-engedelyezese.pdf

[23] https://www.mnb.hu/penzforgalom/psd2-gyakori-kerdesek-es-valaszok/engedelyezes

fejlesztések befejezésére, valamint az új hitelesítési eljárásokra történő átállásra az interneten, fizetési kártyával történő fizetések esetében. Ebben az úgynevezett átállási időszakban a bankok, valamint más pénzforgalmi szolgáltatók ügyfelei erős ügyfél-hitelesítés alkalmazása nélkül is használhatták a fizetési kártyájukat az online kezdeményezett belföldi és külföldi fizetéseknél.

4.2.4 Csalásmegelőzés

A digitális technológiákkal, a nyílt bankolással, valamint az azonnali fizetések által nyújtott lehetőségekkel lényegében olyan paradigmaváltás következett be, amelylyel a kapcsolódó kockázatok, így például a visszaélési kockázatok is átalakulnak. A többféle szereplő bonyolultabbá teszi a rendszert, a fizetési művelet teljesítése immár 5-6 szereplő együttes közreműködésével valósul meg, melyek mindegyike támadható, így új potenciális támadási, sebezhetőségi pontokként jelennek meg. Ez a visszaélési kockázatok átalakulásához, valamint egyéb, még rejtett fenyegetések kialakulásához vezethet. E kockázatok növekedése árnyékot vethet a FinTech-re, ezért ehhez a változáshoz a szabályozási környezetnek is elengedhetetlenül alkalmazkodnia kell. A PSD2 és a kapcsolódó SCAr bár előírja egy modern felügyeleti rendszer üzemeltetését az engedély nélküli, illetve csalárd fizetési műveletek észlelésére, ennek valós időben történő működtetése csak bizonyos feltételek[24] teljesülése esetén kötelező. Ezzel azonban az azonnali fizetések sajátosságaiból eredő, ún. azonnali csalás kockázatának[25] kezelése csak részben valósul meg. Egy modern felügyeleti rendszernek képesnek kell lennie arra, hogy minden felhasználó (beleértve a harmadik fél szolgáltatókat) tevékenység- és eszközkockázatát valós időben elemezze (figyelembe véve az azonnali fizetések néhány másodperces átfutási idejét) az összes digitális csatornán, és reagáljon a gyanús eseményekre, az ismert csalási forgatókönyvekre. A valós idejű felügyeleti rendszer működtetése azonban jelenleg, figyelembe véve az SCAr-ben előírt feltételeket, nem általános érvényű törvényi előírás.

Egy modern felügyeleti rendszernek képesnek kell lennie arra, hogy krízishelyzetben is helytálljon. A koronavírus új típusú sokként érte a világgazdaságot, és a pénzügyi szektornak igen rövid idő állt rendelkezésére arra, hogy reagáljon. Ahogy a lakosság karanténba kényszerült, szükség volt a szinte teljes digitális működésre való átállásra, aminek keretében bővült a netbankon és mobilbankon keresztül elérhető funkciók és szolgáltatások köre. Ahogy korábban tárgyaltuk, bővült azon ügyfélkör is, akik ezeket a szolgáltatásokat igénybe veszik, hogy elkerüljék a személyes megjelenést a bankfiókban. Jelentős kockázatot hordoz azonban, hogy ezen új ügyfelek közül

[24] Műveletkockázat elemzés alapján a távoli fizetési művelet alacsony kockázatúnak tekinthető, és nem kerül alkalmazásra erős ügyfél-hitelesítés.
[25] A kockázatot az jelenti, hogy 5 másodperc alatt már a csalónál van a pénz, így minimális annak az esélye, hogy az eltulajdonított pénz visszaszerzésre kerüljön.

sokan, de különösen az idősebb korúak – akik a leginkább veszélyeztetettek a koronavírus által – soha nem használtak digitális banki szolgáltatásokat a múltban, így a tudás és a tapasztalat hiányát a bűnözők könnyedén kihasználhatják és ki is használják. A digitális technológiák fejlődésével a csalások is egyre inkább kifinomultak, és a koronavírus időszakában a csalási kísérletek és a sikeres csalások gyakorisága is globális szinten nőtt (*Javelin Strategy & Research and SAS 2020*). Az ügyfélkör bővülésével az internetes átutalások és internetes kártyás fizetési műveletek (pl. online bankkártyás fizetés) megnövekedett száma – figyelembe véve a korábban offline generáció digitális banki szolgáltatások terén szerzett ismereteinek alacsonyabb szintjét – jelentős plusz terhet ró az érintett pénzügyi intézmények megfelelőségi területeire a csalások, visszaélések megelőzésében. Különösen problémás, hogy a csalásfelderítés, illetve -megelőzés egy olyan speciális szakterület, amelyre kevés kompetencia áll még rendelkezésre. A csalásfigyelő rendszerekben is egyre szélesebb körben alkalmazzák a mesterséges intelligencián alapuló megoldásokat, amelyek, bár hatékonynak bizonyulnak, számos szabályozási kérdést vetnek fel, így például adatvédelmi szempontból a tiltott készletező adatkezelést, a szigorú követelményekhez kötött profilalkotási lehetőséget, a célhoz kötött adatkezelés megfelelőségét, az adattárolásra vagy az ágazati titok körébe tartozó adatok kezelésére vonatkozó előírásokat. Figyelembe kell venni továbbá, hogy a fent tárgyalt, a mesterséges intelligenciával támogatott döntések megfelelőségi és etikai kérdésein felül az adatok tárolása és feldolgozása jellemzően felhőszolgáltatás igénybevételével történik, ami további adatvédelmi, titokvédelmi és etikai aggályokat vethet fel.

4.2.5. Kiszervezések, felhőszolgáltatások igénybevétele

A pénzügyi intézmények és harmadik fél szolgáltatók körében mind népszerűbb felhőszolgáltatások a költséghatékonyság és az egyszerű felhasználás mellett számos kockázatot rejtenek, így például – a teljesség igénye nélkül – jellemzően a szolgáltatási modell velejárója, hogy a szolgáltató ugyanazt vagy hasonló szolgáltatást más intézmények számára is nyújt, így az adatok, rendszerek megfelelő és biztonságos szeparálásáról gondoskodni kell. Fontos, hogy ne csak más igénybe vevők, de maga a szolgáltató vagy alvállalkozói se, vagy csak a megfelelő – szerződésben vállalt – kontrollintézkedésekkel férhessen hozzá az adatokhoz, és azokon csak a szerződésben meghatározott műveleteket hajtsa végre. Kiemelendő kockázat még a kilépési politika (exit-stratégia), ugyanis – különösen a szoftver szintű szolgáltatáskor (SaaS) – az intézmény elveszítheti a kontrollt a saját adatai kezelése, illetve a feldolgozott adatai megfelelő birtoklása, valamint azok további feldolgozási lehetősége felett.

Legyen szó akár egyes megoldások, akár az infrastruktúra külső szolgáltatóhoz való kihelyezéséről, mindenkor figyelemmel kell lenni a vonatkozó EU-s, nemzeti, ágazati jogi és felügyeleti szabályozó normák betartására. A kihelyezések (klaszszikus outsourcing) fogalmát a magyar jogrend az EU-s jogtól eltérően definiálja: a magyar törvényekben a kiszervezés fogalmát megkülönböztetik az általános

szolgáltatáskihelyezési megoldásoktól. Sajnos az ágazati törvények nem kezelik egyformán a kiszervezések fogalmát, míg a Hpt., a Bszt.[26] az Öpt.[27] és az Mpt.[28] a kiszervezést adatkezeléshez köti, és szigorú szerződéses követelményeket vár el az intézménytől, addig például az Fsztv.[29] vagy a Bit.[30] szerint kiszervezésnek az a tevékenység tekinthető, amelyet az intézmény maga végezne, de azt szerződés alapján külső szolgáltatóval látja el. A Kbftv.[31] pedig a számítástechnikai rendszerfejlesztés, számítástechnikai üzemeltetés és karbantartás szolgáltatásokat kifejezetten kiemeli a kiszervezések köréből. A kiszervezésekre vonatkozó jogszabályi elvárások alkalmazásához az MNB felügyeleti szabályozó eszközökben ad iránymutatást.[32] A korábban említett felhőszolgáltatások igénybevétele – amennyiben a vonatkozó ágazati törvények rendelkezéseinek megfelel – szintén kiszervezésként kezelendő, a szolgáltatás igénybevételekor azonban különös tekintettel kell lenni a technológia sajátosságaira. Az alkalmazandó normákra az MNB speciális felügyeleti szabályozó eszközben nyújt iránymutatást[33].

Függetlenül azonban attól, hogy a harmadik fél szolgáltatók igénybevétele kiszervezésként vagy kihelyezésként történik, elvárt, hogy az intézmények a megfelelő gondossággal járjanak el, és az etikai, erkölcsi és prudenciális normákat – különösen, ha az ügyfelek adatait vagy a velük való kapcsolattartást érinti – akkor is tartsák be, ha azok nem jogszabályi előíráson alapulnak.

4.3. Bizalomépítés, tisztességes, etikus magatartás

4.3.1. A bizalom, megbízhatóság kiépítésének módjai átalakultak

A bizalom, megbízhatóság, etikus magatartás az üzleti jó hírnévvel együtt olyan elvárások, szakmai követelmények, amelyeknek a megfelelés érték, és egyben a sikeres működés és profitabilitás alapját képezik. A FinTech-vállalkozások esetében a bizalom építésének szükségessége a kezdeti időszakban még érdemben nem merült fel, a szabályozás is laza, megengedő volt. A bizalom, megbízhatóság kiépítésének

[26] A befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény
[27] Az Önkéntes Kölcsönös Biztosító Pénztárakról szóló 1993. évi XCVI. törvény
[28] A magánnyugdíjról és a magánnyugdíjpénztárakról szóló 1997. évi LXXXII. törvény
[29] Az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény
[30] A biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény
[31] A kollektív befektetési formákról és kezelőikről, valamint egyes pénzügyi tárgyú törvények módosításáról szóló 2014. évi XVI. törvény
[32] A külső szolgáltatók igénybevételéről szóló 7/2020. (VI.3.) MNB ajánlás közvetlenül a kiszervezésekre vonatkozik, a belső védelmi vonalak kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és kontroll funkcióiról szóló 27/2018 (XII.10.) MNB ajánlás az ellenőrzési feladatokra, míg az Informatikai rendszer védelméről szóló 8/2020 (VI.22.) MNB ajánlás az informatikai vonatkozású kiszervezések kezelését és ellenőrzését külön-külön fejezetekben tárgyalja.
[33] A felhőszolgáltatások speciális kockázatainak kezelésére az Európai Bankhatóság 2017. december 20-i, a felhőszolgáltatóknak történő kiszervezésről szóló ajánlásait (EBA/REC/2017/03 https://eba.europa.eu/sites/default/documents/files/documents/10180/2170125/9fa68167-91e8-412f-87b3-36ad28811cc4/Recommendations%20on%20Cloud%20Outsourcing%20%28EBA-Rec-2017-03%29_HU.pdf?retry=1) is magában foglaló, a közösségi és publikus felhőszolgáltatások igénybevételéről szóló 4/2019. (IV.1.) MNB ajánlásban foglaltakat várja el. (Az EBA a felhőre vonatkozó ajánlást ugyan hatályon kívül helyezte, de az abban megfogalmazott elvárásokat integrálta a kiszervezésről szóló EBA/GL/2019/2 ajánlásba.)

módjai is átalakultak az internetes és digitális technológiák miatt. A bizalom, megbízhatóság egyre inkább az ügyfelek egymás közötti kommunikációjától, ajánlásaitól, személyes kapcsolati hálózatától függ. Azonban az egyre gyakoribb panaszok az adathalászatra, valamint a személyes adatok, elsősorban a szolgáltatás nyújtása során kezelt, valamint az úgynevezett hátrahagyott adatok olyan gyűjtésére, kezelésére és felhasználására vonatkozóan, amelyről a szolgáltatás felhasználója, aki egyben az adat tulajdonosa, nem is tud, rávilágítanak a FinTech-szolgáltatások árnyoldalaira, a szolgáltatás igénybevételéhez kapcsolódó kockázatokra. A FinTech-vállalkozások izgalmas új termékeket, hozzáadott értékű szolgáltatásokat hoznak létre válaszul az ügyfelek igényeire, felhasználva az olyan technológiákat, mint a mesterséges intelligencia, robotika és gépi tanulás. A hagyományos hitelintézetek is innovatív fejlesztéseket kezdeményeztek, különböző típusú partnerséget alakítottak ki az ezen a területen megjelenő szolgáltatókkal, vagy egyszerűen csak felvásárolták a kialakított új megoldásokat magával a FinTech-startupokkal együtt, és integrálták azokat a saját működésükbe. A digitális technológiák és immáron a nyílt bankolás, ötvözve az azonnali fizetések által nyújtott lehetőségekkel, megváltoztatták a hagyományos hitelintézetek kockázati profilját is. Fontos tehát, hogy nem elégséges a jogszabályok általi szabályozás, a tisztességes, etikus magatartás követelményére is szükség van. A megváltozott kockázati profil kezeléséhez a hatékony szabályozási környezet mellett hatékony megfelelőségi és belső ellenőrzési programra van szükség. A megfelelő, folyamatosan karbantartott megfelelőségi és belső ellenőrzési program megoldást nyújthat az új, esetleg még rejtett fenyegetések feltárására, valamint az azonosított kockázatok megfelelő kezelésére. A bizalmas és megbízható légkör alappillére a prudens, etikus működés biztosítása, ehhez azonban nélkülözhetetlen a vezetőség elköteleződése, valamint az, hogy a munkavállalók ismerjék és betartsák a vonatkozó jogszabályokat, szabályzatokat, etikai normákat. Ez elsősorban a tudatosság növelésével, folyamatos tájékoztatással, oktatással és rendszeres – tervezett – ellenőrzésekkel érhető el. Előremutató gyakorlat, ha a megfelelőségbiztosítási terület konzultatív, tanácsadási, megelőzési feladatkörében folyamatosan képes biztosítani a munkavállalók számára vonatkozó kérdéseik kielégítő megválaszolását akár személyesen, akár telefonon, elektronikus csatornákon, vagy bizonyos esetekben anonim módon, például whistleblower-ként. Figyelembe kell venni azonban azt is, hogy a FinTech-vállalkozások szolgáltatásaik nyújtásához igénybe veszik a digitális technológia minden elérhető elemét, ezért az etikus magatartási normákat nemcsak közvetlenül a FinTech-re és a digitális pénzügyi szolgáltatókra vonatkozóan kell meghatározni és betartatni, hanem kiterjesztésük elkerülhetetlen a tevékenységükhöz nélkülözhetetlen eszközökre, technológiákra, megoldásokra is, ezzel „szabályozva" a FinTech és BigTech pénzügyi szolgáltatások eszköztárát, azaz például a mesterséges intelligenciát, a big data keretében kezelt és a hátrahagyott adatok felhasználását.

4.3.2 Az etikai, gondossági keretek fejlesztése

A megfelelőségbiztosítási területnek a megfelelőségi program kialakítása és végrehajtása során a jogszabályi megfelelőség biztosítása mellett kiemelt figyelemmel kell lennie a gondossági kötelezettségre is. Ez arra kötelezi a megfelelőségbiztosítási területet, hogy ne csak azt vizsgálja, hogy a vállalkozás a tevékenysége során megfelel-e a hatályos jogszabályoknak, hanem azt is, hogy mindaz, amit tesz, helyes-e, és a bizalom, a megbízhatóság, az etika követelményei sem sérülnek. Ennek keretében fontos megfelelőségi feladat egyrészt az etikai kultúra ösztönzése, folyamatosan tájékoztatva a menedzsmentet, valamint a munkavállalókat arról, hogy mi helyes és mi elfogadhatatlan, másrészt a megfelelés-tudatosság alapjainak megteremtése és megismertetése a munkavállalókkal. A közvetítő rendszerre és a pénzpiacokra kiterjedő kockázatokat felismerve a szükséges jogszabályok kidolgozása és bevezetése mellett elindult egy folyamat az etikai, gondossági keretek fejlesztésére, kiterjesztve a normákat a FinTech-vállalkozásokra, valamint az általuk igénybe vett eszközökre is. Az Európai Bizottság 2019 áprilisában tette közzé az „Etikai iránymutatás a megbízható mesterséges intelligenciára vonatkozóan" című dokumentumot (*Európai Bizottság 2019*), melynek célja a megbízható mesterséges intelligencia használatának és fejlesztésének előmozdítása.

A megbízható mesterséges intelligencia három olyan elemből áll, amelyeknek a rendszer egész életciklusa alatt teljesülniük kell: jogszerűnek kell lennie, vagyis meg kell felelnie a hatályos törvényeknek és rendelkezéseknek, etikusnak kell lennie, vagyis meg kell felelnie az etikai elveknek és értékeknek, valamint műszaki és társadalmi szempontból is stabilnak kell lennie, mivel a mesterségesintelligencia-rendszerek még jó szándék esetén, akaratlanul is okozhatnak kárt.

A jogszabályok nem mindig tudják tartani a lépést a technológiai fejleményekkel, időnként előfordulhat, hogy nem felelnek meg az etikai normáknak, vagy bizonyos kérdések kezelésére egyszerűen nem alkalmasak. Ahhoz azonban, hogy a mesterségesintelligencia-rendszerek megbízhatók legyenek, etikusaknak is kell lenniük az etikai normákkal való összhang biztosítása révén.

4.3.3. Az ügyfelekkel szemben tanúsított prudens, etikus magatartás

Napjainkban egyre hangsúlyosabb szerepet kap az ügyfelekkel szemben tanúsított etikus eljárások alkalmazása. A fogyasztóvédelmi hatóságok szerepe mind nagyobb, ennek hatására a pénzügyi közvetítőrendszerbe és annak felügyeletébe vetett bizalom fokozatosan növekedik. Az ügyfelek érdeksérelmükkel – ha arra a pénzügyi szolgáltatótól nem kaptak kielégítő választ – felkereshetik a felügyeleti hatóságot, és ott egyedi ügyekben fogyasztóvédelmi panaszt, jogszabálysértés vagy más fogyasz-

tókat is érintő, rendszerszintű probléma esetén közérdekű bejelentést tehetnek[34]. A fogyasztók és a pénzügyi szervezetek közötti vitarendezés a bírósági úton kívül a Pénzügyi Békéltető Testület[35] fórumán is lehetséges.

A prudens működés feltétele, hogy az ügyfél megfelelő, teljes körű tájékoztatásának már a szerződéskötést megelőzően is, időben, igazolhatóan meg kell történnie. Az ügyfél tájékoztatására különféle jogszabályi előírások vonatkoznak az adatkezeléstől a szolgáltatás igénybevételével kapcsolatos megfelelő döntés kialakításához szükséges feltételek biztosításáig, azonban a jogszabályok itt sem rendeznek minden kérdést, ezért a gondos, etikus és prudens magatartásnak az ügyfelek megfelelő tájékoztatásában kiemelt szerepe van.

Az adatkezeléssel kapcsolatos rendelkezések a GDPR szabályain felül a vonatkozó ágazati törvényekben is megfogalmazásra kerültek. A kiszervezett tevékenységek igénybevételekor a hitelintézetek esetében például az ügyfeleket az üzletszabályzatban is tájékoztatni kell arról, hogy az adatfeldolgozás során kik férhetnek hozzá az érzékeny adatokhoz[36]. Ugyan nem jogszabályi előírás, de a tisztességes gyakorlathoz hozzátartozik, ha az intézmény az igénybe vett alvállalkozókat és a teljes kiszervezési láncot transzparenssé teszi az ügyfelei számára.

A fogyasztóvédelmi előírások a vonatkozó törvényben[37] fogyasztónak minősülő ügyfelek számára nyújtanak védelmet. Fontos etikai kérdés, hogy azok az ügyfelek is, amelyek nem tekinthetők fogyasztónak, kapjanak hasonló védelmet az alkalmazott eljárások vonatkozásában.

Az MNB a vonatkozó jogszabályi előírások alkalmazásának elősegítésére, valamint a prudens elvárásokra felügyeleti szabályozó eszközt[38] bocsátott ki. Mivel sem a jogszabályi, sem a szabályozói normák nem lehetnek teljes körűek, a tisztességes és méltányolható eljárásról az intézményeknek az előírásokon felül gondoskodni kell. Elvárás továbbá, hogy az intézmények vessék alá magukat a vonatkozó etikai, magatartási kódex(ek)nek és a Pénzügyi Békéltető Testület döntéseinek.

A tisztességes eljárás része az is, hogy minden fogyatékkal élő számára a megfelelő technikai megoldásokkal, lehetőség szerint azonos minőségben és azonos ügyfélélmény nyújtásával biztosítsuk a szolgáltatások igénybevételének lehetőségét.

[34] A panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvény, illetve a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény rendelkezései szerint
[35] https://www.mnb.hu/bekeltetes
[36] A Hpt. 68. § (12) bekezdésben foglaltak szerint
[37] A fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról szóló 2008. évi XLVII. tv.
[38] A pénzügyi szervezetek számára a fogyasztóvédelmi elvek alkalmazásáról szóló 10/2016. (X.24.) MNB-ajánlás

5. Konklúzió

A digitális pénzügyi infrastruktúra akadálymentes építéséhez és fejlődéséhez szükséges követelményeknek eddig még csak részben sikerült eleget tenni, így áthidaló megoldásként előtérbe kerültek az etikai, bizalmi elvárások, üzletviteli magatartási kódexek. Fontos szerep hárul a pénzügyi szektorban tevékenykedő vállalkozások megfelelőségbiztosítási területeire, hiszen a hiányos szabályrendszer keretei között ez az a terület, amelynek feladata a jogszabályoknak, illetve egyéb, követendő ajánlásoknak, etikai normáknak, iránymutatásoknak, útmutatásoknak való megfelelés biztosítása és a működésében rejlő megfelelőségi kockázatok azonosítása és kezelése. Nem elegendő csak azt vizsgálni, hogy a szolgáltatások nyújtása a hatályos jogszabályoknak megfelelően történik, azt is vizsgálni kell, hogy a bizalom, a megbízhatóság, az etika követelményei nem sérültek. Nehezíti a feladatot, hogy a megfelelőségbiztosítási területnek egy folyamatosan változó, fejlődő szabályozási környezetben kell tudni helytállnia, ráadásul olyan időszakban, amikor a koronavírus-járvány gazdasági-pénzügyi életre ható következményei is elérték a digitális világot. De minden krízis, így a koronavírus-járvány által okozott is, amellett, hogy jelentős kockázatokat hordoz, egyben lehetőség is. Az óvintézkedésként bevezetett izolációs lépések online térbe mozgattak sok tevékenységet, aminek hatására a fogyasztói viselkedés is drasztikusan megváltozott, előmozdítva a digitalizálódási folyamatokat. A hazai digitalizációt is jelentős mértékben ösztönözték a koronavírus-helyzetre, illetve az okozott nehézségekre adott gyors és hatékony válaszok, amelyek hosszabb távon egyben az ország versenyképességét is erősítik. Számos új, digitális szolgáltatás került bevezetésre, és a járvány miatt hozott intézkedések kifejezetten felgyorsították a digitális projektek megjelenését. Így a személyes megjelenést biztosító ügyfélszolgálatok és a fiókokban történő ügyfélkiszolgálás korlátozása hozzájárult a digitális szerződéskötési, továbbá a távoli ügyfélazonosítási megoldások és az elektronikus fizetési lehetőségek gyorsabb fejlődéséhez. A pénzügyi szektor rövid idő alatt átállt a szinte teljesen digitális működésre, melynek keretében bővült az elektronikus ügyfélcsatornákon (webes és mobilfelületeken) keresztül elérhető funkciók és szolgáltatások köre, és egyben bővült azon ügyfélkör is, ahol ezeket a szolgáltatásokat igénybe veszik. Ennek oka – a kényelmen túl – a pandémiás kockázatok csökkentése a személyes érintkezések számának redukálásával. Jelentős kockázatot hordoz azonban, hogy az új ügyfelek közül sokan, de különösen a koronavírus által leginkább veszélyeztetett időskorúak – nem használtak korábban digitális banki szolgáltatásokat, ezért a megfelelő tudásuk és a tapasztalatuk hiányát a bűnözők könnyedén kihasználhatják. A FinTech-szolgáltatásokat előnyben részesítő, fiatalabb generáció, bár fejlett digitális, internethasználati készségekkel rendelkezik, a gyors, olcsó és kényelmes fizetési megoldásokban hisz, azonban se pénzügyi, se biztonságtudatosságuk nincs összhangban ezzel a képességükkel, így a kockázat az ő esetükben is fennáll. A korábban offline generáció digitális banki szolgáltatások terén szerzett ismereteik alacsonyabb szintjének kockázata mellett az internetes

átutalások, internetes kártyás fizetési műveletek (például online bankkártyás fizetés) és a készpénzfelvételi tranzakciók jelentősen megnövekedett száma is jelentős plusz terhet ró az érintett pénzügyi intézmények megfelelőségi területeire a csalások, visszaélések megelőzésében, ami a banknak és az ügyfélnek is egyaránt érdeke.

A digitalizáció, robotizáció és mesterséges intelligencia fejlődésének, továbbá a válságok, krízisek, így jelen helyzetben a koronavírus-járványból adódó globális gazdasági-pénzügyi problémák következtében mindig újabb és újabb kockázatokra kell a szabályozóknak választ adni. Ahogyan korábban említettük, a szabályozás – szükségszerűen – mindig elmaradásban lesz az új igényekhez és a megjelenő új technológiákhoz képest, mivel ezek működését és kockázatait teljeskörűen meg kell ismerni ahhoz, hogy megfelelő szabályozást lehessen rájuk vonatkozóan kialakítani. A szabályok pedig egyébként is – mint azt a közismert mondás is tartja – annyit érnek, amennyit be tudunk tartatni belőlük. Ezért tehát nagyon fontos az etika szerepe a globális világ működésében, mert a mindenki számára kielégítő együttélési szabályok az etikai elvek és célok mentén kell, hogy elültetésre kerüljenek a társadalom gondolkodásában. Olyan etikát kell megfogalmazni, kidolgozni és alkalmazni a globális világra, amely túlmutat a mai értelemben vett egyéni érdekeken, a gazdasági profit maximalizálásán. Az egész emberiségre kiterjedő megfelelő életminőség, biztonság, fenntarthatóság biztosítása kell legyen a cél, és ennek eléréséhez a megfelelőségbiztosítási területnek is készen kell állnia a kapcsolódó feladatok elvégzésére.

Felhasznált irodalom

Európai Bizottság (2019): *Etikai iránymutatás a megbízható mesterséges intelligenciára vonatkozóan*. https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-hu

Európai Bizottság (2020): *Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom Európai megközelítése.* https://op.europa.eu/hu/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1. Letöltés ideje: 2021. február 8.

Javelin Strategy & Research and SAS (2020): *The Escalation of Digital Fraud: Global Impact of the Coronavirus.* https://www.javelinstrategy.com/sites/default/files/files/reports/20-5010J-FM-The%20Escalation%20of%20Digital%20Fraud-SAS_0.pdf

MNB (2019): FinTech stratégia. Magyar Nemzeti Bank. https://www.mnb.hu/letoltes/mnb-fintech-strategia-final.pdf

Müller János – Kerényi Ádám (2019): *A bizalom és etika igénye a digitális korszakban – Napfény és árnyék a FinTech világában*. Hitelintézeti Szemle, 18(4): 5–34. http://doi.org/10.25201/HSZ.18.4.534