GAZDASÁG ÉS PÉNZÜGY • 12. ÉVF. 3. SZ. • 2025. SZEPT. • DOI: 10.33926/GP.2025.3.2

ERŐSÍTÉS A PÉNZÜGYI SZEKTORT ÉRINTŐ ONLINE BŰNCSELEKMÉNYEK ELLENI HARCBAN

Új jogintézmények bemutatása a köz- és magánszféra együttműködésében

Jancsó Gábor[1]

ABSZTRAKT

A koronavírus járványt követően átalakult digitális pénzügyi szokásokat kihasználva, a pénzügyi szektort érintő online csalások száma exponenciális növekedésnek indult. Ez olyan minőségileg új bűnügyi jelenség megjelenését eredményezte, amely a korábban jellemzően alkalmazott – mennyiségi jellegű – bűnüldözési megoldásokkal eredményesen nem kezelhető. A pénzügyi szektor sajátos jellemzői és képességei ugyanakkor lehetővé teszik a köz- és magánszféra új együttműködési lehetőségeinek (private-public-partnership, PPP rendszer) kihasználását, amelyek érdemben lehetnek képesek a jelenség visszaszorítására. A cikk az online csalásokkal kapcsolatban kialakult együttműködési fórumokat (KiberPajzs és az Igazságügyi Minisztérium által koordinált munkacsoport), valamint a PPP rendszer működőképességét, hozzáadott értékét kívánja bemutatni. Ismertetjük továbbá az elért eredményeket, az elmúlt másfél évben bevezetett intézkedéseket, a jogintézményeket: a nyomozó hatóságok és a bankok közötti együttműködési megállapodásokat, a Központi Visszaélésszűrő Rendszert, az objektív bejelentést és az információmegosztást.

JEL-kódok: G21, K14, K24, K42, O38

Kulcsszavak: online csalás, köz- és magánszféra együttműködése, PPP rendszer, pénzügyi szolgáltató, bűnmegelőzés, bűnüldözés, együttműködési megállapodás, KVR, objektív bejelentés, információmegosztás

1 *Jancsó Gábor* levelező szerző, az Igazságügyi Minisztérium büntetőjogi jogalkotásért felelős volt helyettes államtitkára. E-mail: gabor.jancso@im.gov.hu.

1. BEVEZETÉS – A BÜNTETŐ IGAZSÁGSZOLGÁLTATÁS ALAPVETÉSEI

A szerző gyakorló büntetőjogász, aki számára az állami erőszak-monopólium, az állam büntetőjogi igénye, a bűncselekmények állam általi üldözésének kötelezettsége, valamint az ezekhez szükséges eszközrendszer rendelkezésre állása nem egy vitatható, megvitatandó kérdés, sokkal inkább a büntető igazságszolgáltatás alapjait és kereteit meghatározó axióma. A jogállamiság, a békés társadalmi együttélés alapjait jelenti, hogy a büntető igazságszolgáltatás terén az állam igénye lényegében kizárólagos, az egyéni igényérvényesítés kevésbé tűrt jelenség. A jogos önvédelem, a végszükség mellett a jogos vagy jogosnak vélt igények meg nem engedett módon történő érvényesítése akár bűncselekményt is megvalósíthat.

Bibó így ír Etika és büntetőjog című értekezésében: „A büntetőjog történeti kialakulása a legmesszebbmenően alátámasztja a büntetés funkciójának ilyen értelmezését. A magánbosszúnak a közösség számára való kisajátítása volt az az út, amelyen keresztül a büntetőjog kialakult. Nem a sértettek keresték először a köz védelmét a bűntettesekkel szemben, hanem a vádlottak a bosszuló rokonnal, a lincselő tömeggel szemben. Minden büntetőjogi dogmatika élén ott áll az a jogtörténeti megállapítás, amely szerint a büntetőjog olyan módon jött létre, hogy a megtorlás jogát a köz fokozatosan kivette az egyes ember kezéből." (Bibó, 1986, 174).

A büntetőjog számára tehát az állami feladat- és garanciarendszer egy nem vitatható alapvetés, amelyre figyelemmel a büntetőjog szabályozási logikája, hogy az állam számára, illetve az állam által kell biztosítani azokat az eszközöket, erőforrásokat, amelyek az ezzel kapcsolatos feladat ellátásához szükségesek. A büntetőeljárási törvényünk[2] ugyan – törvényi keretek között – tűri például a magánnyomozást (sajátos módon a védő jogaként nevesítve)[3], azonban azt érdemben már nem támogatja, többlet erőforrás biztosításáról vagy a hatósági erőforrások, információk megosztásáról nem beszélhetünk. Még a vádkorrigendumok, azaz a vádemeléssel kapcsolatos esetleges hiányosságok javítását szolgáló intézményrendszer keretei között (a sértett pótmagánvádlóként történő fellépése, vagy a közelmúltban bevezetett közhatalom gyakorlásával vagy közvagyon kezelésével kapcsolatos kiemelt bűncselekmények esetén külön eljárásban lényegében bárki által benyújtható /pót/vádindítvány)[4] esetében sem biztosított, hogy az állam mellett vádemelésre jogosultságot kapott személy a nyomozó hatóság erőforrásait igénybe vehesse. Az állami vádmonopólium tehát tűri, hogy a sértett, vagy az

2 A büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: Be.)

3 Be. 42. § (2) c) pont.

4 Be. CV. és CV/A. Fejezet

arra jogosult más személy, az eltérő jogi álláspontja vagy a rendelkezésére álló egyéb információk alapján (pót)vádat emeljen, de a nyomozás eszközrendszerének használata, hasznosítása, az állami kényszer alkalmazhatósága már nem biztosított. A vádemeléssel a bírósági eljárás, az adott kérdés bíróság által történő megítélése tehát „kikényszeríthető", de a nyomozás kikényszerítése, a nyomozó hatóság erőinek, eszközeinek, erőforrásainak magáncélok érdekében történő felhasználása nem tűrt. A magánvádas eljárásban is kizárólag a feljelentett személy személyazonosságának megállapítására, és kizárólag a bíróság irányítása mellett képzelhető el a nyomozó hatóság erőforrásainak rendkívül szűk célból történő felhasználása.

Látható tehát, hogy a büntető igazságszolgáltatás tradicionálisan nem tekinti partnernek a sértetteket vagy más „civil" aktorokat.

Az utóbbi években ugyanakkor olyan társadalmi tendenciák figyelhetők meg, amelyek alapvetően változtatják meg ezt a működési mechanizmust. Az informatikai fejlődés, illetve a pénzügyi szektor kihívásai a bűnüldözés területén új szabályozási és munkamódszerek kialakulásához vezettek, a bűntető igazságszolgáltatás kezd partnerként tekinteni a magánszektorra, és igényként fogalmazódik meg a rendelkezésre álló erőforrások megosztása.

2. EGYÜTTMŰKÖDÉSI FORMÁK A BŰNÜLDÖZÉSSEL KAPCSOLATBAN

A bűnüldöző szervek, illetve a szélesebb körben vett bűnügyi tudományok együttműködése más szervekkel, szakterületekkel nem példa nélküli. A bűnügyi adatok, tapasztalatok hasznosítása például a városi építészetben, vagy a polgárőrséggel történő együttműködés nem újkeletű együttműködési megoldások. Az építészeti bűnmegelőzés (Barabás ed., 2023) során ugyanakkor a bűnözés kriminológiai elemzése, a bűnügyi adatok – lényegében közérdekű adatok, bűnözési statisztikák és azokból levont tudományos eredmények – hasznosításáról van szó, tehát az „együttműködés", az információ hasznosítása meglehetősen egyirányú. A polgárőrséggel[5], a helyi civil kezdeményezéssekkel történő együttműködés pedig kevésbé stratégiai jellegű, sokkal inkább a rendőrség rendészeti kapacitásainak (leginkább a bűnmegelőzési célú jelenlét, illetve a tetten ért elkövető visszatartása területén történő) kiegészítéséről beszélhetünk; a rendőrségi bűnügyi erőforrásainak, konkrét információk intézményesített megosztása nem lehetsé-

5 A polgárőrségről és a polgárőri tevékenység szabályairól szóló 2011. évi CLXV. törvény

ges. Kétségtelen ugyanakkor, hogy a céljának megfelelően ez az együttműködés is képes kiváló szinten és hatékonysággal működni.

Megítélésünk szerint e szűk körben és nagyon röviden bemutatott együttműködési megoldások is azt mutatják, hogy a bűnüldöző szervek legfeljebb csak érintőlegesen, egy-egy bűnügyi jelenségtől eltávolodva, általános szinten tarják elképzelhetőnek az együttműködést. Ehhez képest ugyanakkor a pénzügyi szektor esetében kialakult, illetve kialakulóban lévő együttműködési formák minőségileg különböznek, és valós feladatmegosztásról, erőforrások/információk kölcsönös rendelkezésre bocsátásáról beszélhetünk.

3. A PÉNZÜGYI SZEKTORT ÉRINTŐ EGYÜTTMŰKÖDÉSI IGÉNY KIALAKULÁSÁNAK FELTÉTELEI

Ahhoz, hogy a pénzügyi szektort érintően minőségi szemléletváltásra kerüljön sor a köz- és magánszféra együttműködésével (public-private-partnership vagy PPP rendszer) kapcsolatban, több sajátos kényszerítő körülmény, illetve adottság együttes fennállására volt szükség.

3.1. Online csalások, a bűnözés minőségileg új jelensége

Mindenekelőtt annak felismerése volt indokolt, hogy az online csalások esetében egy újszerű társadalmi, büntetőjogi jelenség alakult ki. A korábbi években egyes – többnyire vagyon elleni – bűncselekmény-típusok elszaporodása esetében azt lehetett tapasztalni, hogy megfelelő igazgatási, munkaszervezési megoldások alkalmazásával, a hatósági kapacitások megfelelő átcsoportosításával viszonylag hatékonyan lehetett kezelni egyes jelenségeket. Például, a 2000-es években jellemző zsebtolvajlás elszaporodását eredményesen kezelte a Budapesti Rendőrfőkapitányságon belül egy speciális rendőri egység felállítása, majd a térfigyelő kamerák megszaporodása; a gépkocsilopásokat, illetve a gépkocsik futásteljesítményének manipulálását az eredetvizsgálati, műszaki vizsgáztatási, a nyilvántartási szabályok szigorítása[6]; a közelmúltban megszaporodott unokázós csalásokat[7] a felvilágosító kampányok, illetve a fokozott rendőri fellépés eredményeképpen a szervezők elfogása.

6 https://www.mgoe.hu/nem-csak-magyar-betegseg-az-oratekeres-de-javul-tendencia

7 https://vansegitseg.im.gov.hu/idosek-celkeresztben-igy-vadasznak-aldozataikra-az-unokazos-csalok/

A térben vagy időben elszaporodott bűncselekmények közös jellemzője volt, hogy végső soron fizikai korlátok határolták be terjedésüket. Több bűncselekmény elkövetéséhez a bűncselekményt szervezők és elkövetők oldalán is több – többnyire személyi – erőforrás-ráfordításra volt szükség. Emellett az elkövetéshez felhasznált erőforrás-ráfordítás „csupán" arányosan növelte az elérhető „eredményt". Az elkövetési módszerek változásával a bűnözés növekedése elsősorban mennyiségi változást eredményezett, amely alapvetően mennyiségi választ (többlet erőforrást) igényelt, illetve megfelelően innovatív, igazgatási megoldásokkal akár erőforrás-megtakarítást is el lehetett érni, egy-egy jelenség ellehetetlenülésével (például: gépkocsi kilométerszámláló manipulálását ellehetetlenítő műszaki és igazgatási megoldások).

Ehhez képest az online csalások esetében a bűnözés újfajta, minőségi változásával kell szembenéznünk. Egyrészt ebben az esetben a bűncselekmények mennyiségi változása lényegében független az elkövetésben közreműködők számától. Az informatikai megoldásokkal tulajdonképpen végtelen számú sértett sérelmére, végtelen számú kísérlet elkövethető, amely így nem igényel végtelen számú emberi erőforrást, és a tevékenységet a térben sem korlátozza semmi (Kovács–Terták, 2024). Másrészt kijelenthető, hogy nehezen képzelhető el kijátszhatatlan rendszer, különösen, ha a sértetti oldal megtévesztésével – tehát a sértett aktív közreműködésével – valósul meg a bűncselekmény (Biró–Kiss, 2024).

A korábban hasznosnak bizonyult „igazgatási" jellegű megoldások így kevésbé működőképesek. Természetesen elképzelhető lenne a biztonsági megoldások olyan mértékű szigorítása (offline térbe terelése), amely minimálisra szűkíti a visszaélés kockázatát, ez azonban a jelenlegi pénzügyi rendszer lényegét, kényelmi funkcióját üresítené ki és a bekövetkezett digitális forradalom eredményével nem is egyeztethető össze (Schenk, 2018). Ez az út tehát nem tűnik járhatónak, nem igazán képzelhető el egy olyan egyszerű módszer, amely az online pénzügyi szolgáltatások minden innovatív és kényelmi funkcióját megtartva egyik napról a másikra ellehetetleníti az online csalások elkövetését.

Az online csalások esetében tehát olyan minőségileg új jelenség jelent meg, amelylyel szemben a bűnüldöző szervek kapacitásának növelése nem eredményezhet megfelelő megoldást. Minőségi kihívást nem lehet csupán mennyiségi megoldással kezelni, ezért indokolt alternatív megoldás keresése, amely egyébként több mint kézenfekvő.

3.2. Informatikai rendszereket támadó kiberbűnözés esetén a bűnmegelőzési adottságok és képességek hiánya

Az alternatív megoldáskeresés sürgető kényszere mellett az online csalások elleni küzdelem területén a PPP rendszer evolúcióját a pénzügyi szektor sajátos adottságai, képességei is alapjaiban meghatározták.

Jelen cikk szerzője a PPP rendszerben rejlő lehetőségekről és az ezzel kapcsolatos szemléletváltásról először 2020 decemberében egy kiberbűnözésről[8] tartott konferencián hallott egy érdekes előadást. Az előadás lényege az volt, hogy az informatikai rendszereket érő támadások esetén az informatikai rendszer működtetője és a bűnüldöző hatóság érdeke azonos, az informatikai tudás a rendszer működtetőjének oldalán jelentős és nélkülözhetetlen, így a rendszer működtetője érdemben közre tud és közre is kíván működni a büntetőeljárás eredményes lefolytatásában. Jóllehet a kiberbiztonságot sértő bűncselekmények és a pénzügyi szektor sérülékenységét „kijátszó, kihasználó" online csalások között számottevő hasonlóság fedezhető fel, az informatikai rendszereket közvetlenül támadó kiberbűnözés területén közel sem tud a köz- és magánszféra olyan szintű stratégiai együttműködése kialakulni, mint a pénzügyi szektort érintő online csalások esetében.

Az informatikai biztonsági rendszerek működtetése esetében ugyanis a sértetti oldalon alapvetően két érdekkör azonosítható, amely alapjaiban szűkíti le az együttműködési lehetőségeket: vagy egy rendszert működtető informatikai fejlesztőről beszélhetünk, amelynek számos ügyfele van (például operációs rendszert fejlesztő, vírusvédelmet biztosító fejlesztő, stb.), vagy egy adott entitásról (gazdasági társaságról, magánszemélyről), amely a saját informatikai rendszerét működteti. Első esetben nehezen határozható meg, hogy a rendszer sebezhetősége milyen célból használható ki, hiszen a felhasználók nem alkotnak homogén rendszert, így számos módon, okból, célból, indítékból válhatnak sértetté. A fejlesztő elsődleges célja az informatikai rendszer aktuális sebezhetőségének kijavítása, függetlenül attól, hogy azt milyen célból használták, használhatták ki, a sérüléssel milyen kárt okoztak. A saját/egyedi informatikai rendszert működtető entitások esetében kriminalisztikai szempontból szintén nehéz lenne általánosítani, miért az adott entitás informatikai rendszerét érte támadás. Az elkövetett bűncselekmény alapvetően egyedi. A bemutatott esetekben tehát a bűncselekmény elkövetését követően valóban van a büntetőeljárás eredményességéhez fűződő érdek és együttműködési képesség a fejlesztő, rendszert működtető oldalán, azonban ez alapvetően egy egyedi ügyben felmerülő, egyoldalú – a büntetőeljárás eredményessége irányába mutató – együttműködés, ami nem különbözik

8 V4CyberPower Conference 2020.12.3-4. https://iws.gov.pl/en/konferencja-v4cyberpower/

minőségileg a sértetteknek a bűnüldöző hatóságokkal történő együttműködési készségétől, képességétől. A sajátosság ebben az esetben nyilvánvalóan a rendkívül speciális, a sértetti oldalon azonosítható professzionális informatikai tudás. Nem azonosítható azonban egy olyan társadalmi vagy bűnügyi jelenség, amely az aktorok együttműködésével lenne hatékonyan kezelhető. A megelőzés, a jövőbeni bűncselekmény elhárítása körében – tehát a büntetőeljárásból „visszafelé" irányuló módon – nem igazán képzelhető el érdemi együttműködés. Egy adott informatikai rendszert érintő támadás sikere többnyire független más informatikai rendszerek sebezhetőségétől. Az adott informatikai támadást lehetővé tevő sérülékenységet pedig többnyire a fejlesztő, a rendszert működtető maga tárja fel, ebben a bűnüldöző szervek nem igazán tudnak érdemben hozzáadott értéket képviselni. Az így azonosított és kijavított sérülékenységek nem hozhatók összefüggésbe a jövőbeni – teljesen új módszereket, sérülékenységet kihasználó – támadásokkal. Emellett az azonosított támadási módszerek olyan informatikai megoldások, adatok, amelyek esetében az adatvédelem, illetve a magán- vagy egyéb titok védelemének jogi problémái nem értelmezhetők, így annak sincs akadálya, hogy az érintett fejlesztők a tapasztalataikat – minden további hatósági közreműködés nélkül – megosszák egymással. Amennyiben pedig az adott biztonsági incidenst kiváltó sérülékenységet kijavították, az elkövetéshez használt konkrét módszer a továbbiakban ellehetetlenül. Végezetül alapvető különbség az is, hogy az informatikai rendszereket érintő támadások esetén a sértettek (akár az informatikai rendszert fejlesztő, akár az azt használó személyek) köre oly mértékben heterogén, hogy nem azonosítható olyan személyi kör, akik vonatkozásában értelmezhető lenne valamilyen jövőbeni sérülékenység kezelésére irányuló stratégiai együttműködés.

3.3. A pénzügyi szektor sajátos bűnmegelőzési adottsága és képessége

Az informatikai rendszereket támadó kiberbűnözéssel ellentétben a pénzügyi szektort érintő online bűncselekmények esetében sajátos helyzet állt elő:

- az érintetti kör körülhatárolható és homogén (pénzügyi szolgáltatást nyújtó gazdasági társaságok),
- az online csalások célja nem az egyes szolgáltatók informatikai infrastruktúrájának megtámadása (a különböző rendszerek miatt nem beszélhetnénk homogén jelenségről), hanem az informatikai megoldásokat felhasználók támadása,
- az informatikai sérülékenység kiküszöbölésével ellentétben, amikor a biztonsági rés bezárása megszünteti a jelenséget, egy felhasználó biztonsági kockázatának csökkentése nem eredményezi más felhasználók biztonsági kockáza-

tának csökkenését, sőt még az sem zárható ki, hogy a korábban megtévesztett felhasználó váljon ismét visszaélés áldozatává,

– a pénzügyi szektor által a felhasználóknak nyújtott szolgáltatások és azok igénybevételi megoldásai alapvetően egységesek, illetve egységesen fejleszthetők (pénzügyi szolgáltatás),
– az elkövetői kör a rendszer felhasználóit (az ügyfeleket) arra tekintet nélkül támadja, hogy mely pénzügyi szolgáltatóhoz tartoznak, vagyis az ügyfelek sokaságán keresztül a pénzügyi szektor egésze áll az elkövetők célkeresztjében, és nem csupán egyes pénzügyi szolgáltatók,
– az elkövetés során használt megoldások nem egyediek (például, az elkövetéshez használt technikai eszköz/megoldás, „money-mule számlaszám"[9], célszámla, készpénzfelvételi hely, stb. [Nagy, 2018]),
– a pénzügyi szektor oldalán rendkívül jelentős erőforrások és kiváló szakemberek állnak rendelkezésre, akik az informatikai rendszereket működtetik, fejlesztik.

Ebben az esetben tehát olyan homogén tulajdonságokat mutató tömegjelenséggel állunk szemben, amelyben az

– elkövetés sajátosságai,
– a pénzügyi szektor képessége és érdekei (Vass–Kovács, 2019),
– a bűnüldöző szervek képessége és érdekei

érdemi lehetőséget biztosítottak a stratégia együttműködésre, feladatmegosztásra.

A stratégiai együttműködés mindkét érintett (pénzügyi szolgáltatók és bűnüldöző szervek) számára valódi hozzáadott értéket jelent, mert nem csupán a bűncselekmény megvalósulását követően képzelhető el a nyomozás szakértői szintű támogatása (ahogy az az információs rendszereket érintő együttműködésnél is lehetséges), hanem a jövőbeni bűncselekmények elkerülése terén is. Ez utóbbi azt eredményezi, hogy az állam, illetve a hatóságok közreműködésével a pénzügyi szektor immunrendszere számottevően erősíthető és képessé tehető az újabb visszaélések megakadályozására. Az együttműködési/feladatmegosztási forma az állam/hatóság részéről továbbá nem csupán általános, módszertani jellegű lehet (mint például az építészeti bűnmegelőzés területén), hanem konkrét, egyedileg azonosítható turpis tranzakciók elkerülését is képes biztosítani. Az együttműködés révén a pénzügyi szektor szereplői a bűncselekmény elkövetését követően

9 A pénzeszközök nyomon követésének megnehezítését szolgáló olyan köztes számlák, amelyeket időszakosan használnak, gyűjtőszámlaként, illetve továbbutalás érdekében.

érdemben közre tudnak működni a felderítésben, a bűncselekményből származó vagyon biztosításában, a hatósági oldal pedig érdemben közre tud működni az újabb visszaélések megelőzésben. A végeredmény is egymást erősítő, ugyanis nem csupán a büntetőeljárások hatékonysága nőhet, hanem a bűncselekmények száma is visszaszorítható, vagyis a meglévő hatósági kapacitások is hatékonyabban, eredményesebben tudnak hasznosulni. Nyilván hiúság lenne azt állítani, hogy ekképpen az online csalások jelensége leküzdhető lenne, de az talán kijelenthető, hogy ilyen módon minden korábbi egyoldalú megoldásnál hatékonyabban kezelhető.

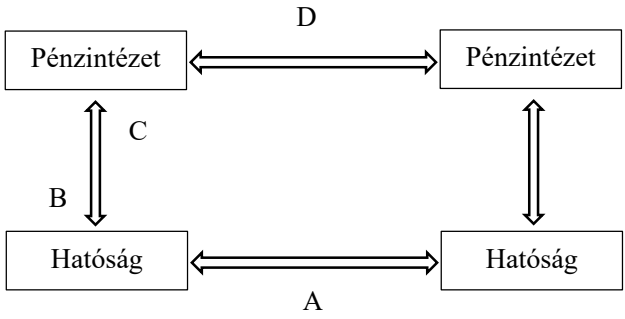
4. A PÉNZÜGYI SZEKTORT ÉRINTŐ PPP RENDSZER SAROKPONTJAI

Az együttműködés módszertanának két megoldandó kihívása: az információmegosztás (Vogel–Costa–Lassalle /eds., 2024/; EUCPN, 2023), valamint a rendelkezésre álló erőforrások hatékony elosztása.

4.1. Információmegosztás

A pénzügyi szektort érintő bűnügyi jellegű információmegosztásnak sematikusan négy iránya képzelhető el *(1. ábra)*:

1. ábra
A pénzügyi szektort érintő bűnügyi jellegű információmegosztás irányai



Forrás: saját szerkesztés

A: A hatóságok közötti információmegosztás nem újszerű, ennek kereteit a törvényi rendelkezések pontosan meghatározzák. A hatóságok közötti információmegosztás esetében a megosztás iránya szerint nem indokolt különbséget tenni

(mely hatóság, mely hatósággal oszt/ oszthat meg információt), a szabályozási logika lényegében azonos: az adott hatóság hatáskörében eljárva, feladatának ellátásához szükséges információ megszerzése, megosztása mikor, milyen feltételekkel biztosított. Általánosságban kijelenthető, hogy a büntetőeljárásban eljáró szervek hozzáférése rendkívül szűk körben korlátozott (egyes védett érdekek, mint műveleti érdek vagy adat nemzetbiztonsági célból történő minősítése képezheti a megismerés akadályát).

B: A pénzintézetek és a hatóság közötti információmegosztás, a megosztás iránya mentén két részre osztandó. A hatóságok irányába történő magán információ megosztása szintén rendkívül szűk körben korlátozott. Egyes kiemelt védendő érdekektől eltekintve (például a védői titok) a büntetőeljárásban eljáró szervek lényegében bármilyen adathoz hozzáférhetnek. Jellemző az adatok megismerésének bizonyos garanciális feltételekhez (ún. külső engedélyhez) kötése, azonban ez nem a megismerés akadályozását, hanem annak észszerű keretek között tartását célzó intézkedés.

A hatóság irányában történő információáramlás alapvető logikája a hatóság megkeresésére történő adatszolgáltatás, amelynek teljesítése ki is kényszeríthető. Ez a logika következik a büntetőeljárásban eljáró szervek feladatából és az ehhez biztosított kényszer alkalmazhatóságából. A PPP konstrukcióhoz tartozó információmegosztás újszerűsége ehhez képest két eltérést tartalmaz. Egyrészt a saját kezdeményezésre történő (önkéntes) információmegosztást, másrészt a hatósági megkeresésre történő (kényszer)információ-megosztás hatékonyságának növelését.

Ezek azonban az információmegosztás lehetőségét érintően minőségi újdonságnak nem tekinthetők, a szabályozás alapvető logikája nem változott.

C: A pénzintézetek és a hatóság közötti információmegosztás másik iránya, amely a magánszektor irányába mutat, ugyanakkor már minőségi eltérést jelent. A hatósági eljárások logikájára nem jellemző az információ kijuttatása a saját rendszeréből. Az érdemi együttműködés és a pénzügyi szektor bevonása a bűncselekmények megelőzésébe ugyanakkor nem képzelhető el az információk ilyen irányú megosztása nélkül. Természetesen ez nem jelenthet parttalan információáramlást, az elérni kívánt célhoz igazodó keretek kialakítása igazi szabályozási kihívás, amelynek kereteit meg kellett teremteni.

D: Végezetül a magánszektorban kezelt információk, adatok megosztásának kérdéskörét kell áttekinteni. A pénzügyi szektor esetében ezt a kérdést alapjaiban korlátozza az adatvételem és a banktitok, fizetési titok, értékpapírtitok, pénztártitok vagy biztosítási titok (a továbbiakban együtt: pénzügyi titok) szigorú és nem véletlenül kialakult szabályozása. A pénzügyi szektor nem válhat egy kötetlenül kezelhető óriási adatbázissá, amelyben a pénzintézetek egymás adatait szabadon

megosztva és felhasználva döntenek a megelőzéshez általuk szükségesnek tartott intézkedésekről. A megelőzéshez szükséges korlátozások (tranzakció tiltás) az állami kényszermonopóliumhoz tartoznak, amelyek teljes körű magánkézbe adása, „kiszervezése" alapvető jogállamisági problémákat vetne fel. A hatékony PPP együttműködéshez ugyanakkor az információmegosztás ezen irányát is biztosítani kell, ami szintén jelentős szabályozási kihívást jelent.

4.1. Erőforrások és feladatok hatékony megosztása

A PPP rendszer működőképességét meghatározó másik kihívás a hatékony feladatmegosztás, a két szektor feladatainak – profilhoz illő – összehangolása, ezáltal a két szektorban rendelkezésre álló erőforrások hatékony felhasználásának biztosítása. Olyan hatékony megoldás kidolgozása szükséges, amely egyrészt összhangban van az érintett szereplők alkotmányos helyzetével, másrészt összhatását tekintve szinergiát eredményez, vagyis nem pusztán arra alkalmas, hogy például egy adott feladathoz kétszer annyi erőforrást biztosítson, amellyel az adott feladat fele annyi idő alatt elvégezhető. Ez csupán az erőforrások arányos – mennyiségi – növekedését jelenti, azonban, ahogy azt korábban már jeleztük, az online bűncselekmények minőségi kihívására nem elégséges mennyiségi választ adni.

Az alkotmányos keretek megtartása mellett nem elfogadható például a magánszektor állami feladatokkal, hatósági intézkedési kötelezettséggel, kényszerintézkedési lehetőségekkel történő közvetlen felruházása. Az állami erőszak monopólium, a bűnüldözéssel kapcsolatos állami feladat nem átruházható. Amellett, hogy ez az állam egyik esszenciája, az alkalmazásával járó felelősségi- és garanciarendszer sem biztosítható, miközben a hatósági jogkörök keretei évszázadok tapasztalatai alapján váltak szükségessé. A pénzügyi szektor szereplői az ügyfeleikhez hasonlóan a magánszférába tartoznak, közöttük alapvetően az egyenrangúság az irányadó, felelősségi rendszerük kiegyensúlyozott. A hatósági döntéseket és lehetőségeket ezzel szemben aszimmetria jellemzi, és a döntések következményeiért viselt felelősség is eltérő jogi alapokon nyugszik. Amellett, hogy a pénzügyi szektor hatósági jogkörökkel történő felruházása beláthatatlan következményekkel, alappal feltehetően például az ügyfelek részéről jelenleg fennálló bizalom elenyészésével járna, egy ilyen megoldás nem lenne tényleges feladatmegosztásnak sem tekinthető, pusztán a hatósági erőforráshiány kiszervezését jelentené a magánszektorba. Ráadásul, nem lenne elkerülhető a hatósági oldal fejlesztése sem, hiszen a nyomozóhatósági feladatok kiszervezésével a büntetőeljárások száma is sokasodna, így a törvényességi oldal (bíróság, ügyészség) fejlesztése sem maradhatna el. Mi több, a büntetőeljárások számának várható növekedésével járó terhekkel a büntető igazságszolgáltatás nyilvánvalóan nem bírna lépést tartani.

Egy ilyen megoldás továbbá szükségszerűen termelné ki a szektorok közötti ellentmondásokat is, hiszen a pénzügyi szektor „rövid távú" érdeke azt diktálná, hogy minden egyes cselekményt megakadályozzon, illetve helyrehozzon, míg a nyomozó hatóság műveleti érdeke sok esetben kívánja meg a folyamatok – többnyire – időleges tovább engedését.

Szintén elképzelhetetlen a fordított irányú szélsőséges megoldás: a nyomozóhatósági erőforrások teljes körű rendelkezésre bocsátása a pénzügyi szektor számára, hogy ezáltal legyen biztosított a pénzügyi tranzakciók biztonságos lebonyolítása, a turpis jogügyletek elkerülése, a megvalósult online csalások esetén pedig vagyon visszaszerzése. A büntetőeljárás alapvetően retrospektív jellegű, az állam számára a büntetőjog széles eszköztára azért áll rendelkezésre, mert a társadalmat olyan sérelem érte (vagy annak közvetlen veszélye áll fenn), amely indokolja mindezen eszközök alkalmazhatóságát. A büntetőjogi eszközrendszer bűnmegelőzési célokra nem, vagy csak rendkívül korlátozottan alkalmazható. Amellett, hogy a nyomozóhatósági eszközrendszer felhasználása a pénzügyi szektor érdekeinek – egyébként nem vitatható – védelmében szintén alapvető alkotmányos elveket sértene, a büntető igazságszolgáltatás erőforrásait lényegében teljes mértékben elvonná a bűnüldözési feladattól. Így a büntető igazságszolgáltatás végső soron éppen azt nem lenne képes megvalósítani, ami a feladata: az elkövetett bűncselekmény felderítését, az elkövető felelősségre vonását (mert tökéletes megelőzés nem képzelhető el). A nyomozó hatóság erőforrásainak ilyen célú felhasználása hatékonysági szempontból is elégtelen. A nyomozóhatósági erőforrások – ügyletekre koncentráló – elaprózódása hátráltatná a bűncselekményeket szervező, irányító, az elkövetési módszereket kidolgozó, az ahhoz szükséges technikai eszközöket biztosító személyek felderítését.

A bemutatott – szándékosan – végletes megoldási módszerek helyett célravezetőbb a két szektor természetes szervezeti (ön)érdekeit szem előtt tartó megoldás keresése. Nehezen vitatható, hogy a pénzügyi szektor érdeke az egyes visszaélést megvalósító tranzakciók elkerülése (bűnmegelőzés), a büntető igazságszolgáltatás célja pedig inkább a megvalósult bűncselekmény hatékony felderítése, az elkövető(k) felelősségre vonása (bűnüldözés). Ennek megfelelően a feladatok és az erőforrások olyan megosztása indokolt, amely eredményeképpen

1. számottevően javul a pénzügyi szektor bűnmegelőzési képessége,
2. a pénzügyi szektor megelőzési eredményei (adatai) képesek érvényesülni a bűnüldözés területén is, továbbá
3. a pénzügyi szektor által elvégzett, illetve átvállalható feladatok okán, csökken a büntető igazságszolgáltatásra nehezedő nyomás, így a hatóságok a rendelkezésre álló erőforrásaikat jobban tudják elsődleges feladatukra, az elkövetők elfogására és felelősségre vonására koncentrálni.

A szektorok sajátosságaihoz ilyen módon illeszkedő feladatmegosztás több szempontból is szerencsés. Egyrészt nem szükséges hozzá a hatósági és a magánjogi feladatok, felelősségi körök keveredése. Ennek megfelelően a pénzügyi szektor bűnmegelőzési (illetve pénzügyi rendszeren belüli vagyonbiztosítási) feladatához szükséges eszközök nem vetnek fel alkotmányos aggályokat, így a pénzügyi szektor eszközei lényegesen alacsonyabb garanciális követelmények mellett is működtethetők. A feladatmegosztás a pénzügyi szektor munkatársi oldalán sem eredményez szereptévesztést, és nem kényszerít hatósági logikát, szemléletet igénylő döntéshozatalra. Másodsorban az egyes szektorok valóban azzal tudnak hatékonyan foglalkozni, amiben érdekeltek, vagyis nem szükséges külön motivációs megoldásokat, eredményességet mérő módszereket kidolgozni. A hatékony bűnmegelőzés a kár számszerűen kimutatható csökkenését eredményezheti a pénzügyi szektor oldalán, ami objektív értékmérője lehet a szakterület hatékonyságának. A nyomozó hatóságok esetében sem szükséges külön motiváció ahhoz, hogy egy-egy jelentősebb szervezett bűnözői csoportot felderítsenek és eredményesen bíróság elé állítsanak, amelyet nagyban elő tud segíteni, ha a rendelkezésre álló erőforrásaikat nem egy-egy csalárd tranzakció nyomonkövetésére kell szétforgácsolni.

5. EGYÜTTMŰKÖDÉSI FÓRUMOK

Adott tehát egy olyan minőségileg új jelenség, amelyben az érintett szereplők (pénzügyi szolgáltatók, bűnüldöző hatóságok) jelentős erőforrásokkal rendelkeznek, amelyek újszerű összehangolása valóban képes lehet minőségi választ nyújtani az előttünk álló kihívásokra. Az elmúlt években az együttműködés, illetve az együttműködési formák kidolgozása több fórumon is megindult.

5.1. KiberPajzs - 2022

Mára már lényegében széles körben elfogadott tény, hogy a koronavírus járvánnyal járó társadalmi változások, a mindennapjaink egyre inkább online térbe történő áthelyeződése nyomán indult el az online csalások exponenciális növekedése.[10] A jelenség változását és méreteit elsőként a közvetlenül érintett pénzügyi szektor észlelte. Nem véletlen tehát, hogy a jelenséggel szembeni közös fellépés igénye is szakmai kezdeményezésként indult el.

10 https://www.mnb.hu/letoltes/1-fizetesi-rendszer-jelentes-2024-tovabb-fejlodik-a-hazai-penzforgalom-indul-a-qvik.pdf; Frész, 2025; Terták–Kovács, 2023.

A KiberPajzs[11] együttműködési platformot a Magyar Nemzeti Bank, a Magyar Bankszövetség, a Nemzeti Média- és Hírközlési Hatóság, a Nemzeti Kibervédelmi Intézet és az Országos Rendőr-főkapitányság (a továbbiakban: ORFK) 2022-ben hozta létre.

A kezdeményezéshez azóta számos további résztvevő – más kormányzati szereplők mellett – az Igazságügyi Minisztérium is csatlakozott, legutóbb pedig 2024. év végén bővült a kezdeményezés a Szerencsejáték Zrt., a Mastercard és a Visa szakmai partnerként történő csatlakozásával.

Az alulról építkező szakmai kezdeményezés a meglévő jogszabályi és szervezeti keretek között, „puha eszközként" tud működni. Ennek megfelelően a köz- és magánszféra közötti együttműködés korábban bemutatott információmegosztás, illetve feladatmegosztás jogrendszeri kötöttségéből eredő kihívásaival érdemben nem birkózhatott meg. Ennek ellenére a kezdeményezés mérföldkő volt az online bűncselekmények elleni harcban, mert egyértelművé tette az aktorok számára, hogy a jelenséggel együtt, összefogva kell megküzdeni. A meglévő jogi keretek között a nyomozó hatóság és a pénzügyi szektor közötti együttműködés alapvetően általános jellegű tudásmegosztást, tapasztalatcserét, illetve meglévő eszközök gördülékeny működtetését tűzhette ki célul. A KiberPajzs egészének célja is leginkább a figyelemfelhívás, a tudatosságnövelés, az áldozatvédelem, illetve a jelenséghez kapcsolódó általános tudásmegosztás volt. Emellett a KiberPajzs célkitűzései között megjelent a szakmai együttműködés keretei között felmerült jogalkotási javaslatok kormányzat irányába történő becsatornázásának igénye is.

A KiberPajzs munkája, eredményei és szellemisége nagyban segítette az egyes pénzintézetek és az ORFK között létrejött együttműködési megállapodások aláírását.

5.2. Az Igazságügyi Minisztérium által koordinált kormányzati munkacsoport – 2023

A szakmai kezdeményezés és együttműködés mellett a jelenség társadalmi mértéke és hatása egyértelművé tette, hogy a megoldáskeresés során a meglévő jogi keretek felülvizsgálata és szükség esetén annak átalakítása sem mellőzhető, amely kormányzati fellépés nélkül nem lehetséges. Erre figyelemmel dr. Tuzson Bence igazságügyi miniszter kezdeményezésére 2023. december 14-én az érintett kormányzati, bűntetőeljárásban eljáró és a pénzügyi szektorhoz tartozó szervezetek vezetőinek támogatásával egy olyan munkacsoport felállítására került sor, amely-

11 kiberpajzs.hu.

nek célja az online bűncselekmények elleni hatékony fellépéshez szükséges jogszabály-módosítások előkészítése volt.[12] A munkacsoportban megjelenő szervek többsége a KiberPajzsban is aktív közreműködő volt, ugyanakkor a két formáció feladatmegosztása nem szükségtelen párhuzamot, hanem hatékony munkamegosztást eredményezett. Az Igazságügyi Minisztérium (a továbbiakban: IM) által koordinált munkacsoportban hasznosulhattak azok a szakmai tapasztalatok, amelyeket a pénzügyi szakterület a KiberPajzs keretei között már feldolgozott, így egyes szakkérdések már kiforrott álláspontként jelentek meg a kormányzati munkacsoportban. Másrészt az IM munkacsoport célja kifejezetten a megfelelő, esetleg hiányzó jogi keretek, jogintézmények kialakítását tűzte ki célul, így a két munkacsoport fókusza sem volt átfedésben.

A köz- és magánszféra együttműködésének újszerűsége és hatásossága a munkacsoport tevékenységében is megjelent. Annak ellenére, hogy egy kifejezetten büntetőjogi jelenséggel szembeni fellépést célzó jogszabály előkészítő munka folyt, rendkívül hatékonynak bizonyult, hogy az érintett szektorok a kezdetektől részesei lehettek a megoldás keresésének, ezzel is támogatva a hiábavaló, eleve működésképtelen vagy kevéssé hatékony megoldások elkerülését. A munkacsoport emellett lényegében a kezdetektől a korábban bemutatott információmegosztáson, valamint hatékony együttműködésen és feladatmegosztáson – a bűnmegelőzés-bűnüldözés különböző szektorok szerinti elhatárolásán – alapuló megoldások, jogintézmények keresése érdekében végezte a munkáját, amely elképzelhetetlen lett volna valamennyi érintett bevonása nélkül. A munkacsoport így a büntetőeljárások hatékonyságának növelése mellett, talán még nagyobb figyelmet fordított a jelenség büntetőeljáráson kívüli hatékony kezelhetőségének tárgykörére, ezzel a büntető igazságszolgáltatásra nehezedő túlterhelés csökkentésére.

A munkacsoport működésének megkezdését követően a büntetőjogi szabályozás területén több, kifejezetten az online bűncselekmények elleni fellépés hatékonyságát növelni hívatott jogszabály módosítására került sor (keretengedély, illetékességi szabályok átalakítása, stb.). Ezek a módosítások a büntetőjogi szabályozás organikus fejlődéséhez tartoznak, és a büntetőeljárással érintett hivatásrendekkel szoros együttműködésben, a felmerült gyakorlati tapasztalatok alapján alakultak ki. A bűnüldözés hatékonyságát közvetlenül érintő szabályozási megoldások ugyan fontosak, és a jogalkotásnak a jövőben is fogékonynak kell lenni azon szakmai igényekre, amelyek ezen a területen felmerülnek. Ugyanakkor, véleményünk szerint a munkacsoport elmúlt másfél évben elért eredményei valódi, minőségi

12 Az egyeztetésen az Igazságügyi Minisztérium, a Belügyminisztérium, a Pénzügyminisztérium, a Gazdaságfejlesztési Minisztérium, a Magyar Nemzeti Bank, a Magyar Bankszövetség, az Országos Bírósági Hivatal, a Legfőbb Ügyészség, az Országos Rendőr-Főkapitányság és a Nemzeti Adó- és Vámhivatal Pénzmosás- és Terrorizmusfinanszírozás Elleni Iroda vezetői vettek részt.

előrelépést jelentenek. Számos olyan jogszabály született, amely mind a pénzügyi, mind a bűnügyi szektort érinti, és amelyeket kifejezetten a fent bemutatott köz- és magánszféra együttműködése, valamint az információ- és feladatmegosztás irányába tett lépésként lehet értékelni.

6. AZ ELMÚLT IDŐSZAK PPP RENDSZERHEZ KAPCSOLÓDÓ EREDMÉNYEI

6.1. Együttműködési megállapodások

A köz- és magánszféra közötti stratégiai együttműködés kezdetét az egyes pénzintézetek és az Országos Rendőr-főkapitányság közötti együttműködési megállapodások jelentették. A kifejezetten az online csalások elleni hatékony fellépést célzó együttműködési megállapodás megkötésére az OTP Bankkal 2023 novemberében[13], a CIB Bankkal 2025. január elején[14] került sor.

Az együttműködési megállapodások alapvetése, hogy tartalmuk, illetve a bennük foglalt együttműködési mechanizmusok nem nyúlhatnak túl a meglévő jogszabályi kereteken. Az együttműködési megállapodás tehát nem keletkeztethet jogot, ugyanakkor képes lehet a meglévő jogi eszközök hatékony működésének biztosítására. Az információmegosztás kerete, jogalapja, alaki követelményei tehát nem módosíthatók, de meghatározhatók például azok a csatornák, adatkérési sillabuszok, amelyek az információ áramlását rendkívüli mértékben felgyorsíthatják. Minden érdekelt számára előnyös helyzetet eredményez, ha a hatóság megismeri azokat az adatköröket, amelyeket a pénzintézetek kezelnek, megismeri azokat a mechanizmusokat, amelyek eredményeképpen egy-egy adatkör lassabban vagy gyorsabban hozzáférhető, azokat a paramétereket, amelyek mentén az adatkérés gyorsan feldolgozhatóvá válik, stb. Számottevően gyorsítható az együttműködés, ha a hatóság tudja, mit kérhet, mely adatok állnak azonnal rendelkezésre, milyen megjelöléssel, formában kérheti az információt. Az együttműködési megállapodások a feladatok észszerű tervezésére is irányulhatnak, megkülönböztetve sürgős és hosszabb időt igénylő/tűrő eseteket, ezzel is segítve, hogy az együttműködés ne terhelje túl a pénzügyi szektor kapacitásait.

Az együttműködési megállapodások a meglévő jogi kereteket nem feszíthetik szét, ezért azok megkötése valójában nem igényel külön jogi felhatalmazást

13 https://www.portfolio.hu/bank/20231117/az-online-csalasok-ellen-kotott-egyuttmukodesi-megallapodast-az-orfk-es-az-otp-652277.

14 https://hvg.hu/gazdasag/20250108_banki-csalas-megallapodas-rendorseg-cib-bank.

sem. Az együttműködési megállapodások „puha eszközök", azonban jelentőségük rendkívül nagy. Amellett ugyanis, hogy valóban képesek jelentősen javítani a meglévő jogintézmények gyakorlati alkalmazását, kézzelfogható bizonyítékai annak is, hogy a megállapodást megkötő felek egyaránt elkötelezettek a feladat végrehajtásában és ebben egymást partnerként kezelik; ez különösen a hatósági oldalon hozott szemléletváltást. Erre figyelemmel a kormányzat – már az Igazságügyi Minisztérium által koordinált munkacsoportban felmerült szakmai igények alapján – egyértelmű jogalkotási felhatalmazással kívánta támogatni e kezdeményezés elterjedését.

Ennek megfelelően az online csalások elleni további hatékony fellépés érdekében szükséges és egyéb törvények módosításáról szóló a 2024. évi LXIV. törvény valamennyi pénzügyi szektort érintő jogszabályban kifejezett felhatalmazást adott a pénzügyi (és más a nyomozó hatósággal kapcsolatban álló) szolgáltatók számára együttműködési megállapodás megkötésére.

6.2. Központi Visszaélésszűrő Rendszer

A Központi Visszaélésszűrő Rendszer[15] (a továbbiakban: KVR) elindítása a pénzügyi szektor monitoring tevékenységét támogató rendkívül modern informatikai megoldás, amely azonban csak érintőlegesen kapcsolódik a köz- és magánszféra együttműködésének kérdésköréhez. Ennek ellenére a 2025. július 1. napján indult[16] rendszer több sajátosságát is indokolt e körben megemlíteni.

Egyrészt a KVR is a pénzügyi szektort érintő információ közös hasznosítására törekszik. Ennek érdekében a GIRO Zrt. rendszerén átmenő tranzakciók elemzésére és a tranzakciók kockázati besorolására kerül sor. A KVR tehát nem jelenti az egyes pénzintézetek monitoring tevékenysége eredményeinek közvetlen megosztását, összekapcsolását. Az egyes pénzintézetek saját – szintén mesterséges intelligenciát alkalmazó – monitoring tevékenysége (Bagó Péter, 2023) alapvetően megelőzi a KVR értékelését, ugyanis az adott pénzintézet által kockázatosnak tartott tranzakció felfüggesztésével a tranzakció el sem jut a KVR értékeléséig. Természetesen a pénzintézet által átengedett, majd a KVR által kockázati besorolással ellátott tranzakció adatai a továbbiakban már beépülnek a pénzintézet

15 A KVR a Magyar Nemzeti Bank és Giro Zrt. által fejlesztett és üzemeltett, mesterséges intelligencia alapú, valós idejű tranzakció figyelő és értékelő rendszer. Az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény 2023. évi módosításával biztosított, hogy a fizetési szolgáltatók a KVR részére történő adattovábbítása ne minősüljön a fizetési titok megsértésének.

16 https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2025-evi-sajtokozlemenyek/mesterseges-intelligenciat-vet-be-a-jegybank-a-penzugyi-kibercsalasok-visszaszoritasaert.

monitoring rendszerébe, így végső soron a pénzügyi szektor egésze képes bizonyos adatok, információk hasznosítására. Egy adott pénzintézet tranzakciót megakasztó ismerete ugyanakkor ebben a rendszerben közvetlenül nem igazán tud hasznosulni: egyrészt, mert a KVR a saját tanulási algoritmusával és nem a pénzintézetek eredményeivel dolgozik, másrészt, mert a tranzakció pénzintézet által történő megszakítása el sem jut a KVR-hez.

Mindez az irányadó adatvédelmi és pénzügyi titokra vonatkozó szabályok, illetve a magánjogi felelősségi körben elérhető hatékonyság maximalizálásának tekinthető. Emellett a KVR organikusan illeszkedik a PPP rendszer feladatmegosztási logikájához is, hiszen jelentős mértékben képes javítani a pénzügyi szektor megelőzési képességein, vagyis az egyes tranzakciók tekintetében nagymértékben képes csökkenteni a terhet a büntető igazságszolgáltatáson, amely így képes az elkövetőkre, a szervezőkre koncentrálni.

A KVR a PPP rendszerében a továbblépés lehetőségeit érintően is izgalmas kérdéseket tartogat. Érdekes lehet majd megvizsgálni a KVR által megjelölt kockázati besorolások büntetőjogi hasznosíthatóságát, akár egyes konkrét büntetőeljárásokban, akár a bűnügyi értékelő-elemző tevékenység során. A KVR működési logikája ugyanis képes lehet összefüggéseket azonosítani egy konkrét büntetőeljárásban felmerült adatkör és a pénzügyi rendszerben végrehajtott vagy végrehajtani tervezett további tranzakciók között. Emellett a KVR által kimutatott mintázatok, összefüggések a büntetőeljárások megindításához szükséges rendészeti/bűnügyi hírszerzés, illetve előkészítő eljárások során alkalmazott értékelő-elemző tevékenység során is hasznosulhatnak (Nyeste–Szendrei, 2020; Nyeste, 2016).

Végezetül érdemes lehet megfontolni a KVR továbbfejlesztését a PPP rendszerében abból a szempontból, hogy a hatósági oldalról (legyen szó akár a pénzmosás és terrorizmus-finanszírozás elleni küzdelemről, akár a büntetőeljárások lefolytatásáról) felmerülő adatok milyen módon hasznosíthatók a KVR rendszerében.

6.3. Objektív bejelentési kötelezettség

Az online csalások elleni fellépés érdekében szükséges törvények és egyéb büntetőjogi tárgyú törvények módosításáról szóló 2024. évi XVIII. törvény 2024. augusztus 1. napjával módosította a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvényt (a továbbiakban: Pmt.) és bevezette az ún. objektív bejelentési kötelezettség jogintézményét. A Pmt. 30. §-a pénzmosás, terrorizmus finanszírozása vagy más bűncselekmény gyanúja esetén írja elő az adatszolgáltatásra kötelezettek számára (jelen esetben a pénzügyi szektor számára is), hogy az ilyen cselekményre utaló adat, tény, körülmény felmerülése esetén a Nemzeti Adó- és Vámhivatal Pénzmosás és Terro-

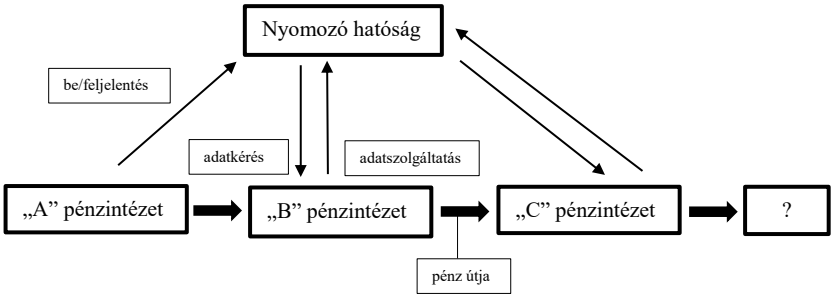
rizmusfinanszírozás Elleni Iroda (a továbbiakban: NAV PEI) számára bejelentést tegyenek. Tekintettel arra, hogy a bejelentés alapja a pénzintézet alkalmazottainak személyes észlelése, így a bejelentés ezen formáját indokolt szubjektív bejelentésnek nevezni.

2024. augusztus 1. napjával e bejelentési forma kiegészült a törvény új, 37/A. §-a szerinti bejelentési formával. A törvény visszaéléssel érintett ügyletként határozza meg az olyan fizetési műveletet – ide nem értve a kártyaalapú fizetési műveletet –, amely esetében észszerű okból csalás gyanúja merül fel azzal kapcsolatban, hogy a fizetési műveletet az ügyfél nem kívánta jóváhagyni, vagy tévedésben levő ügyfél hagyta jóvá. Ilyen körülmény felmerülése esetén a szolgáltató részére mérlegelést nem tűrő bejelentési és intézkedési kötelezettséget ír elő a törvény, ezért a gyakorlatban ez a bejelentési forma az objektív bejelentési kötelezettségként terjedt el.

A jogintézmény kidolgozására az IM által koordinált munkacsoportban, az ott felmerült szakmai igények alapján került sor. A pénzintézetek által végzett monitoring tevékenység (vagy a közelmúltban működésbe lépett KVR) képes megakadályozni a turpis tranzakciók indítását. Nyilvánvalóan ez tekinthető az ideális helyzetnek, hiszen ebben az esetben a sérelem nem következik be, a tranzakciót nem hajtják végre, a megszerezni kívánt pénzeszközök az észlelő pénzintézetben maradnak, a bűncselekmény befejezetlen marad. Ilyen esetben a pénzügyi szektor megelőző tevékenysége eredményes volt, a bűnügyi szakterület pedig megkezdheti a cselekmény felderítését, az elkövetők felkutatását, további sérelem a konkrét tranzakcióval kapcsolatban nem várható. Ugyanakkor nyilvánvaló, hogy a megelőző/monitoring rendszer nem lehet képes valamennyi csalárd tranzakció azonosítására és elhárítására. Ezekben az esetekben a pénzintézet rövid vagy kevésbé rövid időn belül értesül a turpis tranzakciókról. A gyakorlati tapasztalatok azt mutatták, hogy az egyes számlák közötti pénzmozgások, majd a pénz készpénzben történő felvétele vagy külföldre juttatása rendkívül rövid idő alatt, néhány órán, legfeljebb egy-két napon belül képes elérhetetlenné tenni a pénzeszközöket. Szakmai igényként fogalmazódott meg, hogy amennyiben a végrehajtott csalárd tranzakció észlelésére – akár a sértett bejelentése, akár más információ alapján – rövid időn belül sor kerül, úgy álljon rendelkezésre olyan eszköz, amely képes a pénzügyi rendszerben még elérhető pénzeszközök biztosítására.

Tekintettel arra, hogy ezekben az esetekben bűncselekmény elkövetéséről beszélünk, kézenfekvő megoldásnak tűnt a nyomozó hatóság lehetőségeinek, illetve kapacitásainak olyan mértékű bővítése, amely képes lehet kezelni a problémát. A büntetőeljárás klasszikus hatósági, illetve a hatósággal való együttműködési logikája alapján a nyomozó hatóság „csillagpontos" rendszerben kommunikál az adatszolgáltatásra kötelezettekkel. Vagyis a bejövő, beszerzett adat alapján azonosítja az újabb érintettet (pénzintézetet), majd annak megkeresését és a beérkezett adat feldolgozását követően tisztázza a soron következő érintettet (pénzintézet).

2. ábra
A folyamat sematikus ábrázolása



Forrás: saját szerkesztés

Belátható, hogy az online banki szolgáltatások világában elképzelhetetlen olyan mértékű erőforrás biztosítása vagy együttműködési megoldás kidolgozása, amely ebben az adatáramlási logikában képes lenne felvenni a versenyt a pénzügyi tranzakciók végrehajtásának sebességével. A tranzakciós láncban érintett pénzintézetek együttműködési (bejelentési) képességét és készségét pedig korlátozza, hogy jellemzően nincsenek tudatában annak, hogy a hozzájuk érkezett, illetve továbbengedett pénzeszközök csalárd jogügyletből származnak. Ez az információ csupán az „A" pénzintézet számára ismert, a „B" pénzintézet ezzel csak akkor szembesül, amikor a nyomozó hatóság a megkeresésével erről tájékoztatja. Így – a pénzintézetek belső monitoring rendszerének esetleges önálló jelzéseitől eltekintve – a tranzakciós folyamatban érintett további pénzintézetek nem képesek eredményes fellépésre, hiszen megfelelő információ hiányában ezek az intézmények nem azonosítják csalárdnak a tranzakciót.

A probléma kezelésének másik lehetséges elméleti megoldása a pénzügyi szervek számára biztosított teljes körű felhatalmazás, hogy az általuk csalárdnak minősített pénzügyi tranzakciók adatait szabadon megoszthassák más pénzintézetekkel, ezzel biztosítva, hogy a pénzeszközök a pénzügyi rendszeren belül maradjanak. Ez azonban ebben a formában egyrészt nem lenne összeegyeztethető az adatvédelmi, illetve a pénzügyi titokra vonatkozó szabályokkal, másrészt a korábban már említett állami kényszermonopólium – és az ezzel járó felelősség – kiszervezését jelentené, ami minden szempontból kerülendő.

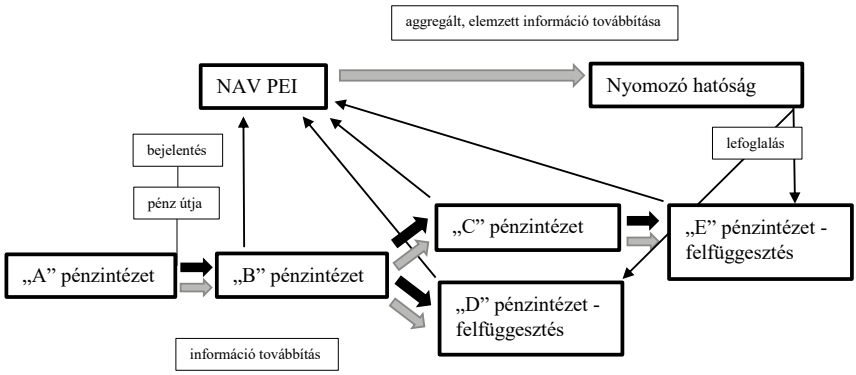
Mindezeket szem előtt tartva alakult ki az objektív bejelentés szabályozási kerete, amely egyaránt képes megfelelő hatósági keret- és felelősségi rendszert biztosítani, értelmezhető hatósági erőforrás-ráfordítással működőképessé tehető, kezeli az adatvédelmi, illetve pénzügyi titokkal kapcsolatos aggályokat, egyúttal nem

eredményezi az állami erőszak monopólium szükségtelen áttörését, az állami büntetőjogi igény kiszervezését.

Az objektív bejelentési rendszer sarokpontjai:

– a csalárd tranzakcióval érintett pénzintézetek közötti információmegosztás lehetőségének célhoz kötött biztosítása,
– automatizálható informatikai megoldási lehetőségek,
– a NAV PEI mint a rendszer központi hatósági szereplője egyaránt biztosítja a hatósági döntést, az összetartozó adatok integrálását és elemzését, miközben nem terheli a nyomozó hatóság eljárását kötő officialitás és más alaki kötelezettség[17],
– a pénzügyi szektor ideiglenes visszatartási – tranzakció felfüggesztési – képességgel rendelkezik,
– a vagyon biztosítására és a sértett részére történő visszajuttatására már a büntetőeljárás keretei között kerül sor.

3. ábra
Az objektív bejelentési rendszer sematikus ábrázolása



Forrás: saját szerkesztés

17 A Be. rendelkezései alapján a büntetőeljárás során eljáró hatóságoknak kötelezettsége a büntetőeljárás megindítása és az eljárás lefolytatása, ha annak törvényi feltételei fennállnak (officialitás), ugyanakkor a büntetőeljárás megindítása, az egyes eljárási cselekmények végrehajtása csak a törvényi feltételek fennállása esetén lehetséges. Így például a feljelentés alapján dönteni kell a nyomozás elrendeléséről, vizsgálni kell, hogy a kényszerintézkedés feltételei fennállnak-e, vagy ahhoz további adatok beszerzése szükséges, stb.

A jogintézmény lényegében a Pmt. bejelentési kötelezettségének jogi kereteit, jogalapját és eszközrendszerét használja fel és integrálja a büntetőeljárási eszköz és intézményrendszerrel. A szubjektív bejelentéshez képest azonban a Pmt. határozza meg azokat az a körülményeket, amelyek esetében a pénzintézet további mérlegelés nélkül köteles intézkedni (visszaéléssel érintett ügylet). További különbség, hogy ebben az esetben a pénzintézet nem csupán a NAV PEI-hez tesz bejelentést, hanem jogosult a tranzakcióval érintett másik pénzintézet(ek) tájékoztatására is. Sőt, az online banking szolgáltatások gyorsaságához igazodva a pénzintézet előbb továbbíthatja a csalárd tranzakcióra vonatkozó információt, és a bejelentési kötelezettség csak a címzett pénzintézet oldalán – utólagosan – merül fel.

A szabályozás alapvetése, hogy a törvény a bejelentés alapjául szolgáló körülmények esetében intézkedési kötelezettséget ír elő. Ez az intézkedési kötelezettség a NAV PEI oldalán is fennáll, így a csalárd tranzakcióval érintett pénzintézet megkeresése/tájékoztatása a számára is kötelezettség lenne. A szabályozás ezt törvényi kötelezettségen alapuló, ugyanakkor szükségtelen oda-vissza információáramlást „rövidíti le" azzal, hogy a két pénzinézet között közvetlen lehet az információtovábbítás, egyúttal a bejelentés, tehát a hatóság bevonása is megtörténik.

A közvetlenség és a fordított ügyintézési sorrend kényszerítő indoka egyértelműen az, hogy más módon az online banki ügyletek utánkövetése, az érdemi beavatkozási képesség lehetősége nem lenne megoldható. Az új eszköz így szükséges és arányos az elérni kívánt célhoz képest.

Amennyiben a tranzakciós láncban további pénzintézetek érintettek, a pénzügyi információ továbbítási és bejelentési kötelezettség az előbbiek szerint alakul. Ha tehát a tranzakció eredményeképpen a „B" pénzintézethez beérkezett pénzeszköz továbbutalására került sor, úgy a „B" pénzintézet a szükséges információt haladéktalanul továbbítja a „C" pénzintézet részére, ahol az információ beérkezésével újabb bejelentési kötelezettség is keletkezik. Az informatikai csatornán továbbítható és automatizálható információ továbbítási folyamat eredményeképpen a turpis tranzakcióra vonatkozó információ képes lehet „utolérni" a szintén informatikai csatornákon végrehajtott és szintén nagyban automatizálható csalárd pénzügyi tranzakciókat.

A jogintézmény működésének eredményeképpen, ha a tranzakciós lánc végén lévő pénzintézetnél a pénzeszköz rendelkezésre áll, az azzal kapcsolatos további rendelkezés (újabb tranzakció) felfüggeszthető, a vagyon biztosítható, ami szintén a Pmt. 34-35. §-a szerint szabályozott, már létező jogintézmény. A felfüggesztésre vagy a pénzintézet által, az ezzel kapcsolatos bejelentés mellett, vagy a NAV PEI rendelkezése alapján kerülhet sor. A felfüggesztés határideje négy munkanap, amely legfeljebb további három munkanappal hosszabbítható.

A tranzakciós láncolatot a NAV PEI a pénzintézetek bejelentése alapján összegzi és értékeli. Amennyiben a bejelentések alapján csalárd ügylet nem azonosítható, úgy a felfüggesztés elmarad vagy azt haladéktalanul feloldják. A NAV PEI a kiértékelt és a saját értékelő, elemző tevékenysége (Pmt. 39. §-a szerinti operatív elemzés) eredményeképpen adott esetben kiegészített információkat a Pmt. 48-49. §-a alapján már érdemben feldolgozva, aggregált formában továbbítja a hatóságok részére. A NAV PEI kockázatalapú tevékenységet végez, működését nem köti a büntetőeljárásban eljáró szerveket érintő intézkedési kényszer. Ennek megfelelően a NAV PEI számára megfelelő idő áll rendelkezésre, hogy a beérkezett információkat összegezze, elemezze. Amennyiben a beérkezett információk alapján megállapítható, hogy a bejelentés alapjául szolgáló információ téves, a tranzakció nem csalárd, úgy haladéktalanul és szükségtelen adminisztratív terhek nélkül képes intézkedni annak érdekében, hogy a felfüggesztésre ne kerüljön sor vagy a felfüggesztett tranzakciókat végrehajtsák. Ebben az esetben arra nézve sincs hivatali kötelezettsége, hogy az információt a hatóság részére továbbítsa, tehát a büntető igazságszolgáltatás felesleges terhelése is elkerülhető.

A NAV PEI – jelentős mértékben automatizált – értékelő-elemző tevékenysége végezetül nem csupán arra képes, hogy az adott csalárd tranzakciós láncolatra vonatkozó információkat összegezze, hanem adott esetben több összetartozó tranzakciós láncolat közötti összefüggéseket is képes kimutatni. Ezzel a nyomozó hatóság számára biztosítható, hogy az elkövetők/elkövetési módszer szempontjából összetartozó ügyeket eleve egységesen kezeljék, és elkerüljék, hogy az egyes csalárd tranzakciók különálló esetekként szerepeljenek a rendszerben.

A vagyon tényleges biztosítására – elvonására – már a büntetőeljárás keretei között, kényszerintézkedés elrendelésével kerül sor. Az állami kényszermonopólium, amely a magántulajdonhoz való jog érdemi korlátozását eredményezi, szintén megmaradhat a meglévő jogi keretek között, valamennyi már ismert és működőképes döntési és felelősségi kompetenciával, illetve garanciális, jogorvoslati elemmel. A nyomozó hatóság a NAV PEI által továbbított információk feldolgozása alapján vizsgálhatja a nyomozás elrendelésének, valamint – amennyiben pénzügyi tranzakció felfüggesztésére került sor – a vagyon biztosításának (lefoglalás, zár alá vétel) törvényi feltételeit. Az információ továbbítási folyamat, illetve a felfüggesztés Pmt.-ben meghatározott határideje megfelelő időkereteket biztosít arra, hogy a nyomozó hatóság érdemben mérlegelje, indokolt-e a nyomozás elrendelése és a kényszerintézkedés alkalmazása.

A kényszerintézkedések kiszervezésének elkerülése érdekében különösen jelentős körülmény, hogy a vagyon biztosítása után annak a sértettekhez történő visszajuttatása és az eredeti állapot helyreállítása így hatósági feladat- és felelősség maradt. A gyakorlatban ugyanis a legritkább esetben fordul elő, hogy egy lineáris tranzakciós folyamatot sikerül az információ-továbbítással megakasztani. Jel-

lemzőbb, hogy a pénzeszközök több pénzintézet között osztódnak, egyesülnek, illetve keverednek legális tranzakciókkal. Egy összetett, adott esetben számos pénzintézetet érintő tranzakciós láncolat esetén nyilvánvalóan nem várható el az adott tranzakciót felfüggesztő pénzintézettől, hogy felderítse a vagyon eredetét, és döntsön arról, hogy ki vagy kik tekinthetők sértettnek, és milyen mértékben szükséges közöttük a meglévő pénzeszközöket felosztani. Az ehhez szükséges jogi eszközök ugyanakkor a büntetőeljárás keretei között rendelkezésre állnak, ezen kérdések tisztázása a büntetőeljárás „normál" menetrendjébe illeszkedik, ezért az ilyen feladatok ellátása elvárható a büntetőügyekben eljáró hatóságoktól.

Az objektív bejelentési kötelezettség további előnye, hogy az információ-továbbítás mind a pénzintézet, mind a NAV PEI, mind a nyomozó hatóság oldaláról automatizálható. A bejelentett információkat így az informatikai rendszer automatikusan dolgozza fel és továbbítja, hogy az emberi beavatkozást igénylő kérdések a lehető leggyorsabban és a lehető legjobban előkészített módon születhessenek meg.[18]

Az új jogintézmény jelentős mértékben illeszkedik a korábban bemutatott PPP konstrukció működési logikájához és kihívásaihoz. Sikerült megoldani, hogy a pénzügyi szektoron belül észszerű és fontos jogszabályi korlátokat jelentő adatkezelési/információ továbbítási szabályok ne akadályozzák a hatékony működést. Az információ továbbítása célhoz kötött és a törvény által meghatározott céllal arányos maradt. Az állam büntetőjogi hatalmának kiszervezésére sem került sor, a pénzügyi rendszer feladatköre a csalárd tranzakcióhoz kapcsolódó vagyon átmeneti biztosítása, legfeljebb csupán annyi időre, hogy a büntetőeljárásban szükséges döntéseket érdemben meg tudják hozni. Az információ továbbítása és a tranzakció felfüggesztése hatósági „kontroll" alatt áll, a NAV PEI részéről biztosított a beavatkozási lehetőség, amennyiben szükséges. Ez alkalmas arra, hogy megfelelő ellenőrzést, felügyeletet gyakoroljon az esetleges visszaélések vagy téves intézkedések felett, amely a beavatkozások tárgyának és időbeli korlátainak figyelembevételével elégséges és hatékony garanciát, korrekciós mechanizmust nyújt. A vagyon érdemi korlátozását jelentő büntetőjogi kényszerintézkedések esetében pedig már biztosított a teljes körű jogorvoslati rendszer. A folyamat egészében az egyes civil és hatósági aktorok felelősségi szabályai egyértelműek, ami igazodik a szervezeti jellegükhöz.

Végezetül az új szabályozás a feladatmegosztás területén is érdemi előrelépést jelentett. A pénzintézetek együttműködésével biztosítható a vagyon megőrzése és a

18 A bejelentéseket a NAV PEI automatizált informatikai rendszere fogadja és dolgozza fel. A NAV PEI által szintén automatizált módon továbbított információt az ORFK Dante rendszere (Digitális Adatelemző és Nyomozástámogató Rendszer) fogadja és dolgozza fel. (https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/helyi-hirek/dante).

csalárd tranzakciós folyamat láthatóvá tétele. Az adott turpis tranzakcióhoz kapcsolódóan a pénzintézetek között megosztott információk emellett az egyes pénzintézetek monitoring rendszerének továbbfejlesztéséhez, tanulásához is hozzájárulhatnak, ezáltal segítve az újabb csalárd tranzakciók kiszűrését, a monitoring rendszer hatékonyságának növelését. A jogintézmény képes továbbá arra is, hogy a bűnüldözési szempontból összetartozó tranzakciós láncokat összekapcsolja. Ez azonban már nem a pénzintézetek, hanem a hatóságok, első sorban a NAV PEI feladata. A folyamat végén a bűnügyi szervek a vagyon biztosításával és a rendelkezésükre bocsátott strukturált információ feldolgozásával kezdhetik meg az elkövetők felkutatását, felelősségre vonását. A nyomozó hatóság tehát mentesülhet attól, hogy a sértetti bejelentések alapján maga próbáljon meg a hagyományos büntetőjogi eszközökkel egy-egy csalárd tranzakció nyomába eredni, ezt a feladatot az objektív bejelentési rendszer útján a pénzügyi szervek végzik el (ráadásul lényegesen nagyobb hatékonysággal). A pénzügyi szektor ezáltal a bűnüldözési folyamatok aktív szereplőjévé vált, míg a nyomozó hatóság terheinek mérséklődése lehetővé teszi az elkövetők felelősségre vonását és a szervezők tevékenységének eredményes felderítését.

Az új jogintézmény működése nyilvánvalóan nem tökéletes és a működés tapasztalatai alapján mindig lesz lehetőség a fejlődésre. Ennek ellenére úgy véljük, a jogintézmény működőképességét jelzi, hogy az ORFK tájékoztatása szerint a bevezetése óta, 2025. június 10-ig eltelt 11 hónap alatt több mint 2 milliárd forintnyi bankszámlapénz biztosítására került sor, mely pénzeszközök ezáltal rövid úton visszajuttathatók a sértettekhez.

6.4. Információmegosztás

Az objektív bejelentési rendszer egy adott, már végrehajtott tranzakciós folyamathoz kapcsolódóan biztosítja az információ hatékony megosztását és a beavatkozási lehetőséget a pénzügyi szektor, a NAV PEI és a bűnüldöző szervek számára. A KVR-hez hasonlóan, ebben a rendszerben a pénzintézet által előzetesen kiszűrt, a belső monitoring rendszerben megakasztott tranzakciókkal kapcsolatos információ, illetve tudás azonban továbbra sem tud szélesebb körben érvényesülni. Az adatkezelési és pénzügyi titokra vonatkozó szabályok azt nem teszik lehetővé, hogy az egyes pénzintézetek az általuk kockázatosnak tartott adatokat egymással közvetlenül megosszák. Jóllehet ez a megoldás kézzelfoghatónak tűnhet, ez valójában egyes ügyfeleknek a pénzügyi rendszerből történő teljes kizárását eredményezné („blacklisting"), amely már az állami feladatok körébe tartozó szabályozási, garanciális, felelősségi és alapjogi kérdéseket vetne fel.

A jogosan felmerülő jogállami kifogások ellenére az információmegosztás iránti igény valós szakmai indokok mentén alakult ki, hiszen a leghatékonyabb megelőzési módszer éppen az lenne, ha már az egy pénzintézet által egyértelműen beazonosított kockázat, lényegében azonnal az egész pénzügyi szektor immunválaszát képes lenne kiváltani. Az online csalások – egyik – jellegzetessége éppen az, hogy az informatikai megoldásokkal tömegjelenséget generálnak, vagyis tömegesen próbálják meg ugyanazt az elkövetési módszert hasznosítani. Amennyiben az első sikeresen azonosított turpis kezdeményezést vagy megvalósított tranzakciót követően minden további, ugyanazt a megoldást (technikai eszközt, „money-mule számlát", célszámlát, stb.) alkalmazó próbálkozást blokkolni lehetne, éppen az online csalások tömeges jellegzetességétől lehetne megfosztani az elkövetőket. A bűnmegelőzés ilyen mértékű sikere akár a cselekmény „megtérülését" is képes lehet olyan mértékben lerontani, hogy azt követően az újabb csalárd jogügyletekhez szükséges erőforrás ráfordítás már nem állna arányban a várható haszonnal. Ez akár az online csalások jelenségének természetes zsugorodását, elhalását is eredményezhetné. A pénzügyi szektor egészét érintő hatékony és megbízható immunválasz kidolgozása ezért jelentős eredményekkel kecsegtet.

E szakmai igény megvalósítását célozta a 2025 tavaszán elfogadott, az igazságügyi tárgyú törvények módosításáról szóló 2025. évi XLIX. törvény. A szabályozás ebben az esetben is a Pmt. módosításával kíván megoldást nyújtani a problémára. A Pmt. szabályozási rendszere ugyanis már jelenleg is felhatalmazást ad arra, hogy a pénzintézetek a gyanúsnak talált tranzakciókról a NAV PEI felé bejelentést tegyenek. Abban az esetben azonban, ha a pénzintézet a saját rendszerében – üzletszabályzata alapján – kezelni tudja a csalárd tranzakció meghiúsítását, a bejelentéssel járó adminisztratív kötelezettségek viselése nem feltétlenül áll a pénzintézet érdekében. Az ilyen információnak a NAV PEI felé történő bejelentését már nem szervezeti érdek, legfeljebb a bejelentés elmulasztása miatti felügyeleti szankció elkerülése motiválja. A szervezeti érdek hiánya abból fakad, hogy ha a konkrét tranzakciót a pénzintézetnek saját hatáskörben már sikerült megakasztania, a bejelentés csupán további adminisztratív teherrel jár, miközben a bejelentés további hatósági hasznosulása számára érdektelen és bizonytalan. Ezzel szemben, ha a pénzintézetek konkrét ismeretekkel rendelkeznének arról, hogy az általuk továbbított információ közvetlenül hasznosul az egész pénzügyi szektorban, úgy minden pénzintézet érdekeltté válhat az információ továbbításában, hiszen egyrészt joggal számíthat arra, hogy a más pénzintézetek által megosztott adat legközelebb az ő megelőzését, monitoring tevékenységét fogja támogatni, másrész joggal tarthat attól, hogy szakmai elmarasztalásban részesül, ha kiderül, hogy egy megosztható – és így más intézeteket segítő – információt mulasztott el továbbítani.

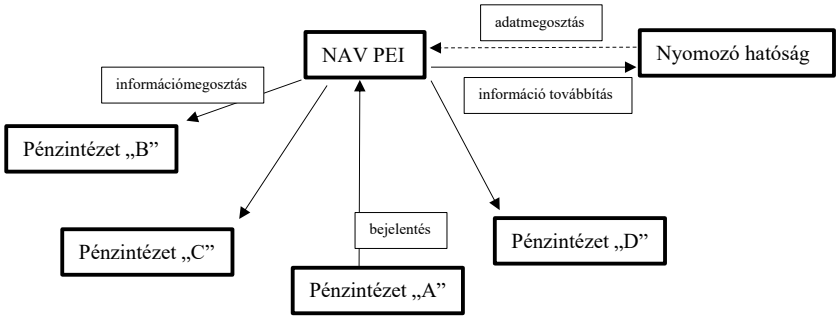
Az új szabályozás egyértelművé teszi, hogy a bejelentés alapjául szolgáló információkat a NAV PEI – megfelelő értékelést követően – lényegében azonnal visszajuttathatja a pénzügyi szektor irányába, biztosítva ezzel, hogy a pénzintézeti bejelentés szektorszintű hatás közvetlen kiváltására lesz alkalmas. A szabályozás ezen eleme nóvum. Ameddig ugyanis a pénzügyi szolgáltatók részéről a NAV PEI-hez nyújtott strukturált információáramlás eddig is az intézményrendszer részét képezte, a NAV PEI-nek általános „információ-visszafordítási" lehetősége nem volt. A bejelentések alapján volt ugyan lehetőség egyes konkrét pénzintézetek megkeresésére, beavatkozására, ugyanakkor általános jellegű, az egész szektort mozgósító információmegosztásra nem.

Az általános információmegosztás elméleti síkon felfogható a jelenlegi rendszer mennyiségi változásaként. A NAV PEI-nek lehetősége van az általa rendelkezésre álló információ elemzése alapján egyes szolgáltatók megkeresésére, illetve a szolgáltatótól kapott információ alapján bizonyos tranzakciók felfüggesztésére. Tegyük fel, hogy ezen felhatalmazás alapján a NAV PEI nagyon rövid időintervallumon belül ismétlődve (néhány másodpercenként) megkereséseket küld az általa gyanúsnak értékelt adatok ellenőrzése végett, majd a szolgáltatók pozitív találata esetén, automatikusan megteszi a szükséges intézkedést, hogy a beazonosított tranzakció felfüggesztésre kerüljön. Egy ilyen rendkívül erőforrásigényes elméleti megoldás az eredményét tekintve egyenértékűnek tekinthető az információ általános megosztásával. E megoldás a pénzügyi szolgáltatók és a NAV PEI rendszerének túlterheléses támadását jelentené, egyúttal a szabályozás szerinti eredeti jogintézmény nyilvánvaló kijátszásának is minősülne. A mennyiségi módosítás már minőségi eltérésként lenne értékelhető, hiszen célját, hatását és működését tekintve is alapvető különbség van egy adott információt érintő célzott megkeresés, és egy általános, lényegében folyamatosan fennálló riasztási rendszer között, amely a szolgáltatók állandó rendelkezésre állását is megkövetelné. Ennek megfelelően garanciális jelentőségű, hogy az új jogintézmény nem a hatályos szabályozás kijátszása útján jött létre, hanem önálló törvényi meghatározást és szabályozási keretet kapott.

A szabályozás központi eleme, hogy az információ megosztására a NAV PEI kapott törvényi felhatalmazást, ahogy az is, hogy a megosztott információ felhasználhatósága időben korlátozott. A NAV PEI állami feladatot ellátó, elemző kapacitással és a céljának eléréséhez szükséges hatósági jogkörökkel rendelkező szerv. A pénzügyi szolgáltató a bejelentésben megosztott információt a NAV PEI a saját adatbázisában megfelelő ellenőrzésnek (operatív és stratégiai elemzésnek) veti alá, és így az információ pénzügyi szektorral történő megosztására már hatósági aktusként, a törvényi feltételeknek megfelelően kerülhet sor. Az egyes aktorok felelőssége elkülöníthető: a pénzügyi szolgáltató az általa tapasztaltakat, monitoring tevékenységének eredményét jelenti be a NAV PEI felé. E lépésben

a bejelentés alapjául szolgáló tények valóságtartalmáért felel. A NAV PEI a bejelentés tartalmát elemzi, saját adatbázisával összevetve értékeli, és akkor osztja meg, ha a törvényi (a megosztással elérni kíván cél) feltételek fennállnak, és az információmegosztás ezen célok eléréséhez szükséges. A NAV PEI hatósági felelőssége, hogy a bejelentés alapját képező információ megosztásának az információval érintett tranzakciókra milyen (érdemben blokkoló) hatása lesz. Az információ megosztását követően a NAV PEI további feladata annak eldöntése, hogy az információt mikor és milyen egyéb információkkal és elemzéssel együtt továbbítja a nyomozó hatóságok részére.

4. ábra
Az információmegosztás (első körének) sematikus modellje:



Forrás: saját szerkesztés

A pénzügyi szolgáltatók a NAV PEI által megosztott információhoz olyan formában férnek hozzá, amely lehetővé teszi az információ automatikusan feldolgozását, így az lényegében valós időben képes beépülni a saját monitoring rendszerükbe. Az információmegosztással kapcsolatos riasztási jelzések pedig korábbi tranzakciókhoz kapcsolódó, vagy az információ beérkezését követően kezdeményezett újabb tranzakciókhoz kapcsolódó bejelentési kötelezettséget, illetve tranzakció-felfüggesztést vonhatnak maguk után. Ezáltal az egyes pénzügyi szolgáltatók monitoring tevékenységének eredménye rövid időn belül az egész pénzügyi szektorban hasznosulhat, illetve újabb, a csalárd tevékenységhez kapcsolódó információk azonosításához, megosztásához vezethet. A megosztott információ egyúttal a büntetőeljárásokban is felhasználható és segítheti az elkövetői körhöz tartozó cselekmények azonosítását, az elkövetők felderítését, miközben a káros eredmények bekövetkezését a pénzügyi szektor folyamatosan képes elhárítani.

Az információmegosztás rendszerének logikája tökéletesen illeszkedik a PPP konstrukció lényegéhez. A pénzügyi szektor erőforrásai összeadódnak és képesek

hatékonyan fellépni a bűncselekmények megelőzése érdekében, miközben jelentős mértékben tehermentesítik a büntető igazságszolgáltatást. Emellett a bűnüldözés számára az összetartozó próbálkozások információi aggregáltan és feldolgozható struktúrában állnak rendelkezésre, lehetővé téve a próbálkozások mögött álló infrastruktúra felszámolását, az elkövetők felderítését és felelősségre vonását.

A hatékony működés feltétele a rendszer megfelelően automatizált, informatikai rendszer útján történő működtetése, hiszen a bemutatott információáramlási modell emberi feldolgozással időszerűen nem működtethető. Az objektív rendszer működtetése során kialakított informatikai megoldások bizakodásra adnak okot, hogy a jogintézmény 2026. június 1-ei hatálybalépésére ezen rendszer működéséhez szükséges informatikai megoldások is kidolgozásra kerülnek.

A rendszer működésének logikájához hozzátartozik, hogy akkor működik eredményesen, ha a pénzügyi szolgáltatók a monitoring tevékenységüket hatékonyan, megfelelő erőforrások biztosításával végzik. Korábban már érintettük, hogy a szolgáltatók nemcsak a törvényi kötelezettségük miatt, hanem azért is érdekeltek lesznek az információmegosztásban, mert számíthatnak arra, hogy ők maguk is részesülhetnek a többi szolgáltató által megosztott adatok előnyeiből, vagyis önkéntes egyetértés alakulhat ki a rendszer közös működtetésében való érdekeltségükre nézve. Egyes szolgáltatók ugyanakkor indokolatlan és visszaélésszerű előnyre tehetnek szert, ha a saját monitoring tevékenységüket hanyagolva, csupán a más szolgáltatók információmegosztásának haszonélvezőiként kívánnak érvényesülni. Ezzel elérhető a monitoring tevékenységük költségeinek minimalizálása, miközben más szolgáltatók erőforrás-ráfordításának eredményét maximális eredményességgel, szabadon hasznosíthatják. Amellett, hogy ez nyilvánvaló visszaélés a rendszer alapját képező kölcsönös bizalommal, felelősséggel, észszerűséggel szemben, ezért erkölcsileg is mélységesen elítélendő, nyilvánvalóan a kormányzati felelősség körébe tartozik egy olyan szabályozási és felügyeleti környezet kialakítása, amely képes biztosítani, hogy minden pénzügyi szolgáltató megfelelő erőforrás biztosítására, illetve közreműködésre legyen köteles, és a rendszer működésének eredményeit csak akkor hasznosíthassa, ha a rá háruló feladatot megfelelően teljesíti.

7. ÖSSZEGZÉS

Az online csalások elmúlt évek során bekövetkezett változásai (társadalmi, informatikai, stb.) alapján kijelenthető, hogy a bűncselekmények, a bűnözés egy új jelenségével állunk szemben. Hiú elképzelés azt feltételezni, hogy létezik olyan megoldás, amely képes teljes mértékben kizárni a jelenség működését. Feltehetőleg erre akkor kerülhetne sor, ha a jelenség kialakulását lehetővé tevő előfel-

tételeket szüntetnénk meg, amivel ugyanakkor a jelenlegi pénzügyi megoldások lényegében minden előnyéről, kényelmi és gazdaságilag hasznos funkciójáról le kellene mondanunk. Az online csalások mértéke ugyanakkor még mindig csak ezrelékekben mérhető az összes pénzügyi tranzakció volumenéhez, értékéhez viszonyítva[19], így egy ilyen jellegű visszalépés a gazdaság versenyképessége és a jelenlegi megoldások népszerűsége miatt nyilván nem lenne támogatható. Az online csalások elleni küzdelem egésze jó eséllyel nem nyerhető, ami azonban nem jelenti azt, hogy csaták ne lennének nyerhetők, eredmények ne lennének elérhetők. Az online csalások új jelensége azonban új módszereket, új együttműködési formákat igényel és ebben kiemelt szerepet indokolt biztosítani a pénzügyi szektor erőforrásait hatékonyan hasznosítani képes PPP együttműködésnek.

A most bemutatott szakmai és kormányzati kezdeményezések időszerűen észlelték, hogy az erőforrások összehangolására, a feladatok hatékony megosztására van szükség. Az ismertetett új együttműködési formák, jogintézmények meggyőződésünk szerint megfelelő irányba tett lépések, ígéretes kezdeményezések, amelyek alapjai lehetnek a pénzügyi szektor és a bűnüldöző hatóságok hatékony együttműködésének, az egyes jogintézmények továbbfejlesztésének, valamint az újabb és újabb kihívásokra reagálni képes megoldásoknak. Ehhez azonban elengedhetetlen a megindult folyamatok tapasztalatainak folyamatos figyelemmel kísérése, értékelése. A kialakult együttműködési formák pedig (KiberPajzs, kormányzati munkacsoport) megfelelő terei lehetnek ennek a munkának.

19 https://www.mnb.hu/letoltes/bartha-lajos-prezi-kiberpajzs-sajtotajekoztato-03-20.pdf; https://fintechzone.hu/a-kozponti-visszaelesszuro-rendszer-megvedheti-a-penzforgalmat-a-kibertamadasoktol/.

HIVATKOZÁSOK

Vogel, B. – Costa, E. – Lassalle, M. (eds., 2024): Law of Pubic-Private Cooperation against Financial Crime – Developing Information Sharing to Counter Money Laundering and Terrorism Financing; *Intersentia Ltd.* 2024. https://www.larcier-intersentia.com/en/law-public-private-cooperation-financial-crime-9781839704666.html.

Bagó, P. (2023): A kiberbiztonság és a mesterséges intelligencia kapcsolata. https://bankszovetseg.hu/Public/gep/2023/196-221%20Bago.pdf. (letöltve: 2025.07.12.).

Bibó, I. (1986): Válogatott tanulmányok 1935-1944. *Magvető Könyvkiadó* 1986.

Biró, G. – Kiss, M. (2024): Adathalászat és az ellene történő egyes védekezési lehetőségek. https://bankszovetseg.hu/Public/gep/2024/G%C3%89P/417-440%20BiroKiss.pdf. (letöltve: 2025.07.12.).

Barabás, A. T. (ed. 2023): Kriminológia MA. Budapest: *Akadémiai Kiadó – Ludovika Egyetemi Kiadó*. https://mersz.hu/barabas-kriminologia-ma/. (letöltve: 2025.07.12.).

EUCPN (2023): A köz- és magánszféra közötti partnerségek a bűnmegelőzésben: kihívások és ajánlások. https://eucpn.org/sites/default/files/document/files/Public%20private%20partnerships_Hungarian.pdf. (letöltve: 2025.07.12.).

Frész, F. (2025): Az online csalások mögött álló bűnözői csoportok és kötődéseik. https://www.cyberthreat.report/p/az-online-csalasok-mogott-allo-bunozoi. (letöltve: 2025. 07.12.).

Kovács, L. – Terták, E. (2024): A kiberbűnözés legjobb ellenszere a pénzügyi műveltség. https://bankszovetseg.hu/Public/gep/006-029%20Kovacs_Tertak.pdf. (letöltve: 2025.07.12.).

Nagy, R. (2018): A kibertérben elkövetett vagyon elleni bűncselekmények nyomozásának egyes kérdései. https://real.mtak.hu/120711/1/3850-Cikk%20sz%C3%B6vege-17536-1-10-20200721.pdf. (letöltve: 2025.07.12.).

Nyeste, P. – Szendrei, F. (2020): A bűnügyi hírszerzés kézikönyve. (https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/A%20bu%CC%8Bnu%CC%88gyi%20hi%CC%81rszerze%CC%81s%20ke%CC%81ziko%CC%88nyve.pdf. (letöltve: 2025.07.12.).

Nyeste, P. (2016): A bűnüldözési célú titkos információgyűjtés története, rendszerspecifikus sajátosságai, szektorális elvei. PhD. értekezés. https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/12375/Teljes%20sz%c3%b6veg%21.pdf?sequence=13&isAllowed=y. (letöltve: 2025.07.12.).

Schenk, T. (2018): Digitális forradalom a bankszektorban. https://bankszovetseg.hu/Public/gep/2018/imp%20100-112ig%20Schenk%20Tamasuj.pdf. (letöltve: 2025.07.12.).

Terták, E. – Kovács, L. (2023): Fókuszban a pénzügyi biztonság kibertérben is – Pénz7. https://bankszovetseg.hu/Public/gep/2023/005-020%20Tertak%20Kovacs.pdf. (letöltve: 2025.07.12.).

Vass, P. – Kovács, L. (2019): A pénzügyi szektor szabályozásának aktuális kihívásai az európai unióban (2019–2024). https://www.bankszovetseg.hu/Public/gep/2019/413-430%20Kovacs%20Vass.pdf. (letöltve: 2025.07.12.).