Magyar Rendészet 2026/3. 21–30.
DOI: 10.32577/mr.2026.3.2

BÜNTETŐJOG

Egy jelentéktelennek tűnő jogeset tanulságai

Az informatikai rendszer felhasználásával elkövetett csalás tényállásának kritikája

Lessons Learned from a Seemingly Insignificant Legal Case

A Critique of the Information System Fraud

GÁSPÁR Zsolt[1]

Bevezetés: Az információs rendszer felhasználásával elkövetett csalás tényállásának jelentősége a magyar büntetőjogban a digitalizáció előrehaladásával párhuzamosan fokozatosan megnövekedett. Nem tisztázott azonban, hogy a csekély elkövetési értékű, marginális társadalomra veszélyességű esetekben indokolt-e a bűncselekményi szintű kriminalizáció fenntartása, összhangban áll-e ez a büntetőjog *ultima ratio* jellegével.

Célkitűzések: A tanulmány célja annak vizsgálata, hogy az információs rendszer felhasználásával elkövetett csalás hatályos szabályozása arányos-e csekély elkövetési értékű, kisebb jelentőségű ügyekben vagy indokolt lenne a szabálysértési alakzat bevezetése.

Módszertan: A kutatás módszertani alapját egy konkrét – a közvélemény által bagatell jelentőségűnek bélyegezhető – jogeset dogmatikai és normatív elemzése képezi. A vizsgálat során az anyagi büntetőjogi (Btk.) és szabálysértési jogi szabályozás (Szabs. tv.) áttekintését a konkrét jogeset elemzése követi. A tanulmány kiterjed az értékhatárok, a minősített esetek, valamint a büntetési tételek összevetésére, továbbá figyelembe veszi 2001. évi budapesti egyezmény releváns rendelkezéseit.

Eredmények: A tanulmány arra helyezi a hangsúlyt, hogy a vizsgált jogesetben – ahol az okozott kár elenyésző mértékű volt – a cselekmény

[1] PhD, egyetemi adjunktus, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Büntető-eljárásjogi Tanszék, e-mail: gaspar.zsolt@uni-nke.hu

kizárólag az elkövetési mód miatt minősül bűntettnek, miközben az azonos vagy magasabb értékre, „hagyományos" módon elkövetett cselekményeket szabálysértésként bírálják el. Megállapítható, hogy a jelenlegi szabályozás nem biztosítja a differenciálást az elkövetési magatartás társadalomra veszélyessége, az elkövető tudattartalma és informatikai jártassága alapján. Rögzíthető továbbá, hogy az elemzés tárgyát képező esetben az eljárási költségek aránytalanul meghaladhatják az okozott kár mértékét. Az is kimutatható, hogy az egyes áruházi technikai védelmi rendszerek (kiléptető kapuk) elterjedése ténylegesen olyan helyzetet teremt, amelyben a „klasszikus" lopás helyett az információs rendszer működésének befolyásolása válik az egyetlen reális elkövetési alakzattá. A tanulmány felveti továbbá a budapesti egyezmény revíziójának szükségességét.

Konklúzió: A kutatás elsődleges tanulsága, hogy az információs rendszer felhasználásával elkövetett csalás jelenlegi, differenciálatlan szabályozása csekély elkövetési értékű esetekben sértheti a büntetőjog *ultima ratio* jellegét és az arányosság követelményét. További fontos megállapítás, hogy az elkövetési mód technikai jellege önmagában nem indokolja a bűncselekményi szintű szankcionálást, ha a társadalomra veszélyesség elenyésző mértékű. A jövőbeni jogalkotási és kriminálpolitikai kutatások számára indokolt lehet egy értékhatárhoz kötött szabálysértési alakzat bevezetésének, illetve a budapesti egyezmény arányossági szempontú felülvizsgálatának megfontolása.

Kulcsszavak: büntetőjog, jogeset, információs rendszer felhasználásával elkövetett csalás

Introduction: The significance of the frauds committed using the information system in the Hungarian criminal law has gradually increased in parallel with the progress of digitalisation. However, it is not clear whether it is justified to maintain criminalisation at the criminal level in cases of low value and marginal danger to society, and whether this is in line with the 'ultima ratio' nature of criminal law.

Aims: The aim of the study is to examine whether the current regulation of fraud committed using the information system is proportionate in cases of low value and minor importance, or whether the introduction of the misdemeanour structure would be justified.

Methodology: The methodological basis of the research is the dogmatic and normative analysis of a specific legal case – which can be labelled as trivial by the public opinion. During the study, an overview of the substantive criminal law and misdemeanour law is followed by an analysis of the specific legal case. The study covers the comparison of thresholds, qualified cases and penalty items, and also takes into account the relevant provisions of the Budapest Convention on Cybercrime.

Results: The study emphasises that in the examined legal case – where the damage caused was negligible – the act is classified as a severe crime

solely due to the manner of commission, while acts committed in a 'traditional' manner for the same or higher value are assessed as a misdemeanour. It can be stated that the current regulation does not ensure differentiation based on the social danger of the committing behaviour, the perpetrator's level of consciousness and IT skills. It can also be noted that in the case under analysis, the procedural costs may disproportionately exceed the extent of the damage caused. It can also be shown that the spread of certain technical security systems (exit gates) in stores actually creates a situation in which, instead of 'classic' theft, influencing the operation of the information system becomes the only realistic form of offense. The study also raises the need for a revision of the Budapest Convention.

Conclusion: The primary lesson of the research is that the current, undifferentiated regulation of fraud committed using the information system may violate the ultima ratio nature of criminal law and the requirement of proportionality in cases of low value of the offense. Another important finding is that the technical nature of the method of commission does not in itself justify criminal-level sanctions if the danger to society is negligible. Future legislative and criminal policy research may be justified in considering the introduction of a threshold-based offense form and the revision of the Budapest Convention from a proportionality perspective.

Keywords: criminal law, case law, information system fraud

A jogeset bemutatása

A gyanúsítás szövege – és a gyanúsított teljes körű beismerő vallomása – alapján a cselekmény az alábbiak szerint zajlott. A fiatalkorú (az elkövetéskor 14 éves) gyanúsított barátaival megjelent az egyik áruházban, ahol eltulajdonítottak két darab sajtos krémrudat, 2 darab almás-fahéjas fánkot, valamint két darab virslis rudat akként, hogy a fenti árucikkek helyett az önkiszolgáló kasszánál hat darab zsemlét ütöttek be, és annak az árát fizették meg. A cselekmény végül tettenéréssel zárult, mivel a szolgálatban lévő biztonsági őr felfigyelt a társaságra. Az okozott kár a nyomozó hatóság megállapítása szerint mindösszesen 1463 forint volt. A gyanúsított az eljárás során egyébként a nyomozó hatósággal végig együttműködött, a cselekmény elkövetését beismerte, személyi körülményeit feltárta.

A fenti cselekmény miatt az ügyben az illetékes nyomozó hatóság előtt a gyanúsítottal szemben a Büntető Törvénykönyvről szóló 2012. évi C. törvény (Btk.) 375. § (1) bekezdésébe ütköző információs rendszer felhasználásával elkövetett csalás bűntette miatt indult büntetőeljárás.

Az anyagi jogi háttér

Az információs rendszer felhasználásával elkövetett csalás tényállását a Btk. 375. § (1) bekezdése a következőképpen rögzíti: „Aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő."

A bűncselekmény minősített eseteit a (2)–(4) bekezdések rögzítik, amelyek – a csalás tényállásával egyezően – az okozott kár vonatkozásában értékhatárok szerint rendelnek magasabb büntetési tételt alkalmazni a jogalkotónak:

> „(2) A büntetés egy évtől öt évig terjedő szabadságvesztés, ha
> a) az információs rendszer felhasználásával elkövetett csalás jelentős kárt okoz, vagy
> b) a nagyobb kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.
> (3) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha
> a) az információs rendszer felhasználásával elkövetett csalás különösen nagy kárt okoz, vagy
> b) a jelentős kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.
> (4) A büntetés öt évtől tíz évig terjedő szabadságvesztés, ha
> a) az információs rendszer felhasználásával elkövetett csalás különösen jelentős kárt okoz, vagy
> b) a különösen nagy kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el."

Az információs rendszer felhasználásával elkövetett csalás elkövetési tárgya az információs rendszer, az (5) bekezdés kivételével, amelynél a készpénz-helyettesítő fizetési eszköz.[2] Az információs rendszer fogalmát a Btk. 459. § (1) bekezdésének 15. pontja definiálja: információs rendszer „az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége".

Az elkövetési magatartás kapcsán a BH 2017.8.252 ad iránymutatást, amely megállapítja, hogy az információs rendszer felhasználásával elkövetett csalás megvalósítható adatbevitellel, adat módosításával, annak törlésével vagy hozzáférhetetlenné tételével, továbbá minden más olyan művelet elvégzésével, amely a fentebb definiált információs rendszert befolyásolja, és ezzel kárt okoz. A kár kapcsán szükséges kiemelni, hogy annak az információs rendszer jogtalan befolyásolásából kell erednie, nem pedig a tévedésbe ejtésből vagy tévedésben tartásból, tekintve, hogy ez határolja el a tényállást a csalástól.[3]

---

[2] A készpénz-helyettesítő fizetési eszköz fogalmát a Btk. 459. § (1) bekezdésének 19. pontja határozza meg, a következőképpen: „a hitelintézetekről szóló törvényben meghatározott készpénz-helyettesítő fizetési eszköz és a forgatható utalvány, a kincstári kártya, az utazási csekk, a kifizetőt terhelő adó mellett vagy adómentesen adható, korlátozott körű áruk vagy szolgáltatások ellenértékének kiegyenlítése céljából törvény alapján kibocsátott utalvány és a váltó, feltéve, hogy kivitelezése, kódolása vagy a rajta lévő aláírás folytán a másolás, a meghamisítás vagy a jogosulatlan felhasználás ellen védett."

[3] Ezt rögzíti egyébként a Kúria csalás bűntette tárgyában hozott Bfv.287/2024/7. számú precedensképes határozata is.

A vizsgált jogeset kapcsán – az elkövetési magatartás körében – a bírói gyakorlat vonatkozásában kiemelten fontos a BH 2025.3.57., amely I. pontja rögzíti, hogy

> „az információs rendszer felhasználásával elkövetett csalás bűntettének megállapítására alkalmas, ha az elkövető az önkiszolgáló kassza használata során annak informatikai rendszerébe a nála lévő helyett más árucikkre vonatkozó (vonalkód, illetve mennyiség) – valótlan – adatot visz be, ha azt azzal a – haszonszerzési – céllal teszi, hogy a termékért ne a tényleges, magasabb árat kelljen fizetnie". [4]

Az információs rendszer felhasználásával elkövetett csalás célzatos bűncselekmény, így az csak egyenes szándékkal követhető el.

A fentiekben elemzett tényállással szemben a csalás tényállását a Btk. 373. § rögzíti, amelynek alapesete két évig terjedő szabadságvesztéssel büntetendő vétség abban az esetben, ha a csalás kisebb kárt okoz, vagy a szabálysértési értékhatárt meg nem haladó kárt okozó csalást minősítő körülményekkel (például bűnszövetségben vagy üzletszerűen) követik el. A minősített esetek tekintetében szintén tapasztalható eltérés. Amennyiben a csalás nagyobb kárt okoz, vagy a kisebb kárt okozó csalást minősítő körülményekkel követik el, úgy a büntetés bűntett miatt három évig terjedő szabadságvesztés. A (4)–(6) bekezdésekben az értékhatárok ugyanakkor teljesen megegyeznek az információs rendszer felhasználásával elkövetett csalás minősített eseteivel.

A már taglalt csalás tényállása mellett érdemes kiemelni a Btk. 374. §-a által szabályozott gazdasági csalás tényállását is, amelynek esetében az egyes értékhatárok és büntetési tételek szinte teljesen megegyeznek a csalás tényállásánál tapasztaltakkal azzal a különbséggel, hogy a gazdasági csalás alapesetének elkövetéséhez legalább kisebb vagyoni hátrányt okozva kell elkövetni, a szabálysértési értéket a törvény még minősítő esetek mellett sem rendeli büntetni. Ez az aránytalanság a nyomozási hatékonyság fejlesztését is indokolja, amely a büntető igazságszolgáltatás teljesítményének fenntartható javítását célozza (Vári 2015).

A Btk. rendelkezései mellett érdemes áttekinteni az egyes kriminalizált cselekmények szabálysértési alakzatait is, amelyeket a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi II. törvény (Szabs. tv.) tartalmaz.

A Szabs. tv. 177. §-a rögzíti a tulajdon elleni szabálysértés tényállását:

> „177. § (1) Aki
> a) ötvenezer forintot meg nem haladó értékre lopást, sikkasztást, jogtalan elsajátítást,
> b) ötvenezer forintot meg nem haladó kárt okozva csalást, szándékos rongálást,
> c) ötvenezer forintot meg nem haladó vagyoni hátrányt okozva hűtlen kezelést
> követ el, úgyszintén, aki e cselekmények elkövetését megkísérli, szabálysértést követ el.

[4] Érdemes megjegyezni, hogy a BH által érintett esetben terhelt a bűncselekmény elkövetésével az áruházlánc sértettnek összesen 55 823 forint kárt okozott. Ha részletesen megnézzük a tényállást, az is megállapítható, hogy a jogeset egy folytatólagosan elkövetett bűncselekményt takar, amelynél az egyes alkalmak során pár száz vagy éppen pár ezer forint kár keletkezett.

(1a) Aki lopásból, sikkasztásból, csalásból, hűtlen kezelésből, rablásból, kifosztásból, zsarolásból vagy jogtalan elsajátításból származó dolgot vagyoni haszonszerzés végett ötvenezer forintot meg nem haladó értékben megszerez, elrejt vagy elidegenítésében közreműködik, szabálysértést követ el.
(5) Az (1) és (2) bekezdésben meghatározott szabálysértés miatt szabálysértési eljárásnak csak magánindítványra van helye, ha a sértett az elkövető hozzátartozója.
(6) Az elkövetési érték, kár, illetve okozott vagyoni hátrány összegének megállapítása céljából érték-egybefoglalásnak van helye, ha az eljárás alá vont személy az (1) bekezdés a)–c) pontjában, valamint az (1a) bekezdésben meghatározott ugyanolyan cselekményt több alkalommal, legfeljebb egy éven belül követte el, és ezeket együttesen bírálják el. Nincs helye érték-egybefoglalásnak, ha az üzletszerű elkövetés megállapítható."

Jól megfigyelhető, hogy a jogalkotó a Btk. és a Szabs. tv. megalkotásakor megalapozottan állapította meg a szabálysértési értékhatárokat bizonyos cselekmények (lopás, sikkasztás, jogtalan elsajátítás, csalás, szándékos rongálás, hűtlen kezelés) vonatkozásában ötvenezer forintban. Ennek az egyik legnyilvánvalóbb oka az, hogy ezen cselekmények társadalomra veszélyessége nem éri el a bűncselekmények szintjét. A szabályozás áttekintése felveti azonban a kérdést, hogy miért nincsen szabálysértési alakzata az információs rendszer felhasználásával elkövetett csalásnak.

Az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló egyezményének (az egyezmény kihirdetésére hazánkban a 2004. évi LXXIX. törvénnyel került sor) ratifikálásával hazánk is elköteleződött, hogy bizonyos, az egyezményben meghatározott cselekmények kriminalizálásával elősegíti a tagállamok közötti egység megteremtését. Az elköteleződés részét képezi a Budapesti Egyezmény II. Címének 8. Cikkében rögzített vállalás. Ennek értelmében a tagállamoknak bűncselekményként szükséges minősíteniük és szankcionálniuk a számítógéppel kapcsolatos csalás tényállását, amelyet az egyezmény a következőképpen határoz meg: „a másnak jogosulatlanul és szándékosan történő vagyoni károkozás, amelyet a) számítástechnikai adatok bármilyen bevitelével, megváltoztatásával, törlésével vagy megsemmisítésével, b) a számítástechnikai rendszer működésébe való bármilyen beavatkozással, anyagi haszon saját vagy más részére történő jogosulatlan megszerzésének céljából követnek el" (Budapesti Egyezmény 2. Címének 8. Cikke).

Kritikai észrevételek a jogeset tükrében

A fent bemutatott jogeset kapcsán könnyen belátható, hogy az elkövetővel szemben aránytalan mértékű büntetést kellene kiszabni a hatályos jogszabályok alapján. Véleményem szerint szükséges átgondolni egy ilyen büntetőügy üzenetét a társadalom számára, kifejezett hangsúlyt fektetve mind a generális, mind a speciális prevencióra. Jelen esetben ugyanis több faktort is értékelni kell az elkövető(k) büntetőjogi felelősségre vonása során:

1. Az elkövetővel szemben, amennyiben pusztán zsebre vágta volna az árucikkeket, csak szabálysértési eljárás indult volna tulajdon elleni szabálysértés (lopás) miatt, tekintettel az értékhatárokra. Az okozott kár ugyanis 1463 forint volt.

2. Mivel az áruházból (és már az áruházak többségéből) kizárólag a vásárlást követően kapott nyugtán szereplő vonalkóddal lehet kijönni, így lényegében lopást nehezen lehetne megvalósítani, más módon nem is igazán tudja eltulajdonítani az árucikkeket.
   a) Amennyiben ugyanis az elrejtett árucikkekkel „kikéredzkedik" az áruházból arra hivatkozva, hogy nem vásárolt semmit, úgy álláspontom szerint már csalást követ el, hiszen tévedésbe ejtené a biztonsági őrt vagy más áruházi dolgozót.
   b) Amennyiben viszont a bemutatott jogesetben szereplő módon kívánja eltulajdonítani az árucikkeket, úgy a cselekmény információs rendszer felhasználásával elkövetett csalásnak minősül.
3. Az elkövető képzetében nem feltétlenül egy komplexebb elkövetési mód jelent meg, pusztán alkalmazkodott az áruház védelmi rendszeréhez (jelen esetben a nyugtaolvasóval ellátott kiléptetőrendszerhez).
4. Amennyiben a kár oldaláról közelítjük meg az esetet, úgy megállapítható, hogy az elkövető cselekménye kevesebb kárt okozott, mintha lopást követett volna el, mivel így egy részét lényegében kifizette a termékek vételárának.
5. Jelen esetben, mivel az eljárás során kötelező a védő jelenléte, így már az eljárási költségek (a gyanúsítotti kihallgatáson való részvétel, valamint a bírósági eljárás során a tárgyaláson való részvétel, illetőleg a felkészülési díj összege) is lényegesen meghaladják a kár mértékét.
6. Mivel a fiatalkorú elkövető cselekménye bűncselekménynek minősül, így a fiatalkorúakkal szembeni büntetőeljárás további következményeit is el kell szenvednie a terheltnek, aminek része a jelzés az oktatási intézmény felé, valamint a terhelt vonatkozásában környezettanulmány készítése.

Szabályozási tendenciák az uniós tagállamokban

Lengyelország

A lengyel büntetőjogi kódex[5] az informatikai csalást önálló, a csalástól elkülönült büntetőjogi tényállásként szabályozza. A 287. § 1. bekezdése elkövetési magatartásként rögzíti – az anyagi haszonszerzés vagy károkozás célzatával – a számítógépes adatok automatikus feldolgozásának, összegyűjtésének vagy továbbításának jogosulatlan befolyásolását vagy megváltoztatását, törlését és az erre irányuló adatbevitelt. A jogalkotó büntetési tételként három hónaptól öt évig terjedő szabadságvesztést rendel a tényálláshoz. Szükséges hangsúlyozni azonban, hogy a tényállás 2. bekezdése meghatározza a bűncselekmény privilegizált esetét azzal, hogy kisebb tárgyi súlyú esetekben szankcióként a pénzbüntetést, az elzárást és a legfeljebb egy évig terjedő szabadságvesztést határozza meg.

[5] USTAWA z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. 1997 Nr 88 poz. 553).

Spanyolország

A spanyol büntetőjog rendszerében a csalás tényállását a spanyol Büntető Törvénykönyv[6] IV. fejezete 1. alcímének 248. §-a, míg az informatikai csalás tényállást pedig a 249. § *a)* pontja tartalmazza.

Az informatikai csalás elkövetési módja körében a törvény – haszonszerzés céljából – az információs rendszer működésének akadályozásával vagy indokolatlan megzavarásával, számítógépes adatok nem megfelelő bevitelével, megváltoztatásával, törlésével, továbbításával vagy letiltásával, illetve bármilyen más számítógépes manipuláció vagy hasonló cselekmény alkalmazásával történő elkövetést kriminalizálja. Az informatikai csalás fenti alakzatára a „klasszikus", egyébként a 248. §-ban rögzített csalással azonos, hat hónaptól három évig terjedő szabadságvesztés büntetés kiszabását rendeli a jogalkotó.

A 248. § meghatározza a csalás egy privilegizált esetét is, amennyiben ugyanis a csalással okozott kár nem haladja meg a 400 euró összeget, úgy szankcióként egytől három havi pénzbírság kiszabása között mozoghat a jogalkalmazó. Ezen rendelkezés ugyanakkor nem alkalmazható az informatikai csalás vonatkozásában a hatályos jogszabály tükrében (Ávila Martínez 2024).

Megjegyzendő, hogy a szabályozás csak 2023 óta alakul a fentiek szerint, ekkor lépett ugyanis hatályba az a 2022-es Btk.-módosítás, amely teljesen átrendezte a 248–249. § törvényszövegét.[7]

Ezt megelőzően a 248. § rögzítette a csalás tényállását. Az informatikai csalás nem kapott külön tényállást ezt megelőzően sem, hanem a 248. § 1. bekezdésének *a)* pontja tartalmazta azt, mint a csalás egy bizonyos elkövetési fordulatát. A 249. § ezzel szemben rögzítette a csalás privilegizált esetét, amelyet a hatályos szabályozással egyezően 400 euró összegben állapított meg a jogalkotó. Rögzíteni szükséges ugyanakkor, hogy a törvénymódosítás 2023-as hatálybalépéséig a jogalkalmazó hatóságok a 249. § adta keretek között tudták elbírálni a kisebb értékre elkövetett informatikai csalást is. Álláspontom szerint ezen korábbi szabályozás megfelelően biztosította a fokozatosságra vonatkozó elvárásokat, a büntetőjog *ultima ratio* jellegét.

Zárógondolatok

A fentiek alapján összegezhető, hogy a jogesetben leírt cselekmény a társadalomra olyan csekély mértékben veszélyes, hogy indokolt lenne az információs rendszer felhasználásával elkövetett csalás szabálysértési alakzatát megalkotni. Jelen formában ugyanis a jogesetben szereplő absztrakt cselekmény olyan súlyosan büntetendő, ami nem korrelál a büntetőjog *ultima ratio* jellegével, hanem aránytalan, eltúlzott szankciókat ró a terheltre. Varga Árpád tanulmányában a budapesti kerületi ügyészségek gyakorlatát elemezte az informatikai bűncselekmények vonatkozásában. A kutatása során arra a megállapításra jutott, hogy – habár az általa vizsgált tényállások lefedik az informatikai bűnözés minden

[6] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Ref. BOE-A-1995-25444.
[7] Ley Orgánica 14/2022, de 22 de diciembre. Ref. BOE-A-2022-21800.

formáját – a büntetőjog nem tesz különbséget az elkövetési magatartások között tudás és motiváció alapján, a büntetéskiszabási gyakorlat és a bűnmegelőzés számára ugyanakkor nélkülözhetetlen az elkövetők és az elkövetési magatartások eltérő kategorizálása (Varga 2020). A büntetőjog *ultima ratio* jellegének érvényesülése érdekében a rendőrségi hatékonyságmérés tudományos kidolgozása releváns, amely a jó állam – jó rendészet koncepció keretében biztosította a jogalkalmazás fenntarthatóságát és a nemzetközi trendekhez igazodó visszacsatolást. Ezáltal a kriminalizációs döntések – így az informatikai rendszer felhasználásával elkövetett csalás aránytalanul szigorú szabályozásának – felülvizsgálata is hatékonyabbá tehető (Tihanyi–Vári 2015). Jelen jogeset vonatkozásában kifejezetten érvényesül a szerző ezen megállapítása, hiszen a jogesetben szereplő elkövető informatikai tudását, motivációját tekintve aligha kívánt elkövetni informatikai bűncselekményt, a cselekménye lényegét tekintve a pékáru eltulajdonítására irányult, amit adott helyzetben nem is tudott volna más módon kivitelezni az üzlethelyiség biztonsági szempontból létesített elektronikus, vonalkódolvasóval ellátott kapui miatt. Megjegyzendő, hogy a bírói gyakorlat (BH 2025.3.57) kifejezetten az elemzett jogesettel analóg – hasonlóan alacsony kárérték mellett, habár folytatólagosan megvalósult – esetet vizsgálva rögzíti, hogy a cselekmény az információs rendszer felhasználásával elkövetett csalás bűntettének megvalósítására alkalmas.

Bár a büntetőeljárás más eszközeivel (például megrovás) ellensúlyozható lenne a szigorú szabályozás, annak alkalmazása csak lehetőségként állna a jogalkalmazó szervek részére, így meglehetősen nagy eltéréseket lehetne tapasztalni az ítélkezési gyakorlatban.

Mivel hazánk is részes tagállama a budapesti egyezménynek, így annak rendelkezéseit – mint a tanulmány alapját képező jogeset bűncselekményként történő értékelése – teljesítenie szükséges. Megjegyzendő, hogy az egyezmény 2. Címének 13. Cikke az egyes bűncselekmények vonatkozásában – többek között – arányos retorziót ír elő a tagállamok részére. A fentiek fényében szükségesnek tartom az egyezmény revízióját, amelynek keretében érdemes lenne átgondolni azon felvetést, miszerint bizonyos elkövetési érték alatt az információs rendszer felhasználásával elkövetett csalás szabálysértési alakzata valósulna meg.

Felhasznált irodalom

Ávila Martínez, Víctor (2024): *La estafa informática ¿Cuáles son los tipos más frecuentes?* Online: https://victoravilaabogado.com/estafa-informatica/

Tihanyi Miklós – Vári Vince (2015): Jó állam – jó rendészet, avagy a rendőrség hatékonyságmérésének koncepciója. *Magyar Rendészet,* 15(4), 117–126. Online: https://real.mtak.hu/130416/1/nemesanita-mr-2015-4-09-tihanyi-vri.pdf

Varga Árpád (2020): Informatikai bűnözés egy ügyészségi aktakutatás tükrében. In Kiss Tibor (szerk.): *Válogatás a Magyar Kriminológiai Társaság 2019 és 2020 évben tartott tudományos rendezvényein elhangzott előadásokból.* Budapest: Magyar Kriminológiai Társaság, 125–135. Online: www.kriminologia.hu/files/kiadvany/2020/teljes_kotet.pdf

Vári Vince (2015): Hatékonyság a nyomozásban. In Schaub Anita – Szabó István (szerk.): *III. Interdiszciplináris doktorandusz konferencia 2014 = 3rd Interdisciplinary Doctoral Conference 2014.* Pécs: Pécsi Tudományegyetem Doktorandusz Önkormányzat, 177–195. Online: https://dok.pte.hu/sites/dok.pte.hu/files/2024-03/idk_conference_book_2014.pdf