

Doktori (PhD) értekezés tézisei

**A bizonyítás új dimenziói: Az elektronikus adat, mint a
büntetőeljárás kulcsszereplője**

dr. Bodnár András Péter

Témavezető: Prof. Dr. Elek Balázs
egyetemi tanár



DEBRECENI EGYETEM

Marton Géza Állam- és Jogtudományi Doktori Iskola

Debrecen
2026

I. A doktori értekezés tárgya és célkitűzései, kutatási módszerek, az értekezés struktúrája

I/1. A témaválasztás indoka, aktualitása

Doktori értekezésem az elektronikus adattal, mint új bizonyítási eszközzel foglalkozik, annak elméleti, dogmatikai háttérét dolgozza fel. Megelőzve azt, hogy bárki azt gondolja, a kezében ismételten egy bizonyítás kérdéskörét boncolgató kutatási eredményt tart, amely az amúgy is széleskörű irodalmat egy újabb művel gyarapítja, előre kívánom bocsátani, vizsgálatom nem általánosságban a bizonyítással és ehhez kapcsolódóan egy konkrét bizonyítási eszközzel foglalkozik. A vizsgálat fókuszát kiterjesztem az új bizonyítékhoz – nem feltétlenül szorosan – kapcsolódó területekre is. Első lépésként foglalkozom a bizonyítás általános szabályaival, amely elengedhetetlen, hogy egyes hipotéziseimre a dogmatika oldaláról választ adhassak.

A 2018. július 1-jén hatályba lépett a büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: Be.), amely a korábban hatályban volt 1998. évi XIX. törvény (a továbbiakban: 1998. évi Be.) bizonyítási eszközökre vonatkozó rendelkezéseit kibővítette. A Be. immáron a 165. § f) pontjában önálló bizonyítási eszközként deklarálja az elektronikus adatot.

Arra a kérdésre, miért volt szükség az elektronikus adat önálló szabályozására, a Be. miniszteri indokolását könnyen hivatkozhatnánk, miszerint: *„A törvény egyik kifejezett célja olyan büntetőeljárás kialakítása, amely a jövő kihívásaira is képes választ adni. Az új bizonyítási eszköz definiálása ezért nem öncélú, az elektronikus adatra további részletszabályokban rendezett eljárási cselekmények, így például a lefoglalás különleges szabályai épülnek.”*¹

A helyzet azonban ennél árnyaltabb. Róth Erika álláspontja szerint ugyanis az önálló, új bizonyítási eszközként történő szabályozás arra vezethető vissza, hogy a jogalkotó és főként a jogalkalmazó nem tudta eldönteni, hogyan kell kezelni az ilyesfajta bizonyítékokat. Ez alatt azt kell érteni, hogy a megszerzésükre és megőrzésükre számos esetben nem igazán lehetett alkalmazni a tárgyi bizonyítási eszközre vonatkozó, már rutinszerű módon alkalmazott szabályokat. További problémát jelentett, hogy hiányzott az elektronikus adat átfogó meghatározása, valamint nem volt egyértelmű, mikor igazolható egyes adatok megszerzése

¹ T/19972. számú törvényjavaslat a büntetőeljárásról szóló törvény 165. §-ához.

érdekében a teljes adathordozó lefoglalása, továbbá mikor, milyen eljárásrendben kerülhetett sor az adat lefoglalására. Ezen kérdés nyitott volta nem csupán célszerűségi szempontból jelentett aggályt, hanem a szükségesség, arányosság aspektusából is kérdéses volt, azaz alkotmányossági aggályokat is felvetett. A fentiekből tehát arra lehetne következtetni, hogy nem is az elektronikus adat „önállósítása” volt a cél, az csupán eszköze volt az egyes eljárási cselekmények és kényszerintézkedések pontosabb szabályozásához.²

A fentiekhez kapcsolódó, hogy a Be. fogalommeghatározása szerint az új bizonyítási eszköz definíciója a következőképp hangzik: *„Elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.”*³ A kódex hozzáteszi ugyanakkor: *„Ahol e törvény tárgyi bizonyítási eszközt említ, azon e törvény eltérő rendelkezése hiányában az elektronikus adatot is érteni kell.”*⁴

A Be. meghatározza az elektronikus adat fogalmát, de a szabályozás részévé teszi azt is, ahol a törvény tárgyi bizonyítási eszközt említ, ott a törvény eltérő rendelkezése hiányában az elektronikus adatot is érteni kell. Ezzel kiegészítéssel a törvény maga tette fel a kérdést: valóban újnak tekinthető-e e bizonyítási eszköz?

Kutatásom elindításához részben gyakorlati tapasztalás vezetett. Kutatásom elején még ügyvédjelöltként, később már önálló ügyvédként a büntetőeljárások során védői szerepben eljárva hamar ráébredtem, a magyarországi vádsikerességi ráta mellett egy védő akkor érhet el sikereket, ha az eljárásjog részleteit behatóan ismeri. Ennek kapcsán pedig hatalmas jelentősége van a bizonyítási eljárásnak.

A bizonyítási eljárás pedig nem vitatottan a büntetőper sarokpontja, amelyen áll vagy bukik egy-egy emelt vád sikeressége. Ennek kapcsán pedig kiemelkedő jelentőségű egy adott bizonyítási eszköz mögött meghúzódó jogi szabályozás ismerete. Ha egy dogmatikai szabályozás nem nyújt egyértelmű választ a gyakorlatban felmerülő szituációra, azaz teret

² RÓTH Erika: *Az elektronikus adat, mint új bizonyítási eszköz megjelenése az új büntetőeljárás törvényben.* in.: Miskolci Jogi Szemle, 2019/2., 347-348.

³ A büntetőeljárásról szóló 2017. évi XC. törvény 205. § (1) bek.

⁴ A büntetőeljárásról szóló 2017. évi XC. törvény 205. § (2) bek.

enged eltérő következtetéseknek, döntéseknek, az bizonytalanságot eredményez, mely sértheti a tisztességes eljáráshoz való jogot, és végül veszélybe is sodorhatja a büntetőeljárás egyik célját, az igazság elérését is.

Kutatásom célja tehát, hogy választ adjon az elektronikus adat vonatkozásában felmerülő konkrét kérdések mellett olyan kérdésekre is, mint a tisztességes eljáráshoz fűződő alapjog, a szakértői bizonyítás, a bírói meggyőződés, avagy a Mesterséges Intelligencia által az eljárással szemben támasztott kihívások vizsgálata. Mindezt úgy foglalnám össze, arra keresem a választ, hogy az évtizedekkel korábbi elméleti alapokra épített bizonyításelmélet hogyan válaszol a 21. századi digitális valóságra.

A cél tehát az elektronikus adat helyének megtalálása a jogrendszerben, ennek során pedig olyan kérdéseket szükséges tisztázni, pontosan mit is tekintünk elektronikus adatnak a büntetőeljárásban. Továbbá, az elektronikus adat sui generis bizonyítási eszköz-e, vagy csupán a tárgyi bizonyítási eszköz alkategóriája. Miként garantálható vonatkozásában a hitelesség és az integritás, azaz mi a garancia arra, hogy a keletkezéstől a bírói értékelésig az elektronikus adat változatlan maradt, valamint arra is, hol kezdődik a szakértői bizonyítás határa, avagy a bíró meddig mehet el az adatok értékelésében. Természetesen a fenti kérdésekre történő válaszadás során nem mehetek el amellett, hogy megvizsgáljam a nemzetközi környezetet, így különösen az angolszász jogrendszer tengerentúli megoldásait, avagy az európai, kontinentális jogrendszert alkalmazó államok alkalmazta módszereket.

I/2. Az értekezés struktúrája, módszertani alapvetés

A vizsgálat fókuszát kiterjesztem az új bizonyítékhoz – nem feltétlenül szorosan – kapcsolódó területekre is. Első lépésként foglalkozom a bizonyítás általános szabályaival, amely elengedhetetlen, hogy egyes hipotéziseimre a dogmatika oldaláról választ adhassak. A fenti célok eléréséhez nem kerülhetők meg a bizonyítás történet elemző fejezetrészek mellett olyan más alapvető kérdésekre történő kitérések sem, mint a tisztességes eljáráshoz való jog, a bizonyítást érintő alapelvek, a szakértői bizonyítás, a bírói meggyőződés, vagy éppen a Mesterséges Intelligencia okozta nehézségek a büntetőeljárásban. A hatályos törvényi szabályozáson túlmenően azon kérdések tárgyalása során, ahol ennek relevanciája van, górcső alá veszem a joggyakorlatot aktakutatáson keresztül, mely kapcsán nem hagyható figyelmen

kívül az Emberi Jogok Európai Bíróságának (a továbbiakban: EJEB) és az Európai Unió Bíróságának (a továbbiakban: EUB) gyakorlatának elemzése sem.

A kutatásomat alapvetően alkalmazott kutatásnak titulálom, amelyben a deduktív módszer a hangsúlyos a dogmatika oldaláról. A lényeges elméleti kérdések mellett azonban a társadalomtudományi empirikus módszerek is alkalmazásra kerülnek.

Kutatásom módszertanára lényeges ráhatással van az, hogy gyakorló ügyvéd vagyok, így kutatásom részben mégiscsak saját tapasztalaton alapul. Nyilvánvaló, hogy a bizonyítás a jogtörténeti fejlődés során számos változáson esett át, amelyet az általános bizonyítást érintő fejezetben be is mutatok. A tudományos kutatás eredményeinek eléréséhez vezető úton jelentőséggel bírnak a hazai gyakorlati döntések mellett az EJEB és az EUB konkrét ügyekben hozott döntései is. A hazai szakirodalom feldolgozása és elemzése mellett dolgozatom nem hagyja figyelmen kívül a nemzetközi szakirodalmat sem, néhol annak összehasonlító elemzését sem.

A kutatás eredményeit bemutató munka során vizsgálat tárgyává teszem – legyen szó annak elméleti vagy gyakorlati oldaláról –, hogy az elektronikus adatot érintő kérdésekkel kapcsolatban amennyiben eltérő a gyakorlat, úgy azt lehet-e vagy kell-e jogszabálmódosítással kezelni. Nem titkon célom az, amennyiben a kutatás eredményeit látva azt tapasztalom, a gyakorlaton javítani, változtatni lehet, avagy szükséges, úgy arra javaslatot tegyek.

A dolgozat bevezetésében megfogalmazom a kutatás alapjait, bizonyos felvetéseket, valamint a kutatásom módszereit. A kutatási téma, a kutatási területek, önmagában a kutatás okának és céljának felvázolása mellett kitérek a hipotéziseimre is, amelyek megválaszolása e dolgozat feladata.

I/3. Hipotézisek és kutatási kérdések

1. Az elektronikus adat nem csupán névleg vált önálló bizonyítási eszközzé, az dogmatikai szempontból is új bizonyítási eszköznek tekinthető. Azzal, hogy a Be. a 205. §-ban meghatározza, pontosan mit ért az elektronikus adat alatt, ténylegesen kiemeli a tárgyi bizonyítási eszköz hatálya alól, azt önálló bizonyítási eszköznek tekinti. Erre utalhat önmagában a sui generis szabályozás indoka, ugyanis a korábbiak során a tárgyi bizonyítási

eszközre vonatkozó szabályok nem minden esetben voltak megfeleltethetők az ilyen jellegű adatokra.

2. Az elektronikus adatokat érintő lefoglalás során sérülhet a célhoz kötöttség elve, tekintettel arra, hogy a kényszerintézkedés foganatosítása során elkerülhetetlenül hozzáférhetők a bűncselekményen kívül eső adatok is.

3. Az elektronikus adatok nem eredeti formában való közlése a védővel vagy a terhelttel, sértheti a tisztességes eljáráshoz fűződő jogot. Az olyan jellegű bizonyítékoknál, ahol ennek jelentősége van, a védelemnek és a terheltnek eredeti formájában szükséges megismernie a bizonyítékot. Erre példaként szolgálhat a leplezett eszközök alkalmazásának eredménye. Nem elégséges ugyanis a lehallgatási anyag leírt jelentését átadni a terheltnek, lehetőséget kell biztosítani arra, hogy eredeti formájában ismerje meg a felvételeket. Ha pedig a terhelt letartóztatásban van, úgy a technikai feltételeket is biztosítani kell számára, ellenkező esetben sérül a tisztességes eljáráshoz fűződő joga.

4. A büntetőeljárás gyakorlatában az elektronikus adat eredetisége nehezen értelmezhető, így a bizonyítási eszközből származó bizonyíték értéke nem adat eredetiségén, hanem annak változatlanságát igazoló folyamaton alapul. Az elektronikus adatok esetében nem elegendő a zárt bizonyítási lánc megléte, ha a forráseszközhöz való hozzáférés körülményei nem megfelelően dokumentáltak.

5. Az elektronikus adatok a nagyobb validitást mutatnak a klasszikus személyi jellegű bizonyítási eszközöknél. Az elektronikus adatok objektivitásuk révén alkalmasak egy-egy vallomás – pl.: tanúvallomás – cáfolatára vagy megerősítésére.

6. A Mesterséges Intelligencia terjedésével a digitális képi és hangi bizonyítékok bizonyító ereje kérdésessé válhat. A bíróságnak megfontolás tárgyává kell tenniük az igazságügyi informatikus szakértő kirendelését minden olyan esetben, ahol a terhelt tagadja a felvétel valóságát. A "látni annyi, mint hinni" elvét felváltja a "látni annyi, mint gyanakodni" elve, ami drasztikusan lassíthatja a bizonyítási eljárást, holott a Be. megszületésének egyik indoka a büntetőeljárás hatékonyabbá és gyorsabbá tétele volt.

Ehhez kapcsolódhat az, hogy a rendőrség egyre gyakrabban használ olyan szoftvereket, amelyek arcfelismeréssel vagy mozgásmintázat-elemzéssel azonosítják az elkövetőt. Ha egy algoritmus jelöli meg a terheltet, a Be. szerint ez önmagában nem lehet bizonyíték, csak "adatgyűjtés eredménye". Ezen eredmények elfogadhatóvá tételéhez a jövőben nem egy hagyományos szakértőre lesz szükség, hanem a szoftver forráskódjának és tanítási adatainak "kihallgatására". Ez új eljárási jogi kategóriát teremthet: az algoritmus nem tanú és nem is tárgyi bizonyíték, hanem egy sajátos, "technológiai vélemény", amelynek ellenőrizhetőség a tisztességes eljárás alapfeltételévé válik.

II. Konklúzió, a hipotézisek igazolása

A jelen doktori értekezés célkitűzése az volt, hogy feltárja azokat a fundamentális változásokat, amelyeket az elektronikus adat, mint új bizonyítási eszköz megjelenése és MI-technológiák büntetőeljárási alkalmazása idézett elő. A vizsgálódás során áttekintettük a bizonyítási eljárás fejlődéstörténeti ívét, a 19. századi klasszikus bizonyításelméleti alapoktól eljutva a 21. századi, digitalizált valóságig. E folyamat során vált nyilvánvalóvá, hogy az elektronikus adat nem csupán egy újabb technikai tétel a bizonyítékok listáján, hanem egy olyan paradigmaalkotó erő, amely alapjaiban kérdőjelezi meg a tárgyi bizonyítási eszközökre vonatkozó évszázados dogmatikai struktúrákat. A kutatás során végzett aktakutatás és a hazai, illetve nemzetközi joggyakorlat elemzése rávilágított arra a feszültségre, amely a törvényalkotói szándék, példaként említve a hatékonyabb és gyorsabb eljárás megteremtését és a jogalkalmazói gyakorlat, valamint a tisztességes eljáráshoz való jog garanciáinak érvényesülése között feszül.

A bizonyítási eljárás büntetőperünk sarokpontja, amelyen az anyagi igazság kiderítése és a vádsikeresség egyaránt múlik. Az értekezés központi tézise, miszerint az elektronikus adat önálló bizonyítási eszközként való kezelése dogmatikai szempontból indokolt, beigazolódott. A hatályos törvény, Be. ugyan kísérletet tesz az elektronikus adat fogalmának definiálására, ám a gyakorlati jogalkalmazásban a bíróságok és a nyomozó hatóságok gyakran visszanyúlnak a tárgyi bizonyítási eszközökre vonatkozó, rutinszerűen alkalmazott szabályokhoz. Ez a „visszalépés” azonban a digitális bizonyítékok sajátos természetéből adódóan alkotmányossági aggályokat vet fel. A tárgyi bizonyítási eszközök esetében a fizikai érinthetőség és a közvetlen érzékelhetőség a garancia alapja, addig az elektronikus adat esetében a hitelesség és az integritás az a folyamat, amelyen a bizonyító erő áll vagy bukik. Az adat eredetiségének kérdése helyett tehát a hiteles megőrzés láncolata vált az értékelés kulcskérdésévé.

A kutatás elméleti és gyakorlati vizsgálata során rávilágítottunk arra, hogy a digitális bizonyítékok magasabb validitása okán, amely képes megkérdőjelezni vagy éppen megerősíteni a vallomásalapú személyi bizonyítékokat, a büntetőeljárás objektivitásának irányába mutat. Ugyanakkor – és ez az értekezés egyik legfontosabb megállapítása – a „látni annyi, mint hinni” klasszikus elv a digitális világban, különösen az MI-alapú eszközök megjelenésével, átfordul a „látni annyi, mint gyanakodni” elvébe. Ez a szemléletváltás a bírói szabad mérlegelés elvét is új kontextusba helyezi. A bíróság, mint jogalkalmazó szerv technikai kontroll nélkül, kritika nélkül kénytelen elfogadni az informatikus szakértő véleményét. Ezzel a bírói mérlegelés, de facto szakértői döntéshozattá alakul, ami sértheti a bírói függetlenséget és a tisztességes eljáráshoz való jogot, amennyiben a szakértői vélemény „fekete dobozként” funkcionál.

A MI büntetőeljárás térnyerése, például az arcfelismerő szoftverek alkalmazása, új eljárásjogi kategóriák szükségességét veti fel. A jelenlegi szabályozási keretek között az algoritmus nem tanú, nem is tárgyi bizonyíték, hanem elektronikus adat, amelynek ellenőrizhetősége, azaz a forráskód és a tanítási adatok vizsgálata a tisztességes eljárás elengedhetetlen feltételévé válik. Amennyiben a büntetőeljárás nem képes lépést tartani a technológiai fejlődéssel, a bizonyítási eljárás a valóság megismerésére irányuló törekvés helyett az algoritmusok által generált valóságok elfogadásának színterévé silányulhat.

Ezért elengedhetetlen annak a garanciarendszernek a megerősítése, amely a terhelt számára biztosítja a technológiai alapú bizonyítékok megismerésének jogát, különös tekintettel az eredeti formátumú betekintésre és a technikai segédeszközökhöz való hozzáférésre, még a kényszerintézkedések hatálya alatt is, a bv. intézet keretein belül.

Az elektronikus adat helye a jogrendszerben immár nem csupán elméleti kérdés, hanem a jogállami büntetőeljárás egyik legfontosabb sarokköve, amelynek szabályozása nem tűrt halasztást, és amely a jogtudomány minden szegmensét – az eljárásjogtól a kriminalisztikán át a technológiai jogig – komoly interdiszciplináris feladat elé állítja. A vizsgálatom tehát nem ért véget a jogszabályok elemzésével, hanem egy olyan gondolkodásmód alapozására törekedett, amely a technológiai semlegesség és a garanciális védelem egyensúlyát keresi a jövő büntetőperében, ahol a valóság megismerése már elválaszthatatlan a digitális bizonyítékok megbízható és etikus kezelésétől.

Ebben a szellemenben kívánom lezárni az értekezést, miután választ adtam a dolgozat elején feltett kérdésekre, és egy olyan jövőképet vázoltam fel, amelyben a büntetőeljárás a technológia adta lehetőségeket kihasználva, de a tisztességes eljárás alapelveit szem előtt tartva képes marad az igazság maradéktalan feltárására.

A kutatás során szerzett tapasztalatok, a gyakorlati esetek és az elméleti összefüggések együttes vizsgálata alapján remélhetőleg sikerült olyan szempontokat megfogalmaznom, amelyek elősegítik az elektronikus adat büntetőeljárás szerepének tisztázását és az MI okozta kihívások jogi kezelését, biztosítva ezzel, hogy a büntetőeljárás a 21. században is méltó maradjon az igazság kutatásának nemes feladatához, és ne váljon az elszemélytelenedő technológia passzív eszközévé, hanem megőrizze emberközpontú, garanciális jellegét.

1. Az elektronikus adat nem csupán névleg vált önálló bizonyítási eszközzé, az dogmatikai szempontból is új bizonyítási eszköznek tekinthető. Azzal, hogy a Be. a 205. §-ban meghatározza, pontosan mit ért az elektronikus adat alatt, ténylegesen kiemeli a tárgyi bizonyítási eszköz hatálya alól, azt önálló bizonyítási eszköznek tekinti. Erre utalhat önmagában a sui generis szabályozás indoka, ugyanis a korábbiak során a tárgyi bizonyítási eszközre vonatkozó szabályok nem minden esetben voltak megfeleltethetők az ilyen jellegű adatokra.

Az elektronikus adat új bizonyítási eszközként történő szabályozás arra vezethető vissza, hogy a jogalkotó és főként a jogalkalmazó nem tudta eldönteni, hogyan kell kezelni az ilyesfajta bizonyítékokat. Ez alatt azt kell érteni, hogy a megszerzésükre és megőrzésükre esetekben nem igazán lehetett alkalmazni a tárgyi bizonyítási eszközre vonatkozó, már rutinszerű módon alkalmazott szabályokat. További problémát jelentett, hogy hiányzott az elektronikus adat átfogó meghatározása, valamint nem volt egyértelmű, mikor igazolható egyes adatok megszerzése érdekében a teljes adathordozó lefoglalása, továbbá mikor, milyen eljárásrendben kerülhetett sor az adat lefoglalására. Ezen kérdés nyitottként állása nem csupán célszerűségi szempontból jelentett aggályt, hanem a szükségesség, arányosság aspektusából is kérdéses volt, azaz alkotmányossági aggályokat is felvetett. A fentiekből tehát arra lehetne következtetni,

hogy nem is az elektronikus adat „önállósítása” volt a cél, az csupán eszköze volt az egyes eljárási cselekmények és kényszerintézkedések pontosabb szabályozásához.⁵

Tény, hogy a bizonyíték fogalmának esszenciális része, hogy az információ megszerzése törvény általi forrásból, így bizonyítási eszközből történjen. A digitális bizonyítékok vonatkozásában ez a forrásmegjelölés azonban nem ilyen egyértelmű. A digitális adatok esetében, azok forrása kapcsán két út jelenik meg. Az első választható ösvény, hogy a digitális bizonyítékok forrása mindig egy tárgy, amely a bizonyítékot tartalmazó adatot – legyen az kép-, video- vagy szövegfájl – hordozza. A másik választható ösvény szerint a bizonyíték forrása az elektronikus módon tárolt adat – így a kép-, video- vagy szövegfájl stb. –, hiszen a hatóság közvetlenül ebből kaparítja meg a releváns információt, a hardver csupán tároló, mint a tárgyi bizonyítási eszköz esetében a szekrény.⁶

Előbbi esetben a digitális bizonyítékokat minden esetben olyan tárgyi bizonyítási eszközök hordozzák, amelyek képesek az elektronikus formában létező adatok rögzítésére, tárolására, továbbítására. Ilyen eszközök lehetnek az asztali számítógépek, laptopok telefonok, táblagépek, nyomtatók stb. A másik esetben tehát a bizonyítékforrás maga az adat, hiszen a hatóságok közvetlenül ebből nyerik az információt, a hordozó csupán a „szekrény” funkcióját tölti be.

A fenti indokolások álláspontom szerint elfogadhatók, azokkal mindent tekintetben azonosulni tudok, és kijelenthetem, hogy az elektronikus adat új bizonyítási eszköznek tekinthető a büntetőeljárásban.

2. Az elektronikus adatokat érintő lefoglalás során sérülhetett a korábbi törvény során a célhoz kötöttség elve, tekintettel arra, hogy a kényszerintézkedés foganatosítása során elkerülhetetlenül hozzáférhetők a bűncselekményen kívül eső adatok is.

Álláspontom szerint az állítás igazolás nyert. A korábbi törvény alatt ugyanis viták folytak arról, pontosan mit is szükséges lefoglalni, így az adatok egyes körét, az adathordozót, avagy az egész informatikai rendszert. Példaként említhető, hogy a korábbi eljárásjogi törvényt módosító 2013. évi CLXXXVI. törvény hatálybalépését megelőzően bevett gyakorlat volt a teljes információs

⁵ lsd. RÓTH Erika (2019): *i.m.*, 347-348.

⁶ SORBÁN Kinga: *A digitális bizonyíték a büntetőeljárásban*. In.: Belügyi Szemle, 2016/11.

rendszer lefoglalása olyan, a büntetőeljárás szempontjából relevanciával nem bíró eszközöket is beleértve, mint az eger vagy a billentyűzet.⁷ Az egész számítógépes rendszer lefoglalásával pedig olyan adatok is a hatósághoz kerültek, aminek semmi köze a büntetőeljáráshoz.

Ahogy más bizonyítási eszközök esetében, úgy az elektronikus adat kapcsán is fontos a törvényesség, szakszerűség és a zárt bizonyítási lánc megléte. Három alapvető kritériumnak kell megfelelni a nyomozás szakaszában: a bizonyíték megszerzésénél ne sérüljön vagy módosuljon az eredeti adat, bizonyítható legyen az egyezés az eredetivel, valamint a bizonyíték elemzése azt ne változtassa meg. A Be. egyúttal az elektronikus adatra épülő kényszerintézkedések rendszerét vezette be, így az elektronikus adat lefoglalását (Be. 315. §), ezen belül a megőrzési kötelezettséget (Be. 316. §), valamint az ideiglenes hozzáférhetetlenné tételét (Be. 335. §). Érdemi változtatás a lefoglalás szabályaiban eszközölt az új kódex.⁸

A Be. 151. § (1) bekezdése alapján a lefoglalás célja a bizonyítási eszköz, illetve az elkobozható dolog vagy a vagyonelkobzás alá eső vagyon biztosítása a büntetőeljárás eredményes lefolytatása érdekében. Jelen kényszerintézkedés az elektronikus adat feletti tulajdonjogot korlátozza, amelyet a bíróság, az ügyészség és a nyomozó hatóság is elrendelhet. E jogintézmény kulcsfontosságú szerepet játszik az informatikai bűncselekmények felderítésében, az elektronikus bizonyítékok megszerzésének és megőrzésének eszközeként. Régóta viták folynak arról, hogy pontosan mit is kellene az eljárás során lefoglalni, így a meghatározott adatok körét, vagy az adathordozót, vagy a teljes információs rendszert. Érdemes megemlíteni, hogy az adat lefoglalását először a 2013. évi CLXXXVI. törvény 21. §-a illesztette be az 1998. évi Be-be. Ezt megelőzően bevett gyakorlatként volt érvényben a számítógép egészének a lefoglalása (pl. sokszor a büntetőeljárás szempontjából lényegtelen hardvereszközökkel együtt, mint a monitor és a billentyűzet), később a merevlemez vagy még azt sem, és csak másolatot készítettek róla, majd a módosítást követően csak az adatokat foglalták le.⁹

3. Az elektronikus adatok nem eredeti formában való közlése a védővel vagy a terhelttel, sértheti a tisztességes eljáráshoz fűződő jogot. Az olyan jellegű bizonyítékoknál, ahol

⁷ BODNÁR András Péter: A digitális adatok megjelenése a büntetőeljárásban – különös tekintettel a szakértő igénybevételére. In.: Büntetőjogi Szemle, 2022/1., 22-23.

⁸ MEZEI Kitti: Az elektronikus bizonyítékokkal kapcsolatos kihívások és szabályozási újdonságok. In.: Belügyi Szemle, 2019/10., 27-28.

⁹ MEZEI Kitti: *i.m.*, 27–28.

ennek jelentősége van, a védelemnek és a terheltnek eredeti formájában szükséges megismernie a bizonyítékot. Erre példaként szolgálhat a leplezett eszközök alkalmazásának eredménye. Nem elégséges ugyanis a lehallgatási anyag leírt jelentését átadni a terheltnek, lehetőséget kell biztosítani arra, hogy eredeti formájában ismerje meg a felvételeket. Ha pedig az terhelt letartóztatásban van, úgy a technikai feltételeket is biztosítani kell számára, ellenkező esetben sérül a tisztességes eljáráshoz fűződő joga.

Álláspontom szerint, olyan esetekben, amelyek során az digitális bizonyítéknak – hanganyagnak – jelentősége nagyobb, és a terhelt nem kapja meg a digitális anyagot, akkor sérülhet tisztességes eljáráshoz fűződő joga.

Erre jó példa lehet, hogy a leplezett eszközök az öt évig terjedő vagy súlyosabb szabadságvesztéssel büntetendő szándékos bűncselekmény esetén alkalmazhatók,¹⁰ amely reálissá teszi azt, hogy a terhelttel szemben sor kerülhet a legszigorúbb kényszerintézkedés alkalmazására. A kérdés pedig az, hogy a lehallgatási anyagok leírt formában történő megismerése sérti-e a tisztességes eljáráshoz fűződő jogot, s így – például – a büntetés-végrehajtási intézeteknek biztosítani kell-e, hogy a terhelt meghallgathassa a lehallgatási anyagot. Álláspontom szerint a kérdés lényeges, hiszen a lehallgatási anyagoknál különösen igaz, hogy – a hangsúlyok, szövegkörnyezet alapján – más és más jelentést hordozhat valami előszóban, mint ugyanaz leírva.

Erre nagyszerű példaként szolgálhat az igazságügyi nyelvész szakértő melletti igényen túlmenően a Debreceni Ítéltábla Bf.III.372/2024/32. számú ítélete, amelyben a Táblabírárság rámutatott arra, hogy a videófelvétel – a paradigmaváltást szem előtt tartva, mint elektronikus adat, digitális bizonyíték – könnyebben oszthat el kétségeket a papíron rögzített – nyomozó hatósági tag által gépelt – vallomással szemben, különösen akkor, ha arra gondolunk, nem minden esetben egyeznek az elhangzottak a leírtakkal. a Szegedi Ítéltábla is felismerte ennek jelentőségét. További példa lehet a Szegedi Ítéltábla ÍH2018. 130. számú határozata. Az Ítéltábla rámutatott arra, hogy a büntetőügyben elektronikus formában keletkezett összes iratról a vádlott részéről ismételt előterjesztett elektronikus másolat kiadása iránti kérelem nem utasítható el. A további másolatok kiadását az illeték megfizetését követően engedélyezni kell. A tartalma a következőképp foglalható össze:

¹⁰ 2017. évi XC. törvény a büntetőeljárásról 234. § (1) bekezdés.

Az eseti döntés a büntetőeljárás iratmegismerés jogintézményének – a digitális kor elvárásaihoz igazodó – dogmatikai újraértelmezése szempontjából meghatározó jelentőségű. A döntés a büntetőeljárás során keletkezett elektronikus adatokhoz, illetve a lefoglalt adathordozók tartalmához való hozzáférés szabályozási körét vizsgálja, különös tekintettel a korábbi és a hatályos büntetőeljárás törvény közötti átmeneti időszak jogalkalmazási kihívásaira.

Az eljárás alapjául szolgáló jogvita lényege az elítélt ismételt másolatkészítés iránti kérelme volt, amely a büntetőeljárás során keletkezett, lefoglalt adathordozókon tárolt elektronikus bizonyítékok sokszorosítására irányult. Az elsőfokú bíróság az elutasító döntését az 1998. évi Be. 70/B. § (10) bekezdésére, valamint a másolatkészítés egyszeri teljesítésére alapozta, szemantikailag az "eljárás jogerő" és a "szolgáltatás teljesítettsége" fogalomkörébe helyezve a problémát. Ezzel szemben a másodfokú bíróság – a jogorvoslati eljárásban – a kérdéskört a védelemhez való jog, valamint az iratmegismerés garanciális szabályainak tükrében vizsgálta, élesen elhatárolva az adat megismeréséhez fűződő abszolút jogot az adathordozóra történő, technikai reprodukciót igénylő másolatkészítés szolgáltatási jellegétől.

A döntés egyik legfontosabb jogelvi eleme az iratmegismerés és a másolatkészítés közötti különbség. A bíróság rögzítette, hogy bár a terheltnek az ügyiratok megismeréséhez fűződő joga garanciális jelentőségű, a másolatkészítés, különösen, ha az elektronikus adathordozókon tárolt nagy volumenű adatok fizikai reprodukcióját igényli, már nem tekinthető az eljárási jogok korlátlan, alanyi jogon járó elemének. A jogalkotó által biztosított illetékmentesség az első alkalommal igényelt másolatra vonatkozik, amely a védekezéshez való jog érvényesülését hivatott biztosítani. Ezt követően a további másolatok iránti kérelem már nem a büntetőeljárás alapjogok sérelmét, hanem a technikai erőforrások igénybevétele érinti, így az illetékekről szóló 1990. évi XCIII. törvény szabályai szerint, költségtérítés mellett teljesíthető.

A bírósági érvelés különös jelentőséggel bír az elektronikus bizonyítékok kezelése terén, mivel rámutat arra a dogmatikai nehézségre, hogy a digitális adatok elvi sokszorosíthatósága nem írja felül a büntetőeljárás racionális igazgatásának szempontjait. A döntés implicit módon elismeri a digitális bizonyítékok sajátosságait: az adathordozó (hardware) és az azon tárolt tartalom (adat) kettősségét. Ezzel a bíróság egyfajta költséghatékony procedurális egyensúlyt teremt, ahol az állam az eljárás kezdetén biztosítja a bizonyítékok megismerhetőségét, ám a további, repetitív igényeket már az eljárásjogi és költségvetési fegyelem keretei közé szorítja. A

másodfokú bíróság eljárása ezen a ponton korrigálta az elsőfokú végzés indokolását: az elutasítás helyett a kérelem teljesítését rendelte el, de a költségviselés egyértelmű előírása mellett

4. A büntetőeljárás gyakorlatában az elektronikus adat eredetisége nehezen értelmezhető, így a bizonyítási eszközből származó bizonyíték értéke nem adat eredetiségén, hanem annak változatlanságát igazoló folyamaton alapul. Az elektronikus adatok esetében nem elegendő a zárt bizonyítási lánc megléte, ha a forráseszközhöz való hozzáférés körülményei nem megfelelően dokumentáltak.

Álláspontom szerint az állítás igazolást nyert. Rámutattam arra, annak ellenére, hogy a digitális bizonyíték a kiterjedt információtartalma révén elősegíti a bűnösség megállapítását, egyedi kihívásokat is támaszt. Nagy volumene, gyors keletkezése és a manipulálhatóságának lehetősége bonyolulttá teszi a hitelesítését. A digitális bizonyítékok emellett kitettek különféle külső hatásoknak és emberi tényezőknek is, amelyek veszélyeztethetik a sértetlenségüket. Szemben a fizikai bizonyítékkal, amelynek dokumentálása kézenfekvő, a digitális bizonyíték jóval összetettebb eljárásokat igényel. A távoli hozzáférés egyszerűsége, a fájlok másolhatósága és a felhasználói mobilitás megnehezíti a digitális bizonyítékok dokumentálását és megőrzését. A digitális bizonyíték sérülékeny természete miatt a nyomozás során végig aprólékos dokumentációra van szükség. Az a bizonyíték felel meg csak a felhasználhatóság szigorú kritériumainak, amely változatlan és megbízható marad. Ezért elengedhetetlen a digitális bizonyítékok tekintetében is – ha mondhatom így – egy felügyeleti lánc biztosítása (angolul Chain of Custody), amely garantálja a digitális bizonyíték sértetlenségét és hitelességét a teljes büntetőeljárás alatt.¹¹

Az általam fent használt kifejezés, elv lényege talán úgy ragadható meg, miszerint: „*amit nem írtál le, az meg sem történt*”, hűen tükrözi az alapos dokumentáció iránti alapvető igényt, figyelembe véve a digitális bizonyítékok már említett sérülékeny természetét. A megfelelő dokumentáció elengedhetetlen annak igazolásához, hogy a bíróság elé tárt bizonyíték hiteles és manipulációmentes. A felügyeleti lánc folyamata ezt úgy biztosítja, hogy aprólékosan rögzíti a

¹¹ NATH Souradip–BAEK Jaeojong, Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics, IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, Washington, 2024, 2.

bizonyíték „útjának” minden egyes lépését az ügy teljes életciklusa során. Az elvnek az alábbi kérdésekre kell választ adnia:

- **Mi?** Mi maga a bizonyíték?
- **Hogyan?** Hogyan történt a gyűjtése és a tárolása?
- **Ki?** Ki vette birtokba, ki rendelkezett felette?
- **Mikor?** Mikor történt a begyűjtése, továbbítása vagy kezelése?
- **Hol?** Merre „utazott” a bizonyíték, hol tárolták/vizsgálták?
- **Miért?** Miért volt szükség a bizonyíték továbbítására vagy átadására?

A láncnak részletes beszámolóval kell rendelkeznie a bizonyíték kezeléséről, beleértve a vizsgálatban és elemzésben részt vevő személyek azonosító adatait, a helyszíneket és az elvégzett tevékenységeket. Ez az átfogó dokumentáció fenntartja a bizonyíték sértetlenségét, valamint növeli az átláthatóságot és az elszámoltathatóságot a forenzikus folyamat során. Az eljárásokban a láncolatnak döntő jelentősége lehet a szakértői vélemény alátámasztása kapcsán. A bíróság elé tárva a láncolat igazolja a bizonyíték hitelességét és sértetlenségét, megerősítve a bizonyítékot.

5. Az elektronikus adatok a nagyobb validitást mutatnak a klasszikus személyi jellegű bizonyítási eszközöknél. Az elektronikus adatok objektivitásuk révén alkalmasak egy-egy vallomás – pl.: tanúvallomás – cáfolatára vagy megerősítésére.

Röviden: igen. Bemutatásra került egy pécsi eset, amelyben a terhelti vallomás szerint a fiatalember az adott napon – egyébként a tetthelytől mintegy tíz kilométerre lévő lakóhelyén – 9 óra magasságában ébredt fel. Édesanyja 7 óra körül távozott otthonról autójával, míg édesapja azelőtt 6 órakor indult dolgozni, szintén saját gépjárműjével. Emlékezete szerint 10 óra 30 perc és 11 óra között kapcsolta be a számítógépét, mert szükséges volt neki a német tanuláshoz, tekintettel arra, hogy Ausztriába készült dolgozni. Mobiltelefonja üzemelt, de hívást nem indított és nem is fogadott rajta. A német tanulás befejezését követően felhívta 12 óra 32 perckor barátnőjét, akivel egyeztetette az aznapi találkozót. A nyomozás adatai szerint a mobiltelefonos adatsor azt mutatta, hogy a terhelt nevén lévő telefon folyamatosan bekapcsolt állapotban volt, és az adott napon végig a lakóhelyhez legközelebbi toronyhoz csatlakozott, egészen a terhelt által is megadott távozási időpontig. Fontos adatot szolgáltatott a nyomozó hatóságnak, hogy a terhelt számítógépéről kinyert adatok azt mutatták, hogy a számítógépet az adott napon 11 óra

05 perckor kapcsolták be. Tekintettel arra, hogy a bejelentés 10 óra 49 perckor érkezett a rendőrségre, és a pénztároshölgy azt állította, a deliktum éppen most történt, így az elkövetés időpontja 10 óra 48 percben került megállapításra.¹² Szemben a tanú vallomásával, aki cselekmény másnapján az terhelt fényképét másik három mellett bemutatták a tanúnak, aki hetven százalékban volt biztos abban, hogy a férfi volt az elkövető. Miután a nyomozók letakarták homlokát, már nyolcvan százalékban volt biztos a dolgában. Leginkább akkor lett biztos magában, amikor megmutatták neki a videofelvételt. A későbbi szembesítésen már a hangjáról is határozottan felismerte a későbbi gyanúsítottat.¹³

A fentiekre tekintettel elmondható, hogy a digitális bizonyítékok nagyobb validitást mutatnak a klasszikus személyi jellegű bizonyítékkal szemben, hiszen meg tudják azokat cáfolni. Természetesen, ez nem jelenti azt, hogy a klasszikus személy-jellegű bizonyítási eszközök eltűnnek, hanem azt, hogy azok értékét egy-egy digitális bizonyíték cáfolni, támogatni tudja. Ebben egyetértek Fenyvesi Csabával, ahogyan ezt a fentebb tárgyaltak során ki is fejttem az általános bizonyítással foglalkozó fejezetben.

6. A Mesterséges Intelligencia terjedésével a digitális képi és hangi bizonyítékok bizonyító ereje kérdésessé válhat. A bíróságnak megfontolás tárgyává kell tenniük az igazságügyi informatikus szakértő kirendelését minden olyan esetben, ahol a terhelt tagadja a felvétel valódiságát. A "látni annyi, mint hinni" elvét felváltja a "látni annyi, mint gyanakodni" elve, ami drasztikusan lassíthatja a bizonyítási eljárást, holott a Be. megszületésének egyik indoka a büntetőeljárás hatékonyabbá és gyorsabbá tétele volt. Ehhez kapcsolódhat az, hogy a rendőrség egyre gyakrabban használ olyan szoftvereket, amelyek arcfelismeréssel vagy mozgásmintázat-elemzéssel azonosítják az elkövetőt. Ha egy algoritmus jelöli meg a terheltet, a Be. szerint ez önmagában nem lehet bizonyíték, csak "adatgyűjtés eredménye". Ezen eredmények elfogadhatóvá tételéhez a jövőben nem egy hagyományos szakértőre lesz szükség, hanem a szoftver forráskódjának és tanítási adatainak "kihallgatására". Ez új eljárási jogi kategóriát teremthet: az algoritmus nem tanú és nem is tárgyi bizonyíték, hanem egy sajátos, "technológiai vélemény", amelynek ellenőrizhetőség a tisztességes eljárás alapfeltételévé válik.

¹² FENYVESI Csaba (2016): A felismerésre bemutatás és a digitális adatok jelentősége egy szeméremértő bűncselekmény tükrében, In.: Belügyi Szemle, 2016/9., 121–122.

¹³ FENYVESI Csaba (2016): *i.m.*, 119.

Látni annyi, mint gyanakodni? A válasz: igen. A másik oldalról az ilyen jellegű veszélyek jelentőségét mutatja, hogy az interneten számtalan oldal található arra vonatkozóan, amely abban segít, hogy felismerjük, az előttünk lévő fénykép-, videó-, avagy hangfelvétel nem eredeti.¹⁴ Sőt, vannak olyan internetes oldalak, amelyekkel az MI segítségét lehet kérni abban, az általunk feltöltött kép MI-generált-e.¹⁵

A probléma megoldása sürgető hiszen egy tanulmány rámutatott, hogy a kutatási eredmények feltárják, hogy a kognitív torzítások jelentős szerepet játszanak az MI által gejerált képek megtévesztő erejének felerősítésében, elősegítve a felhasználók bizalmát a fabrikált tartalmak iránt.¹⁶

A digitális bizonyítékok kapcsán nem csupán azok megismerése jelentős, hanem az a kérdés is, hogy adott bizonyíték eredetinek tekinthető-e. Az gondolom, a mesterséges intelligencia korában az ezzel kapcsolatos aggályok nem eltűntek, ha pl. a deepfake technikára gondolunk. A tisztességes eljáráshoz fűződő jog pedig nyilvánvalóan megköveteli a bizonyítás törvényességére vonatkozó szabályok betartását.

A deepfake – magyarra fordítva: „mélyhamisítás” – teljesen vagy részben kitalált vagy egy meglévő, valós tartalom manipulálásával létrehozott videó, hang vagy egyéb tartalom. A deepfake veszélyeként azonosítják, hogy megjelenésével megkérdőjeleződik a valóságba vetett bizalom. A deepfake számos módon bekerülhet a bizonyításba. Könnyen elképzelhető, hogy maga a bizonyítékot előterjesztő hozza létre szándékosan, az is előfordulhat, hogy a más által hamisított bizonyítékot terjeszti be, tudva annak hamis voltáról, de megtörténhet az is, hogy ő maga sem tud róla, mert őt is megtéveszti a manipuláció.¹⁷

Ha belegondolunk abba, hogy a deepfake révén egy ember arca, hangja, de még a mozgása is újrateheremthetővé válik, azaz az arca kicserélhető, animálható, akkor rájövünk a technológia a

¹⁴ 8 jel, amiből felismerheti, ha egy kép AI-kamu. (https://hvg.hu/tudomany/20260318_mesterseges-intelligenciaval-keszített-hamis-fotok-felismerese-felvezetes-kutatas-kozossegi-media) (Letöltés ideje: 2026. 04. 19.)

¹⁵ <https://quillbot.com/ai-image-detector>

¹⁶ Márk MISKOLCZI (2026) The illusion of reality: How AI-generated images (AIGIs) are fooling social media users. In: Computers in Human Behavior, V. 176, 2026., 1-15.

¹⁷ HERKE Csongor (2024): A bizonyítékok újraértékelése: a deepfake technológia hatása a büntető igazságszolgáltatásra, Magyar Jog, 2024/6., 331.

bizonyításra nézve valóban komoly veszélyt hordoz, hiszen összemossa a valóságot a fikcióval.¹⁸

Hogyan kerülhető el, hogy a deepfake által létrehozott hamis, avagy hamisított bizonyítékok beszivároghatva egy-egy büntetőeljárás bizonyítási eljárásába teljes mértékben tévútra vigyék azt? Mindenképp hangsúlyozandó, hogy a jelenleg létező kép- és hangimitációk jellemzően kiforratlanok, azaz az esetek többségében egyszerű körütekintés keretében megállapíthatók azok nem valós volta, de a robbanásszerű fejlődésnek köszönhetően ez a közeljövőben változhat.¹⁹

A digitális bizonyítékok számos formában ölthetnek testet, ami a büntetőeljárásban történő megjelenést illeti. Egyetértek Tóth Marcell szerzővel abban, hogy azokban az esetekben, ahol a büntetőeljáráson belül nagyobb hangsúlyt kap a digitális technológia, a digitális bizonyítékokat, az információs rendszert érintő eljárási cselekmények tekintetében indokolt lehet az igazságügyi informatikai szakértő igénybevétele. A Digital Forensic Science – a bűnügyi informatika egy rövid múlttal rendelkező bűnügyi segédtudomány, amelynek feladata a bizonyítékok hiteles összegyűjtése, elemzése és bemutatása.²⁰

A digitális szakértés lényegi része abban ragadható meg, hogy a számítógépes rendszerek betekintést engednek a múltba. A szakértő elő tud hívni korábbi e-maileket, chatüzeneteket. Ezen adatok felfedhetik az elkövető motivációit, amelyek a bűncselekmény elkövetésére sarkallták. Amíg egy kamera megmutat harminc képet, addig egy szakértő képes lehet további többszáz törlésre került elemet előhívni.²¹

A manipulált bizonyítékok kapcsán ki kell emelni, hogy azok kapcsán nem csupán az igazságügyi informatikus szakértőnek van jelentősége, hanem az igazságügyi nyelvész szakértőnek is. Ebben a tekintetben visszaalakok a lehallgatási anyagok kapcsán arra, hogy az elsődleges forrás a hanganyag, nem annak leírata. Erre vonatkozóan pedig a digitális bizonyítékok szakértői elemzése során foglalkoztam, ahol volt szerencsém feltenni néhány kérdést Ránki Sára igazságügyi nyelvészszakértőnek.

¹⁸ NYITRAI Endre (2025): Digitális adatok és a modern technikai eszközök jelentősége a kriminalisztikában. A deepfake és a fake news jelenségek, Ludovika Egyetemi Kiadó, Budapest, 2025., 131.

¹⁹ TÓTH Marcell (2024): A digitalizáció egyes kihívásai a büntetőeljárásban, Belügyi Szemle, 2024/2., 201.

²⁰ TÓTH Marcell: *i.m.*, 201.

²¹ GARFINKEL Simon L. (2013): *Digital Forensics*, *American Scientist*, 2013/September–October, 370–377.

III. Záró gondolatok

Zárásul megállapítható, hogy a büntetőeljárás digitális átalakulása nem tekinthető lezárt folyamatnak, sokkal inkább egy állandóan változó, dinamikus kölcsönhatásnak a jog és a technológia között. A kutatásom célja nem volt más, mint ezen interakciók feltérképezése és azoknak a dogmatikai alapoknak a lefektetése, amelyek lehetővé teszik a büntetőeljárás számára, hogy megőrizze alapvető funkcióját: az igazság kiderítését egy olyan világban, ahol az igazság sokszor bitekben és algoritmusokban ölt testet.

Az elektronikus adat helye a jogrendszerben immár nem csupán elméleti kérdés, hanem a jogállami büntetőeljárás egyik legfontosabb sarokköve, amelynek szabályozása nem tűrt halasztást, és amely a jogtudomány minden szegmensét – az eljárásjogtól a kriminalisztikán át a technológiai jogig – komoly interdiszciplináris feladat elé állítja. A vizsgálatom tehát nem ért véget a jogszabályok elemzésével, hanem egy olyan gondolkodásmód alapozására törekedett, amely a technológiai semlegesség és a garanciális védelem egyensúlyát keresi a jövő büntetőoperében, ahol a valóság megismerése már elválaszthatatlan a digitális bizonyítékok megbízható és etikus kezelésétől.

Ebben a szellemben kívánom lezárni az értekezést, miután választ adtam a dolgozat elején feltett kérdésekre, és egy olyan jövőképet vázoltam fel, amelyben a büntetőeljárás a technológia adta lehetőségeket kihasználva, de a tisztességes eljárás alapelveit szem előtt tartva képes marad az igazság maradéktalan feltárására.

A kutatás során szerzett tapasztalatok, a gyakorlati esetek és az elméleti összefüggések együttes vizsgálata alapján remélhetőleg sikerült olyan szempontokat megfogalmazom, amelyek elősegítik az elektronikus adat büntetőeljárási szerepének tisztázását és az MI okozta kihívások jogi kezelését, biztosítva ezzel, hogy a büntetőeljárás a 21. században is méltó maradjon az igazság kutatásának nemes feladatához, és ne váljon az elszemélytelenedő technológia passzív eszközévé, hanem megőrizze emberközpontú, garanciális jellegét.

Hangsúlyozom, hogy a dolgozat utolsó fejezetében nem csupán összegezni kívántam az elmondottakat, hanem egyfajta elemzést kívántam adni, amely a dogmatikai alapvetésektől a gyakorlati megvalósításig terjed, és amelyben a jogszabályok, a bírói gyakorlat és a technológiai lehetőségek kölcsönhatásait vizsgálva kerestem azokat a válaszokat, amelyek a

büntetőeljárás hitelességét és hatékonyságát a digitális korban is garantálják. A digitális bizonyítékok és az MI kihívásaival szembenézve a büntetőeljárás nem tehet mást, mint hogy folyamatosan reflektál önmagára, és újragondolja azokat az eljárási formákat, amelyek az igazság megállapítását szolgálják, biztosítva ezzel a tisztességes eljárás érvényesülését minden körülmények között.



Nyilvántartási szám: DEENK/525/2026.PL
Tárgy: PhD Publikációs Lista

Jelölt: Bodnár András Péter
Doktori Iskola: Marton Géza Állam- és Jogtudományi Doktori Iskola
MTMT azonosító: 10076126

A PhD értekezés alapjául szolgáló közlemények

Folyóiratcikkek, tanulmányok (7)

1. **Bodnár, A. P.:** A digitális bizonyítékok bírósági értékelése.
Debreceni jogi műhely : évkönyv. 22 (3-4), 1-19, 2026. ISSN: 1787-775X.
DOI: <http://dx.doi.org/10.24169/DJM/2025/3-4/1>
MTA Állam- és Jogtudományi Bizottság: B
2. **Bodnár, A. P.:** Bitektől a bizonyításig: a tisztességes eljáráshoz való jog a digitális bizonyítékok tükrében = From Accusation to Proof: The Right to a Fair Trial in the Light of Digital Evidence.
Pro futuro. 15 (2), 1-14, 2026. ISSN: 2063-1987.
DOI: <http://dx.doi.org/10.26521/profuturo/2025/2/16621>
MTA Állam- és Jogtudományi Bizottság: A
3. **Bodnár, A. P.:** A digitális bizonyítékok megjelenése a büntetőeljárásban: különös tekintettel a szakértő igénybevételére.
Büntetőjogi Szemle. 2022 (1), 19-29, 2022. ISSN: 2063-8183.
MTA Állam- és Jogtudományi Bizottság: C
4. **Bodnár, A. P.:** A bizonyítási eszközök fejlődése Finkeytől napjainkig.
Erdélyi Jogélet. 2 (1), 25-34, 2021. ISSN: 2734-6226.
DOI: <http://dx.doi.org/10.47745/ERJOG.2021.01.03>
MTA Állam- és Jogtudományi Bizottság: B
5. **Bodnár, A. P.:** Appearance of constitutional constraints in the taking of evidence in criminal proceedings: issue of unlawful evidence.
The Journal of the Faculty of Law Oradea. 2021 (1), 79-85, 2021. ISSN: 1582-7585.
6. **Bodnár, A. P.:** Digitalizáció a büntetőeljárásban: különös tekintettel a nyomozás és a bizonyítás szabályaira.
In: A jog tudománya, a mindennapok joga V. Konferenciakötet. Szerk.: Szűcs Lászlóné Siska Katalin, Talabos Dávidné Lukács Nikolett, Debreceni Egyetem Állam- és Jogtudományi Kar, Debrecen, 63-71, 2021.





**DEBRECENI
EGYETEM**

**DEBRECENI EGYETEM
EGYETEMI ÉS NEMZETI KÖNYVTÁR**

H-4002 Debrecen, Egyetem tér 1, Pf.: 400
Tel.: 52/410-443, e-mail: publikaciok@lib.unideb.hu

7. **Bodnár, A. P.:** Digitization in criminal proceedings: issues related to electronic data.

Büntetőjogi Szemle. 2021 (klsz.), 12-15, 2021. ISSN: 2063-8183.

MTA Állam- és Jogtudományi Bizottság: C

További közlemények

Folyóiratcikkek, tanulmányok (1)

8. **Bodnár, A. P.:** Ünnepnaptól gyásznaptól: a vadászattal összefüggésben álló bűncselekmények.

In: Szakkollégiumi almanach 2018- A Praetor Szakkollégium Büntető Eljárásjogi Műhelyének

Tanulmánykötete. Szerk.: Szabó Krisztián, Printart-Press Kft., Debrecen, 30-49, 2026.

MTA Állam- és Jogtudományi Bizottsága irányelvei szerint:

„A” kategóriás folyóiratban megjelent publikációk: 1, melyek közül az értekezés alapjául szolgál: 1

„B” kategóriás folyóiratban megjelent publikációk: 2, melyek közül az értekezés alapjául szolgál: 2

„C” kategóriás folyóiratban megjelent publikációk: 2, melyek közül az értekezés alapjául szolgál: 2

A DEENK a Jelölt által a Tudóstérbe feltöltött adatok bibliográfiai és tudományometriai ellenőrzését a tudományos adatbázisok és a Journal Citation Reports Impact Factor lista alapján elvégezte.

Debrecen, 2026.08.18.



I. Subject and Objectives of the Doctoral Dissertation, Research Methods, and Structure of the Dissertation

I/1. Rationale and Relevance of the Topic

My doctoral dissertation deals with electronic data as a new means of evidence and examines its theoretical and doctrinal background. To preempt any assumption that this is yet another research study dissecting the issue of evidence—one that merely adds another work to an already extensive body of literature—I wish to state in advance that my study does not deal with evidence in general or with a specific means of evidence in connection with it. I will extend the focus of this study to areas related—though not necessarily closely—to new evidence. As a first step, I will address the general rules of proof, which are essential for me to provide answers to some of my hypotheses from a doctrinal perspective.

Act XC of 2017 on Criminal Procedure (hereinafter: the Criminal Procedure Act), which entered into force on July 1, 2018, expanded the provisions of the previously effective Act XIX of 1998 (hereinafter: the 1998 CPC) regarding means of evidence. The CPC now explicitly recognizes electronic data as an independent means of evidence in Section 165 (f).

To answer the question of why it was necessary to regulate electronic data separately, we could easily cite the ministerial explanatory memorandum to the CPC, which states: “One of the express objectives of the law is to establish criminal proceedings capable of responding to the challenges of the future. The definition of this new means of evidence is therefore not an end in itself; procedural acts governing electronic data—such as the special rules for seizure—are based on it.”²²

The situation, however, is more nuanced than that. According to Erika Róth, the decision to regulate it as a separate, new type of evidence stems from the fact that the legislature—and especially those applying the law—could not decide how to handle this type of evidence. This means that in many cases, the rules governing physical evidence—which are already routinely applied—could not really be applied to the acquisition and preservation of such evidence. A further problem was the lack of a comprehensive definition of “electronic data,” as well as the

²² T/19972. számú törvényjavaslat a büntetőeljárásról szóló törvény 165. §-ához.

lack of clarity regarding when the seizure of an entire data storage medium could be justified to obtain specific data, and when and under what procedural rules such data seizure could take place. The fact that this issue remained unresolved raised concerns not only from a practical standpoint but also from the perspectives of necessity and proportionality, thereby raising constitutional concerns as well. From the above, one might therefore conclude that the goal was not to “separate” electronic data as such; rather, it was merely a means to more precisely regulate specific procedural acts and coercive measures.²³

Related to the above is the fact that, according to the definition in the Code of Criminal Procedure, the definition of this new means of evidence reads as follows: “Electronic data is the representation of facts, information, or concepts in any form suitable for processing by an information system, including any program that ensures the execution of a function by the information system.”²⁴ The Code further adds: “Where this Act refers to ‘evidence,’ such reference shall be understood to include ‘electronic data’ as well, unless otherwise provided by this Act.”²⁵

The Code of Civil Procedure defines the concept of electronic data, but it also stipulates that wherever the law refers to a material means of evidence, electronic data shall also be understood to be included, unless the law provides otherwise. With this addition, the law itself raised the question: can this means of evidence truly be considered new?

My research was partly motivated by practical experience. Early in my research, first as a law clerk and later as an independent attorney acting as defense counsel in criminal proceedings, I quickly realized that, given Hungary’s high conviction rate, a defense attorney can only achieve success if they have a thorough understanding of the details of procedural law. In this context, the evidentiary process is of immense importance.

The evidentiary process is, without a doubt, the cornerstone of criminal proceedings, upon which the success of any given charge stands or falls. In this regard, knowledge of the legal framework underlying a given means of evidence is of paramount importance. If a legal rule

²³ RÓTH Erika: *Az elektronikus adat, mint új bizonyítási eszköz megjelenése az új büntetőeljárási törvényben.* in.: Miskolci Jogi Szemle, 2019/2., 347-348.

²⁴ A büntetőeljárásról szóló 2017. évi XC. törvény 205. § (1) bek.

²⁵ A büntetőeljárásról szóló 2017. évi XC. törvény 205. § (2) bek.

does not provide a clear answer to a situation that arises in practice—that is, if it leaves room for differing conclusions and decisions—this results in uncertainty, which may violate the right to a fair trial and, ultimately, may even jeopardize one of the goals of criminal proceedings: the pursuit of justice.

The aim of my research is therefore to provide answers not only to specific questions arising in connection with electronic data but also to issues such as the fundamental right to a fair trial, expert evidence, judicial conviction, and the challenges posed by Artificial Intelligence to the proceedings. To summarize, I am seeking to answer how the theory of evidence—built on theoretical foundations established decades ago—responds to the digital reality of the 21st century.

The goal, therefore, is to determine the place of electronic data within the legal system; in doing so, it is necessary to clarify questions such as exactly what we consider to be electronic data in criminal proceedings. Furthermore, is electronic data a *sui generis* means of evidence, or merely a subcategory of physical evidence? How can its authenticity and integrity be guaranteed—that is, what assurance is there that the electronic data has remained unchanged from its creation until its evaluation by the court—and where does the scope of expert testimony begin, or how far may the judge go in evaluating the data? Of course, in answering the above questions, I cannot overlook the need to examine the international context, particularly the solutions adopted in the Anglo-Saxon legal system overseas, as well as the methods applied by states that follow the European, civil law system.

I/2. Structure of the Dissertation and Methodological Foundations

I extend the focus of this study to areas related — though not necessarily closely — to new evidence. As a first step, I address the general rules of evidence, which are essential for providing answers to some of my hypotheses from a doctrinal perspective. To achieve the above objectives, in addition to the sections analyzing the history of evidence, it is also necessary to address other fundamental issues, such as the right to a fair trial, the fundamental principles of evidence, expert testimony, judicial conviction, and the challenges posed by artificial intelligence in criminal proceedings. Beyond the current statutory framework, when discussing issues where it is relevant, I will examine case law through a review of case files, in which context an analysis of the case law of the European Court of Human Rights (hereinafter:

ECtHR) and the Court of Justice of the European Union (hereinafter: CJEU) cannot be overlooked.

I classify my research primarily as applied research, in which the deductive method takes center stage from a dogmatic perspective. In addition to key theoretical questions, however, empirical methods from the social sciences are also employed.

The fact that I am a practicing attorney has a significant influence on the methodology of my research; thus, my research is, to some extent, based on my own experience. It is evident that the rules of evidence have undergone numerous changes throughout the history of law, which I will discuss in the chapter on general rules of evidence. In addition to domestic case law, the decisions of the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU) in specific cases are also significant in the process of arriving at the results of this scholarly research. In addition to reviewing and analyzing domestic scholarship, my dissertation does not overlook international scholarship, nor does it neglect to provide a comparative analysis of it in some instances.

In this work, which presents the results of my research, I examine—whether from a theoretical or practical perspective—whether differences in practice regarding issues involving electronic data can or should be addressed through legislative amendments. It is no secret that my goal is to make recommendations if, based on the research findings, I find that current practices can, should, or need to be improved or changed.

In the introduction to this thesis, I outline the foundations of the research, certain propositions, and the methods of my research. In addition to outlining the research topic, the areas of research, and the reasons for and objectives of the research itself, I also discuss my hypotheses, which this thesis aims to address.

I/3. Hypotheses and Research Questions

1. Electronic data has not merely become an independent means of evidence in name only; from a doctrinal perspective, it can also be regarded as a new means of evidence. By defining in Section 205 of the Civil Procedure Code exactly what is meant by “electronic data,” the Code effectively excludes it from the scope of tangible evidence and treats it as an independent means

of evidence. This is implied by the rationale for the *sui generis* regulation itself, as the rules governing physical evidence were not always applicable to this type of data in the past.

2. The principle of purpose limitation may be violated during the seizure of electronic data, given that, in the course of executing the coercive measure, access to data unrelated to the criminal offense is inevitably obtained.

3. Disclosing electronic data to the defense counsel or the defendant in a form other than the original may violate the right to a fair trial. In cases where such evidence is significant, the defense and the defendant must be allowed to review the evidence in its original form. An example of this is the results obtained through the use of covert devices. It is not sufficient to provide the defendant with a written transcript of the wiretap; the defendant must be given the opportunity to review the recordings in their original form. If the defendant is in custody, the necessary technical conditions must also be provided; otherwise, the defendant's right to a fair trial is violated.

4. In criminal proceedings, the authenticity of electronic data is difficult to ascertain; thus, the value of evidence derived from such data is based not on the data's authenticity but on the process verifying its integrity. In the case of electronic data, the existence of a closed chain of evidence is insufficient if the circumstances of access to the source device are not adequately documented.

5. Electronic data demonstrate greater validity than traditional personal forms of evidence. Due to their objectivity, electronic data are suitable for refuting or corroborating a statement—e.g., a witness testimony.

6. With the spread of Artificial Intelligence, the probative value of digital visual and audio evidence may become questionable. Courts must consider appointing a forensic computer expert in all cases where the defendant denies the authenticity of the recording. The principle of "seeing is believing" is being replaced by the principle of "seeing is suspecting," which could drastically slow down the evidentiary process, even though one of the reasons for the enactment of the Criminal Procedure Code was to make criminal proceedings more efficient and faster.

Related to this is the fact that the police are increasingly using software that identifies perpetrators through facial recognition or movement pattern analysis. If an algorithm identifies the accused, under the Criminal Procedure Code this cannot in itself constitute evidence, but is merely the “result of data collection.” In the future, for these results to be deemed admissible, it will not be necessary to rely on a traditional expert, but rather to “examine” the software’s source code and training data. This may create a new category in procedural law: the algorithm is neither a witness nor physical evidence, but rather a specific “technological opinion,” the verifiability of which becomes a fundamental prerequisite for due process.

II. Conclusion: Verification of the Hypotheses

The objective of this doctoral dissertation was to explore the fundamental changes brought about by the emergence of electronic data as a new means of evidence and the application of AI technologies in criminal proceedings. In the course of this study, we reviewed the historical development of the evidentiary process, moving from the classical foundations of evidentiary theory in the 19th century to the digitized reality of the 21st century. In the course of this process, it became evident that electronic data is not merely another technical item on the list of evidence, but a paradigm-shifting force that fundamentally challenges the centuries-old dogmatic structures surrounding physical evidence. The case file research conducted during the study and the analysis of domestic and international legal practice highlighted the tension that exists between the intent of the legislature—such as the goal of creating more efficient and faster proceedings—and judicial practice, as well as the enforcement of guarantees of the right to a fair trial.

The evidentiary process is the cornerstone of our criminal proceedings, upon which both the discovery of the substantive truth and the success of the prosecution depend. The central thesis of this dissertation—that treating electronic data as an independent means of evidence is justified from a doctrinal perspective—has been confirmed. Although the current law, the Criminal Procedure Code, attempts to define the concept of electronic data, in practice, courts and investigative authorities often fall back on the routinely applied rules governing physical evidence. However, this “regression” raises constitutional concerns due to the unique nature of digital evidence. In the case of physical evidence, the ability to physically touch and directly perceive the evidence forms the basis of its reliability, whereas in the case of electronic data, authenticity and integrity are the factors on which the probative value stands or falls. Thus,

rather than the question of the data's origin, the chain of custody has become the key issue in its evaluation.

Through our theoretical and practical examination, we have highlighted that the higher validity of digital evidence—which can either challenge or confirm testimony-based personal evidence—contributes to the objectivity of criminal proceedings. At the same time—and this is one of the most important findings of this dissertation—the classic principle of “seeing is believing” in the digital world, particularly with the emergence of AI-based tools, is shifting toward the principle of “seeing is suspecting.” This shift in perspective also places the principle of judicial discretion in a new context. The court, as the body responsible for applying the law, is compelled to accept the opinion of the IT expert without technical scrutiny or criticism. As a result, judicial discretion effectively becomes expert decision-making, which may undermine judicial independence and the right to a fair trial if the expert opinion functions as a “black box.”

The growing use of AI in criminal proceedings—such as the application of facial recognition software—raises the need for new categories of procedural law. Under the current regulatory framework, an algorithm is neither a witness nor physical evidence, but rather electronic data; its verifiability—that is, the examination of its source code and training data—becomes an indispensable condition for a fair trial. If criminal proceedings fail to keep pace with technological advancements, the evidentiary process may degenerate into a venue for accepting realities generated by algorithms, rather than a pursuit of the truth.

Therefore, it is essential to strengthen the system of safeguards that ensures the accused's right to access technology-based evidence, with particular regard to access to the original format and to technical aids, even while subject to coercive measures within the confines of a correctional facility.

The place of electronic data within the legal system is no longer merely a theoretical question but one of the most important cornerstones of criminal proceedings under the rule of law; its regulation could not be postponed and presents every segment of legal scholarship—from procedural law through forensic science to technology law—with a significant interdisciplinary challenge. My study, therefore, did not end with the analysis of legislation but sought to lay the foundation for a way of thinking that seeks a balance between technological neutrality and the

protection of due process in the criminal trials of the future, where ascertaining the truth is now inseparable from the reliable and ethical handling of digital evidence.

It is in this spirit that I wish to conclude this dissertation, having answered the questions posed at the beginning of the thesis and outlined a vision of the future in which criminal proceedings, while taking advantage of the opportunities offered by technology and keeping the fundamental principles of due process in mind, remain capable of fully uncovering the truth.

Based on the experiences gained during my research and a combined examination of practical cases and theoretical contexts, I hope to have successfully articulated perspectives that will help clarify the role of electronic data in criminal proceedings and address the legal challenges posed by AI, thereby ensuring that criminal proceedings in the 21st century remain worthy of the noble task of seeking justice and do not become a passive tool of depersonalizing technology, but rather preserve their human-centered, rights-protecting nature.

1. Electronic data has not merely become an independent means of evidence in name only; it can also be regarded as a new means of evidence from a doctrinal perspective. By defining in Section 205 of the Civil Procedure Code exactly what is meant by “electronic data,” the Code effectively excludes it from the scope of “objective evidence” and treats it as an independent means of evidence. This is suggested by the rationale for the sui generis regulation itself, as the rules governing physical evidence were not always applicable to this type of data in the past.

The regulation of electronic data as a new form of evidence stems from the fact that the legislature—and, above all, those applying the law—were unable to decide how to handle this type of evidence. This means that, in some cases, the rules governing physical evidence—which had already been routinely applied—could not really be applied to the acquisition and preservation of such data. A further problem was the lack of a comprehensive definition of “electronic data,” as well as the lack of clarity regarding when the seizure of an entire data storage medium could be justified to obtain specific data, and when and under what procedural rules such data seizure could take place. The fact that this issue remained unresolved raised concerns not only from a practical standpoint but also from the perspectives of necessity and proportionality, thereby raising constitutional concerns as well. From the above, one might therefore conclude that the goal was not the “separation” of electronic data per se, but rather

that it was merely a means to more precisely regulate specific procedural acts and coercive measures.²⁶

It is a fact that an essential part of the concept of evidence is that the information be obtained from a source authorized by law, and thus serve as a means of proof. With regard to digital evidence, however, this identification of the source is not so clear-cut. In the case of digital data, two paths emerge concerning its source. The first possible path is that the source of digital evidence is always a physical object that carries the data containing the evidence—be it an image, video, or text file. According to the other possible approach, the source of the evidence is the data stored electronically—such as image, video, or text files, etc.—since the authorities extract the relevant information directly from it; the hardware serves merely as a storage medium, just as a cabinet does in the case of physical evidence.²⁷

In the former case, digital evidence is always carried by physical evidence devices capable of recording, storing, and transmitting data in electronic form. Such devices may include desktop computers, laptops, phones, tablets, printers, etc. In the latter case, therefore, the source of evidence is the data itself, since the authorities obtain the information directly from it, and the medium merely serves as a “cabinet.”

In my view, the above arguments are acceptable; I agree with them in every respect, and I can state that electronic data can be considered a new form of evidence in criminal proceedings.

2. Under the previous law, the principle of purpose limitation could have been violated during the seizure of electronic data, given that, in the course of carrying out the coercive measure, access to data unrelated to the criminal offense was inevitably obtained.

In my view, this assertion has been substantiated. Under the previous law, there were disputes regarding exactly what needed to be seized—that is, whether it was a specific set of data, the data storage medium, or the entire IT system. For example, prior to the entry into force of Act CLXXXVI of 2013, which amended the previous procedural law, it was standard practice to seize the entire information system, including devices irrelevant to the criminal proceedings,

²⁶ lsd. RÓTH Erika (2019): *i.m.*, 347-348.

²⁷ SORBÁN Kinga: *A digitális bizonyíték a büntetőeljárásban*. In.: Belügyi Szemle, 2016/11.

such as a mouse or a keyboard.²⁸ By seizing the entire computer system, data that had nothing to do with the criminal proceedings also ended up in the hands of the authorities.

As with other forms of evidence, legality, professionalism, and the existence of an unbroken chain of evidence are crucial when it comes to electronic data. Three fundamental criteria must be met during the investigative phase: the original data must not be damaged or altered when the evidence is obtained; its conformity with the original must be verifiable; and the analysis of the evidence must not alter it. At the same time, the Criminal Procedure Code introduced a system of coercive measures based on electronic data, including the seizure of electronic data (Section 315 of the Criminal Procedure Code), the obligation to preserve such data (Section 316 of the Criminal Procedure Code), and the temporary restriction of access to it (Section 335 of the Criminal Procedure Code). The new Code has made substantive changes to the rules governing seizure.²⁹

Pursuant to Section 151(1) of the Criminal Procedure Code, the purpose of seizure is to secure evidence, as well as items subject to forfeiture or property subject to confiscation, in order to ensure the effective conduct of criminal proceedings. This coercive measure restricts ownership rights over electronic data and may be ordered by the court, the prosecutor's office, or the investigating authority. This legal institution plays a key role in the investigation of cybercrimes as a means of obtaining and preserving electronic evidence. There has long been debate over exactly what should be seized during the proceedings—namely, whether it should be the specified data, the data storage medium, or the entire information system. It is worth noting that the seizure of data was first incorporated into the 1998 Criminal Procedure Code by Section 21 of Act CLXXXVI of 2013. Prior to this, it was standard practice to seize the entire computer (e.g., often along with hardware devices irrelevant to the criminal proceedings, such as the monitor and keyboard); later, only the hard drive—or sometimes not even that—was seized, and only a copy was made of it; and following the amendment, only the data itself was seized.³⁰

3. Disclosing electronic data to the defense counsel or the defendant in a form other than the original may violate the right to a fair trial. In cases involving evidence of this nature,

²⁸ BODNÁR András Péter: A digitális adatok megjelenése a büntetőeljárásban – különös tekintettel a szakértő igénybevételére. In.: Büntetőjogi Szemle, 2022/1., 22-23.

²⁹ MEZEI Kitti: Az elektronikus bizonyítékokkal kapcsolatos kihívások és szabályozási újdonságok. In.: Belügyi Szemle, 2019/10., 27-28.

³⁰ MEZEI Kitti: *i.m.*, 27-28.

where such disclosure is significant, the defense and the defendant must be allowed to review the evidence in its original form. An example of this is the results of the use of covert devices. It is not sufficient to provide the defendant with a written transcript of the wiretap; the defendant must be given the opportunity to review the recordings in their original form. If the defendant is in custody, the necessary technical conditions must also be provided; otherwise, the right to a fair trial is violated.

In my view, in cases where digital evidence—specifically audio recordings—is of significant importance and the defendant does not receive the digital material, their right to a fair trial may be violated. A good example of this is that covert devices may be used in cases of intentional crimes punishable by imprisonment of up to five years³¹ or a more severe sentence, which makes it a realistic possibility that the most severe coercive measures could be applied against the defendant. The question, then, is whether access to wiretap recordings in written form violates the right to a fair trial, and thus—for example—whether correctional facilities must ensure that the defendant is allowed to listen to the wiretap recordings. In my view, this is a significant issue, since it is particularly true of wiretap recordings that—depending on intonation and context—the same words spoken aloud can convey a different meaning than when written down.

A prime example of this—beyond the requirement for a forensic linguistics expert—is the Debrecen Court of Appeals’ judgment No. Bf.III.372/2024/32, in which the Court pointed out that video recordings—in light of the paradigm shift, as electronic data, digital evidence—can more easily dispel doubts regarding a statement recorded on paper—typed by an investigative official—especially when we consider that what is spoken does not always match what is written. The Szeged Court of Appeals also recognized the significance of this. Another example is Decision No. ÍH2018. 130 of the Szeged Court of Appeals. The Court of Appeals pointed out that a request by the defendant for the issuance of an electronic copy of all documents generated in electronic form in a criminal case—a request that has been repeatedly submitted—cannot be denied. The issuance of additional copies must be authorized upon payment of the applicable fee. Its content can be summarized as follows:

³¹ 2017. évi XC. törvény a büntetőeljárásról 234. § (1) bekezdés.

This case-specific decision is of decisive importance in terms of the dogmatic reinterpretation of the legal institution of access to criminal proceedings documents—in line with the expectations of the digital age. The decision examines the regulatory framework governing access to electronic data generated during criminal proceedings and to the contents of seized data storage media, with particular regard to the challenges of applying the law during the transitional period between the former and current Criminal Procedure Acts.

The essence of the legal dispute underlying the proceedings was the convicted person's request for a duplicate copy, which sought to reproduce electronic evidence generated during the criminal proceedings and stored on seized data storage devices. The trial court based its decision to deny the request on Section 70/B(10) of the 1998 Criminal Procedure Code and on the principle that the production of copies is to be performed only once, framing the issue semantically within the concepts of “res judicata” and “fulfillment of the service.” In contrast, the appellate court—in the appeal proceedings—examined the issue in light of the right to a defense and the rules guaranteeing access to documents, clearly distinguishing the absolute right to access information from the service-oriented nature of making copies onto a data storage medium, which requires technical reproduction.

One of the most important legal principles in the decision is the distinction between access to case files and the making of copies. The court held that while the defendant's right to access case files is of fundamental importance, the making of copies—particularly when it requires the physical reproduction of large volumes of data stored on electronic media—can no longer be considered an unrestricted element of procedural rights granted as a matter of law. The exemption from fees provided by the legislature applies to the first copy requested, which is intended to ensure the exercise of the right to a defense. Subsequent requests for additional copies no longer concern a violation of fundamental rights in criminal proceedings but rather the use of technical resources; thus, pursuant to the provisions of Act XCIII of 1990 on Fees, such requests may be granted upon payment of the applicable fees.

The court's reasoning is of particular significance in the context of handling electronic evidence, as it highlights the legal dilemma that the inherent reproducibility of digital data does not override the need for the rational administration of criminal proceedings. The decision implicitly acknowledges the unique characteristics of digital evidence: the duality of the data storage medium (hardware) and the content stored on it (data). In doing so, the court establishes

a kind of cost-effective procedural balance, whereby the state ensures access to the evidence at the outset of the proceedings but confines further, repetitive requests within the framework of procedural and budgetary discipline. The appellate court's ruling corrected the reasoning of the first-instance order on this point: instead of denying the motion, it ordered that the request be granted, but with a clear stipulation regarding the allocation of costs

4. In criminal proceedings, the authenticity of electronic data is difficult to interpret; thus, the value of evidence derived from such a medium is based not on the authenticity of the data itself, but on the process certifying its integrity. In the case of electronic data, the existence of a closed chain of evidence is insufficient if the circumstances of access to the source medium are not adequately documented.

In my view, this assertion has been substantiated. I have pointed out that, although digital evidence facilitates the establishment of guilt due to its extensive information content, it also poses unique challenges. Its large volume, rapid generation, and susceptibility to manipulation make its authentication complicated. Digital evidence is also subject to various external influences and human factors that can compromise its integrity. Unlike physical evidence, which is straightforward to document, digital evidence requires far more complex procedures. The ease of remote access, the ability to copy files, and user mobility make it difficult to document and preserve digital evidence. Due to the fragile nature of digital evidence, meticulous documentation is required throughout the investigation. Only evidence that remains unchanged and reliable meets the strict criteria for admissibility. Therefore, it is essential—if I may put it this way—to ensure a “chain of custody” for digital evidence as well, which guarantees the integrity and authenticity of the digital evidence throughout the entire criminal proceeding.³²

The essence of the principle I referred to above—which might be summed up as “if you didn’t write it down, it didn’t happen”—faithfully reflects the fundamental need for thorough documentation, given the aforementioned fragile nature of digital evidence. Proper documentation is essential to verify that the evidence presented in court is authentic and free from manipulation. The chain of custody process ensures this by meticulously recording every

³² NATH Souradip–BAEK Jaeojong, Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics, IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, Washington, 2024, 2.

single step of the evidence's "journey" throughout the entire lifecycle of the case. This principle must answer the following questions:

- What? What is the evidence itself?
- How? How was it collected and stored?
- Who? Who took possession of it, and who had control over it?
- When? When was it collected, transferred, or handled?
- Where? Where did the evidence "travel," and where was it stored or examined?
- Why? Why was it necessary to transfer or hand over the evidence?

The chain of custody must include a detailed record of the evidence's handling, including the identifying information of the individuals involved in the examination and analysis, the locations, and the activities performed. This comprehensive documentation preserves the integrity of the evidence and enhances transparency and accountability throughout the forensic process. In legal proceedings, the chain of custody can be of critical importance in supporting expert opinions. When presented in court, the chain of custody verifies the authenticity and integrity of the evidence, thereby corroborating it.

5. Electronic data is more reliable than traditional forms of personal evidence. Due to their objectivity, electronic data can be used to refute or corroborate a statement—such as a witness testimony.

In short: yes. A case from Pécs was presented in which, according to the defendant's testimony, the young man woke up around 9 a.m. on the day in question—at his residence, which was about ten kilometers from the crime scene. His mother left home in her car around 7:00 a.m., while his father had left for work earlier, at 6:00 a.m., also in his own vehicle. According to his recollection, he turned on his computer between 10:30 a.m. and 11:00 a.m. because he needed it to study German, given that he was planning to work in Austria. His cell phone was turned on, but he neither made nor received any calls on it. After finishing his German studies, he called his girlfriend at 12:32 p.m. to arrange a meeting for that day. According to the investigation's findings, the cell phone data showed that the phone registered under the defendant's name remained continuously turned on and was connected to the cell tower closest to his residence throughout the day, right up until the time of departure as stated by the defendant himself. An important piece of evidence provided to the investigating authorities was

that data retrieved from the defendant's computer showed that the computer was turned on at 11:05 a.m. on that day. Given that the report was received by the police at 10:49 a.m., and the cashier stated that the offense had just occurred, the time of the offense was determined to be 10:48 a.m.³³ Contrary to the witness's testimony, on the day after the incident, the suspect's photograph was shown to the witness alongside three others, and the witness was 70 percent certain that the man was the perpetrator. After the investigators covered his forehead, the witness was already 80 percent certain. He became most certain when he was shown the video footage. During a subsequent confrontation, he also positively identified the suspect by his voice.³⁴

In light of the above, it can be said that digital evidence has greater validity than traditional personal evidence, as it can refute such evidence. Of course, this does not mean that traditional personal means of proof will disappear, but rather that the value of such evidence can be either refuted or supported by specific pieces of digital evidence. I agree with Csaba Fenyvesi on this point, as I explained in the chapter on general evidence in the discussion above.

6. With the spread of artificial intelligence, the probative value of digital visual and audio evidence may become questionable. Courts should consider appointing a forensic computer expert in all cases where the defendant denies the authenticity of the recording. The principle of "seeing is believing" is being replaced by the principle of "seeing is suspecting," which could drastically slow down the evidentiary process, even though one of the reasons for the enactment of the Criminal Procedure Code was to make criminal proceedings more efficient and faster. Related to this is the fact that the police are increasingly using software that identifies perpetrators through facial recognition or movement pattern analysis. If an algorithm identifies the accused, under the Criminal Procedure Code this cannot in itself constitute evidence, but is merely the "result of data collection." In the future, for these results to be deemed admissible, it will not be necessary to rely on a traditional expert, but rather to "examine" the software's source code and training data. This could create a new category of procedural law: the algorithm is neither a witness nor physical evidence, but rather a specific "technological opinion," the verifiability of which becomes a fundamental requirement of due process.

³³ FENYVESI Csaba (2016): A felismerésre bemutatás és a digitális adatok jelentősége egy szeméremértő bűncselekmény tükrében, In.: Belügyi Szemle, 2016/9., 121–122.

³⁴ FENYVESI Csaba (2016): *i.m.*, 119.

Is seeing the same as suspecting? The answer: yes. On the other hand, the significance of such risks is illustrated by the fact that there are countless websites on the internet designed to help us recognize when a photograph, video, or audio recording we are viewing is not authentic.³⁵ In fact, there are websites where you can use AI to determine whether an image you've uploaded was generated by AI.³⁶

Solving this problem is urgent, as a study has shown that research findings reveal that cognitive biases play a significant role in amplifying the deceptive power of AI-generated images, thereby fostering users' trust in fabricated content.³⁷

When it comes to digital evidence, it is not only important to understand the evidence itself, but also to determine whether a given piece of evidence can be considered authentic. I believe that in the age of artificial intelligence, concerns in this regard are not exaggerated, especially when we consider techniques such as deepfakes. The right to a fair trial clearly requires compliance with the rules governing the admissibility of evidence.

A deepfake—translated into Hungarian as “deep forgery”—is a video, audio, or other content that is either entirely or partially fabricated or created by manipulating existing, real content. The danger of deepfakes is that their emergence calls into question trust in reality. Deepfakes can enter the evidence chain in numerous ways. It is easy to imagine that the person presenting the evidence creates it intentionally; it is also possible that they submit evidence falsified by someone else, knowing it is fake; but it can also happen that they themselves are unaware of it because they, too, are deceived by the manipulation.³⁸

If we consider that deepfakes make it possible to recreate a person's face, voice, and even movements—that is, to replace or animate their face—we realize that this technology poses a truly serious threat to the integrity of evidence, as it blurs the line between reality and fiction.³⁹

³⁵ 8 jel, amiből felismerheti, ha egy kép AI-kamu. (https://hvg.hu/tudomany/20260318_mesterseges-intelligenciaval-keszitett-hamis-fotok-felismerese-felrevezetes-kutatas-kozossegi-media) (Letöltés ideje: 2026. 04. 19.)

³⁶ <https://quillbot.com/ai-image-detector>

³⁷ Márk MISKOLCZI (2026) The illusion of reality: How AI-generated images (AIGIs) are fooling social media users. In: Computers in Human Behavior, V. 176, 2026., 1-15.

³⁸ HERKE Csongor (2024): A bizonyítékok újraértékelése: a deepfake technológia hatása a büntető igazságszolgáltatásra, Magyar Jog, 2024/6., 331.

³⁹ NYITRAI Endre (2025): Digitális adatok és a modern technikai eszközök jelentősége a kriminalisztikában. A deepfake és a fake news jelenségek, Ludovika Egyetemi Kiadó, Budapest, 2025., 131.

How can we prevent false or fabricated evidence created by deepfakes from infiltrating the evidentiary proceedings of a criminal case and completely derailing them? It must be emphasized that currently existing image and audio imitations are typically crude; that is, in most cases, their inauthenticity can be determined through simple scrutiny. However, due to explosive advancements in the field, this may change in the near future.⁴⁰

Digital evidence can take many forms when it comes to its use in criminal proceedings. I agree with the author, Marcell Tóth, that in cases where digital technology plays a more prominent role in criminal proceedings, it may be justified to engage a forensic IT expert regarding digital evidence and procedural actions involving information systems. Digital Forensic Science—a relatively new auxiliary discipline of criminalistics—is tasked with the authentic collection, analysis, and presentation of evidence.⁴¹

An essential aspect of digital forensics lies in the fact that computer systems provide insight into the past. An expert can retrieve past emails and chat messages. This data can reveal the perpetrator's motivations that drove them to commit the crime. While a camera may show thirty images, an expert may be able to retrieve hundreds more that had been deleted.⁴²

With regard to manipulated evidence, it is important to note that not only the forensic computer expert but also the forensic linguist plays a significant role. In this regard, I refer back to the issue of wiretap recordings, noting that the primary source is the audio recording itself, not its transcript. I addressed this topic during my analysis of digital evidence, where I had the opportunity to ask forensic linguist Sára Ránki a few questions.

III. Concluding Remarks

In conclusion, it can be stated that the digital transformation of criminal proceedings cannot be regarded as a completed process, but rather as a constantly evolving, dynamic interaction between law and technology. The aim of my research was none other than to map out these interactions and lay the doctrinal foundations that enable criminal proceedings to preserve their

⁴⁰ TÓTH Marcell (2024): A digitalizáció egyes kihívásai a büntetőeljárásban, *Belügyi Szemle*, 2024/2., 201.

⁴¹ TÓTH Marcell: *i.m.*, 201.

⁴² GARFINKEL Simon L. (2013): *Digital Forensics*, *American Scientist*, 2013/September–October, 370–377.

fundamental function: the discovery of the truth in a world where truth is often embodied in bits and algorithms.

The place of electronic data within the legal system is no longer merely a theoretical question, but one of the most important cornerstones of criminal proceedings under the rule of law; its regulation could not be postponed, and it presents every segment of legal scholarship—from procedural law through forensic science to technology law—with a serious interdisciplinary challenge. My study, therefore, did not end with the analysis of legislation but sought to lay the foundation for a way of thinking that seeks a balance between technological neutrality and the protection of due process in the criminal trials of the future, where ascertaining the truth is now inseparable from the reliable and ethical handling of digital evidence.

It is in this spirit that I wish to conclude this dissertation, having answered the questions posed at the beginning of the thesis and outlined a vision of the future in which criminal proceedings, while taking advantage of the opportunities offered by technology and keeping the fundamental principles of due process in mind, remain capable of fully uncovering the truth.

Based on the experiences gained during my research and a combined examination of practical cases and theoretical contexts, I hope to have successfully articulated perspectives that will help clarify the role of electronic data in criminal proceedings and address the legal challenges posed by AI, thereby ensuring that criminal proceedings in the 21st century remain worthy of the noble task of seeking the truth, and do not become a passive tool of dehumanizing technology, but rather preserve their human-centered, rights-protecting nature.

I would like to emphasize that in the final chapter of this thesis, I did not merely intend to summarize what has been discussed, but rather to provide a form of analysis ranging from dogmatic fundamentals to practical implementation, in which, by examining the interplay between legislation, judicial practice, and technological possibilities to find answers that guarantee the credibility and effectiveness of criminal proceedings even in the digital age. Faced with the challenges of digital evidence and AI, criminal proceedings have no choice but to continually reflect on themselves and rethink the procedural forms that serve to establish the truth, thereby ensuring that due process is upheld under all circumstances.



Registry number: DEENK/525/2026.PL
Subject: PhD Publication List

Candidate: András Péter Bodnár
Doctoral School: Géza Marton Doctoral School of Legal Studies
MTMT ID: 10076126

List of publications related to the dissertation

Articles, studies (7)

1. **Bodnár, A. P.:** A digitális bizonyítékok bírósági értékelése.
Debreceni jogi műhely : évkönyv. 22 (3-4), 1-19, 2026. ISSN: 1787-775X.
DOI: <http://dx.doi.org/10.24169/DJM/2025/3-4/1>
Level of HAS Committee on Legal and Political Sciences: B
2. **Bodnár, A. P.:** Bitektől a bizonyításig: a tisztességes eljáráshoz való jog a digitális bizonyítékok tükrében = From Accusation to Proof: The Right to a Fair Trial in the Light of Digital Evidence.
Pro futuro. 15 (2), 1-14, 2026. ISSN: 2063-1987.
DOI: <http://dx.doi.org/10.26521/profuturo/2025/2/16621>
Level of HAS Committee on Legal and Political Sciences: A
3. **Bodnár, A. P.:** A digitális bizonyítékok megjelenése a büntetőeljárásban: különös tekintettel a szakértő igénybevételére.
Büntetőjogi Szemle. 2022 (1), 19-29, 2022. ISSN: 2063-8183.
Level of HAS Committee on Legal and Political Sciences: C
4. **Bodnár, A. P.:** A bizonyítási eszközök fejlődése Finkeytől napjainkig.
Erdélyi Jogélet. 2 (1), 25-34, 2021. ISSN: 2734-6226.
DOI: <http://dx.doi.org/10.47745/ERJOG.2021.01.03>
Level of HAS Committee on Legal and Political Sciences: B
5. **Bodnár, A. P.:** Appearance of constitutional constraints in the taking of evidence in criminal proceedings: issue of unlawful evidence.
The Journal of the Faculty of Law Oradea. 2021 (1), 79-85, 2021. ISSN: 1582-7585.
6. **Bodnár, A. P.:** Digitalizáció a büntetőeljárásban: különös tekintettel a nyomozás és a bizonyítás szabályaira.
In: A jog tudománya, a mindennapok joga V. Konferenciakötet. Szerk.: Szűcs Lászlóné Siska Katalin, Talabos Dávidné Lukács Nikolett, Debreceni Egyetem Állam- és Jogtudományi Kar, Debrecen, 63-71, 2021.





**UNIVERSITY of
DEBRECEN**

**UNIVERSITY AND NATIONAL LIBRARY
UNIVERSITY OF DEBRECEN**

H-4002 Egyetem tér 1, Debrecen

Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

7. **Bodnár, A. P.:** Digitization in criminal proceedings: issues related to electronic data.

Büntetőjogi Szemle. 2021 (klsz.), 12-15, 2021. ISSN: 2063-8183.

Level of HAS Committee on Legal and Political Sciences: C

List of other publications

Articles, studies (1)

8. **Bodnár, A. P.:** Ünnepnaptól gyásznap: a vadászattal összefüggésben álló bűncselekmények.

In: Szakkollégiumi almanach 2018- A Praetor Szakkollégium Büntető Eljárásjogi Műhelyének

Tanulmánykötete. Szerk.: Szabó Krisztián, Printart-Press Kft., Debrecen, 30-49, 2026.

By the directives of HAS Committee on Legal and Political Sciences:

Publications in periodicals level „A”: 1, related to the dissertation: 1.

Publications in periodicals level „B”: 2, related to the dissertation: 2.

Publications in periodicals level „C”: 2, related to the dissertation: 2.

The Candidate's publication data submitted to the Tudóstér have been validated by DEENK on the basis of the Journal Citation Report (Impact Factor) database.

18 August, 2026

