DOI: 10.38146/BSZ.2024.2.1

A digitalizáció egyes kihívásai a büntetőeljárásban

Challenges of Digital Transformation in Criminal Procedure

Tóth Marcell Máté
Dr., doktorandusz, bírósági titkár
Eötvös Loránd Tudományegyetem,
Állam- és Jogtudományi Kar,
Állam- és Jogtudományi Doktori Iskola
Fővárosi Törvényszék

Absztrakt

Cél: A rohamos ütemű technológiai fejlődés és annak következményei a jog világát, így a büntető igazságszolgáltatást is új kihívások elé állítják. A büntetőeljárásban a digitalizáció megkerülhetetlen a modern, hatékony igazságszolgáltatás iránti társadalmi igény szempontjából, ugyanakkor arra is megoldást kell találnunk, hogy az információs technológiák térnyerésére adott válasz miként egyeztethető össze a tisztességes eljárást biztosító garanciális szabályokkal. Jelen tanulmányban a digitális technológiák és a büntetőeljárás egyes alapelveinek összefüggéseire kíván rávilágítani a szerző, különös tekintettel a bizonyításra, ahol az olyan követelmények, mint a közvetlenség elve az utóbbi években némileg talán háttérbe szorultak az eljárás időszerűségének javára.

Módszertan: A digitalizáció a jog számára is új kihívásokat teremt. A jogtudomány egyes sarkalatos kérdéseknek jogágtól függetlenül különös figyelmet szentel; a teljesség igénye nélkül ilyenek különösen az úgynevezett Big Data formában történő tömeges adatelemzés, a közösségi platformokon zajló kommunikáció, az adatbiztonság és magánszféra védelme, a kriptovaluták, s végül, de nem utolsó sorban a mesterséges intelligencia kérdésköre. A szerző tanulmányában a témát feldolgozó jogirodalmi munkák megállapításaira építve törekszik levonni következtetéseit, figyelemmel az elmúlt évtizedekben megalkotott, és a jövőben várhatóan lefektetésre kerülő releváns jogi aktusokra, jogalkalmazói gyakorlatra.

Megállapítások: A digitalizáció beférkőzése az élet szinte minden területére egyre inkább áthatja globális társadalmunk kollektív tudatát. A digitális forradalom átírta a kommunikációról, az információáramlásról vagy az adatvédelemről

A szerző a kéziratot magyar nyelven nyújtotta be. Benyújtás: 2023. 10. 03. Átdolgozás: 2023. 11. 10. Elfogadás: 2023. 12. 15.

alkotott elképzeléseinket, de alapvető változást hozott többek között a munka, az oktatás vagy a kereskedelem terén is. A technológiai vívmányok számtalan felhasználási lehetőséget rejtenek magukban a büntetőeljárás során eljáró szervek számára, rendkívüli mértékben elősegítve az időszerűség iránti igény kielégítését. Mindez ugyanakkor – különösen talán a nyomozás és az annak eredményein alapuló bizonyítás terén – felerősítheti azt a tendenciát, hogy a hatékonyság oltárán háttérbe szorulnak az olyan garanciális jelentőségű alaptételek, mint a közvetlenség elve.
Érték: Az elektronikus ügyvitel, az egyre sokoldalúbb digitális eszközök jelentős mértékben hozzájárulnak a büntetőeljárás hatékonyságához, egyúttal az újfajta bűnözési formák felderítése, bizonyítása sajátos kihívások elé állítják az eljáró hatóságokat, de a téma kapcsán a jelen tanulmányban írtakat meghaladóan is számos további kérdés merül fel, melyeket a jogtudomány is kiemelt figyelemmel kísér (például prediktív rendészet).

Kulcsszavak: bizonyítás, digitalizáció, közvetlenség elve, mesterséges intelligencia

Abstract

Aim: Recent technological developments and their potential consequences pose novel challenges to criminal justice. Digital transformation is a necessary consideration for a modern and effective justice system; however, the rise of information technologies must also be reconciled with procedural safeguards that ensure the right to a fair trial. The aim of this study is to shed light on certain aspects of how digital technologies might affect our interpretation of some of the basic principles of criminal procedure, with an emphasis on the taking of evidence, where such fundamental requirements as the principle of immediacy have perhaps recently been somewhat neglected in favour of conducting the procedure within a reasonable timeframe.
Methodology: Our legal framework and justice system must adapt to the advent of the digital age. Certain phenomena, such as Big Data analysis, social media, data and privacy protection, cryptocurrencies, as well as artificial intelligence have recently attracted special attention from legal scholars from all fields of law. The findings of this study are based on the review of the relevant literature in the field of digital technologies and law, as well as legislation and case law from the last few decades and potential future developments.
Findings: The expansion of digital technologies into nearly all aspects of our lives is ever-present in our global collective awareness. The digital revolution challenges our previous concepts about communication, access to information

and data protection, and has also already changed the way we think about work, education, or commerce. Technology has a massive potential for criminal justice as well, including the right to a fair trial within a reasonable time. However, it may also contribute further to recent tendencies in the taking of evidence where procedural safeguards such as the principle of immediacy are sacrificed in favour of efficiency.
Value: Digital technologies open a vast array of possibilities for criminal justice, however, also allow for new forms of criminality to emerge. Digitalisation and criminal procedure have numerous implications beyond the scope of this study (e.g. predictive policing) that merit further research.

Keywords: taking of evidence, digitalisation, principle of immediacy, artificial intelligence

Technológiai-társadalmi háttér

Az átlagos felhasználó számára az információs technológia világának működése átláthatatlannak, már-már misztikusnak tűnhet. Éppen ezért – a téma szempontjából releváns mélységig – szükségesnek tartom felvázolni a napjainkban tapasztalt kihívásokhoz vezető fejlődési folyamatot, valamint az így kialakult társadalmi változásokat, jelenségeket.

Először is érdemes tisztázni, hogy mit értünk digitalizáció alatt. A köznyelv és a szakirodalom egyaránt ismeri és egymással nagyjából felcserélhető fogalmakként használja a digitális, informatika, számítástechnika, vagy újabban akár a kiber kifejezéseket. A digit valójában latinul ujjpercet jelent; a digitalizáció az adatok számok formájába, jellemzően bináris rendszerbe történő konvertálását és ily módon történő feldolgozását jelenti. A köznyelvben a digitalizáció alatt a digitális technológiák, azaz elsősorban a számítógépek elterjedését, illetve a társadalomra, az emberi életre gyakorolt hatását értjük (Ambrus, 2021).

A különféle számítások, logikai műveletek elvégzését megkönnyítő eszközök, melyek a modern számítógépek primitív előképének tekinthetők, több évezredes múltra tekintenek vissza.[1] A korai számítástechnika egyik úttörőjeként is számon tartott Alan Turing 1937-ben fektette le az univerzális gép koncepcióját, amely az elgondolás szerint bármilyen feladat ellátására képes lehetne, és ezáltal minden más gépezetet kiválthatna. Az első elektronikus számítógépek

1 E körben szoktuk említeni például az általános iskolából ismerős abakuszt, vagy a 17. századi Pascaline számológépet.

az 1940-es években jelentek meg, míg az első programozható digitális, ám még elektromechanikai elven működő számítógép a német Konrad Zuse nevéhez köthető Z3 volt. A II. világháború alatt a szövetséges erők is jelentős áttöréseket értek el e téren; a legkorábbi számítógépeket többek között tüzérségi célpontok pontos meghatározására, illetve kódfejtésre használták. A következő évtizedekben a számítógépek felhasználása továbbra is katonai, illetve tudományos kutatási célokra korlátozódott. Végül a mikroprocesszorok megjelenése az 1960-as évek végétől a számítógépek méretének drasztikus csökkenéséhez vezetett, amely a következő évtizedekben lehetővé tette a személyi számítógépek, a civil felhasználású PC-k elterjedését (Berecz et al., 2019).

A következő lépés a ma ismert digitális, online világ irányába az egyes számítógépek közötti kapcsolatok hálózatának kialakítása volt. Az 1960-as évektől kezdődően különféle, eltérő technikai alapokon működő és kiterjedésű megoldások születtek a különálló számítógépek összekötésére. Kiemelendő ezek közül az Egyesült Államok Védelmi Minisztériumának támogatásával kifejlesztett ARPANET, amely elsőként használta a ma is általános TCP/IP internet protokollt az eltérő rendszerek közti kommunikációs protokollok összehangolására (maga az internet kifejezés a hálózatok közötti átjárhatóságra és összefonódásra utal). A TCP/IP-alapú kapcsolat az 1980-as években fokozatosan terjedt el világszerte. Ekkor még a magánszemélyek, vállalkozások csak korlátozott hozzáféréssel rendelkeztek, a magáncélú felhasználás lényegében üzenetküldésre korlátozódott. A world wide webet, azaz a világhálót, amely az interneten alapuló, böngésző-információmegosztó hálózat, a svájci CERN-nél végzett munkája során alkotta meg Tim Berners-Lee angol kutató, majd 1991 végén vált hozzáférhetővé a nyilvánosság számára. A Web 1.0 révén terjedt el az 1990-es években többek között a ma már mindennaposnak vett e-mailezés, az internetes fórumok, a fájlmegosztás, vagy az online vásárlás. Ezt követően az egyre hatékonyabb adatátvitel, valamint az internet-hozzáféréssel rendelkező mobiltelefonok elterjedése a 2000-es évek közepétől átformálta az internethasználat jellegét. A középpontba az úgynevezett user generated content, azaz a felhasználók által létrehozott tartalom került. Ekkortól terjedtek el a különböző közösségi média, illetve videómegosztó oldalak, amelyek – talán túlzás nélkül kijelenthetjük – alapjaiban formálták át az emberi kommunikációt; ezt nevezzük web 2.0-nak (Grech, 2021).

A számítógépek funkciója tehát lényegében az, hogy levegyék az ember válláról a komplex, időigényes kalkulációk elvégzésének, a problémák megoldásának terhét. A számítógép az egyes feladatait az utasítások, műveletek sorozatából álló programokon keresztül látja el, melyeket különböző programnyelveken tudunk a bonyolult numerikus kódokhoz képest érthetőbbé, használhatóbbá tenni.

A program alapvető műveleti lépései az algoritmusok (Berecz et al., 2019).

A digitális technológiák elterjedése nyomán a társadalomtudományok képviselői az 1990-es évek végétől deklarálták, hogy átléptünk az információs korszakba, társadalmunk információs társadalommá alakult. Mindez azt jelenti, hogy végbement egy forradalminak nevezhető változás, melynek eredményeképp a köznapi értelemben vett információ a korábbiakhoz képest sokkal szélesebb körben, immár szinte bárki által hozzáférhetővé vált.

Az információs társadalom komplex fogalom; Ződi Zsolt a technológiai, a gazdasági-foglalkoztatási és a kulturális-szociológiai aspektusát emeli ki:

1) eszerint az információhoz való hozzáférést, illetve az információ feldolgozását, kezelését egyre szélesebb körben lehetővé tevő technológiai változások a társadalom szinte minden szegmensét érintik;
2) gazdasági szempontból az információs társadalomban meghatározó jelentőséggel bír a sajátos tulajdonságokkal rendelkező információs ipar, amely a munkaerőpiacot is átalakítja;
3) végül emlékeznünk kell arra, hogy az információ a kultúrában gyökerezik, így a globális információáramlásból fakadó tömegkommunikáció átformálja szokásainkat, egyúttal a technológia minden korábbinál mélyebben hatol be a magánszféránkba (Ződi, 2002).

Az információs társadalom globális közösség, amelyben a technológia határokon átívelő, szinte közvetlen kommunikációt tesz lehetővé, és a társadalmi folyamatok a fizikai térről egyre inkább áttevődnek az online kibertérre. Ugyanakkor ennek mibenléte, fogalma még nem teljesen kidolgozott. Szathmáry Zoltán a hadtudomány kibervédelmi megközelítéséből kiindulva a következőképp határozza meg a kibertér fogalmát: *„globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese."* A magyar kibertér *„a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne."* (Miskolczi & Szathmáry, 2018). A kibertér tehát egy komplex jelenség, mely fizikai és virtuális elemekből, valamint emberi tevékenységekből tevődik össze.

Közgazdaságtani megközelítésből a digitalizáció hatására bekövetkezett a negyedik ipari forradalom, vagyis az Ipar 4.0. E fogalom ugyancsak több elemből tevődik össze; a különféle szakirodalmi fogalmi meghatározásokban nagyjából

egységesen központi elemként jelenik meg a termelés globális léptéken tetten érhető racionalizálása, melynek hátterében a digitális technológiák, algoritmusok általi hatékony adatfeldolgozás áll, és amely egyúttal az élet szinte minden területén kifejti hatását (Molnár, 2018).

Különböző diszciplínák tehát különböző megközelítésből vizsgálják a digitalizáció kérdését. Egy igen komplex jelenséggel, egy továbbra is kibontakozóban lévő folyamattal állunk szemben. Mindezek középpontjában láthatóan a változásokat előidéző technológiai eredmények állnak.

A digitalizáció a jog számára is új kihívásokat teremt. A jogtudomány egyes sarkalatos kérdéseknek jogágtól függetlenül különös figyelmet szentel; a teljesség igénye nélkül ilyenek különösen az úgynevezett Big Data formában történő tömeges adatelemzés, a közösségi platformokon zajló kommunikáció, az adatbiztonság és magánszféra védelme, a kriptovaluták, s végül, de nem utolsó sorban a mesterséges intelligencia (továbbiakban: MI) kérdésköre (Ződi, 2018).

Ezek a jelenségek természetesen nem függetleníthetők egymástól, az egyes technológiák kölcsönhatásban fejlődnek, de mind közül talán az MI ragadta meg leginkább mind a tudomány, mind a közvélemény fantáziáját.

Az artificial intelligence (AI) kifejezés John McCarthy, az MIT kutatója nevéhez köthető. Az MI koncepciójának születése 1956-ra tehető, amikor is a Dartmouth Egyetemen tartott konferencián először merült fel olyan programok megalkotásának gondolata, melyek önálló gondolkodásra is képesek lehetnek (Ambrus, 2021).

Az MI fogalmát az egyes tudományterületek különféleképp határozzák meg, különböző elemeket helyeznek előtérbe saját szempontrendszerük szerint. Általánosan elfogadott, egységes jogi vagy tudományos definíció tehát jelenleg nincs, de a kérdés lényegét talán abban ragadhatjuk meg, hogy az MI a racionális emberi gondolkodásra – illetve, ahogy erre lentebb kitérek, csupán annak mimikálására – képes algoritmus, program (Ambrus, 2021). A normatív fogalommeghatározáshoz hamarosan egy lépéssel közelebb kerülhetünk az Európai Bizottság 2021/0106(COD) számú, még vita alatt álló jogalkotási javaslata folytán, mely szerint *„mesterségesintelligencia-rendszer (MI-rendszer): olyan szoftver, amelyet az I. mellékletben felsorolt technikák és megközelítések közül egy vagy több alkalmazásával fejlesztettek, és amely az ember által meghatározott célkitűzések adott csoportja tekintetében olyan kimeneteket, például tartalmat, előrejelzéseket, ajánlásokat vagy döntéseket képes generálni, amelyek befolyásolják azt a környezetet, amellyel kölcsönhatásba lépnek.”*[2]

2 Javaslat az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról.

Tág értelemben az MI körébe sorolható minden algoritmus, szoftver, amely alkalmas olyan feladatok ellátásra, amiket korábban csak ember tudott végezni. A szűk értelemben vett MI ezzel szemben már az emberéhez hasonlatos kognitív képességekkel, önállósággal bír, így képes akár a tanulásra és a teljesen autonóm döntéshozatalra is. A szakirodalom megkülönbözteti továbbá az erős MI-t, mely öntudattal rendelkezik, a gyenge MI kategóriájától, amelynek önállósága nem éri el az öntudat szintjét. Az uralkodó tudományos konszenzus szerint a jelenlegi fejlettségi szinten még nem beszélhetünk erős MI-ről. Habár egyes programok valóban akár az emberi agy képességeit messze meghaladó sebességgel képesek rendkívül komplex problémákat megoldani, vagy beláthatatlannak tűnő adatmennyiségeket feldolgozni, mindez még nem jelent valódi intelligenciát, hiszen az automatikus, viszonylagos önállóságú döntéshozatal csupán egy előre meghatározott parancssor végrehajtása. Az öntudatra ébredt, gondolkodó MI koncepciója ezzel szemben túlmutat a puszta automatizmuson; elvileg önálló gondolkodás mentén lenne képes akár előre nem látott problémák megoldására is. Mindezek okán az MI-fejlesztések egyik legnagyobb kihívása az úgynevezett deep learning, avagy mély tanulás képességének elérése, melynek révén az algoritmus strukturálatlan adatokból is képes lehet az önálló gondolkodásra (Ambrus, 2021).

A digitális technológiák megjelenése a tételes büntető eljárásjogi szabályozásban

Mint láthatjuk, a digitalizáció jelensége mélyen beágyazódott a modern társadalmak működésének szinte minden szintjére, így mind a jogalkotónak, mind a jogalkalmazónak naprakész ismeretekkel kell rendelkeznie az egyre nehezebben nyomon követhető technológiai-társadalmi fejleményekről. A jogban, különösen az eljárásjogi szabályozásban a digitalizáció elsősorban az adminisztratív folyamatok optimalizálásának eszközéül szolgál (Ződi, 2018); ennek megfelelően a 21. század igazságszolgáltatása számára megkerülhetetlen a digitális technológiákban rejlő lehetőségek megfelelő kiaknázása.

A jogalkotónak az új technológiák szabályozása során először is mérlegelnie kell, hogy a digitalizáció nyomán felmerülő új életviszonyok, jelenségek beilleszthetők-e a fennálló fogalmi-dogmatikai rendszerbe, azokat a jogalkalmazó analógia útján képes-e megfelelően adaptálni, avagy szükséges-e merőben új jogintézmények lefektetése (Ződi, 2002). Habár az analógia alkalmazása az esetek jelentős részében kielégítő megoldásnak mutatkozik, a kiszámíthatóságot és következetességet mindenekelőtt feltételező büntetőjogi felelősség elbírálása értelemszerűen szigorúbb keretek lefektetését igényli.

Visszatérve az elektronikus ügyintézésre, a jogi informatika fejlődését a fejlett országokban három korszakra oszthatjuk a jogi ügyvitelt támogató eszközök jellege alapján. A legkorábbi időszakban, az 1970-es évektől kezdődően először a nagygépes rendszerek, majd a személyi számítógépek, nyilvántartórendszerek, szövegszerkesztők elterjedése az iratfeldolgozás, elektronizálás részbeni automatizálása révén segítette elő a munkafolyamatokat. A második szakasz, az online kommunikáció korszaka, az internet térhódításával vette kezdetét, melynek nyomán megjelentek az ügyfél és az állami szervek közti elektronikus kapcsolattartást biztosító rendszerek, az online iratbetekintés, illetve a videokonferencia útján történő tárgyalás lehetősége. A jelenlegi, harmadik korszakban a figyelem az MI-re irányul, amely elvileg a puszta optimalizáláson, automatizmuson felül, az eredeti funkcióján túlterjeszkedve merőben új jogi megoldások felfedezésére lehet képes, és akár a jogrendszer egészének átértelmezéséhez is vezethet (Ződi, 2020).

Tehát a digitális technológiák alkalmazása révén a korábbiakhoz képest összehasonlíthatatlanul egyszerűbbé, gyorsabbá és költséghatékonyabbá vált a hatósági, bírósági ügyintézés. Mindezek nélkül az utóbbi években az egyre emelkedő bírósági ügyteher mellett már aligha lenne elképzelhető a hatékony igazságszolgáltatás. Az automatizálás következő szintjét jelentik az olyan megoldások, melyek minimális vagy semmilyen emberi közreműködést nem igényelnek, mint a VÉDA rendszer által lehetővé tett szabálysértési eljárás, vagy a teljesen elektronikus cégeljárás (Ződi, 2018).

Hazánkban a 2000-es évek eleje óta kiemelt jogalkotói célkitűzés az elektronikus ügyintézés lehetőségének minél szélesebb körben történő biztosítása. Az egyik legkorábbi lépés ebbe az irányba az elektronikus aláírásról szóló 2001. évi XXXV. törvény megalkotása volt, a küszöbön álló uniós csatlakozásra is figyelemmel azzal a célkitűzéssel, hogy az elektronikus üzenetküldés biztonságosabbá váljon, és az elektronikus formában létrejött iratok feladójának személye ellenőrizhető legyen.

Az információs társadalom előretörésével tapasztalt újfajta bűnözési formák elleni küzdelem nemzetközi szintű összehangolásának jelentős lépése volt az Európa Tanács 2001. november 23-án, Budapesten kelt Számítástechnikai Bűnözésről szóló egyezményének, azaz a Budapesti Egyezménynek, vagy Cybercrime Egyezménynek az aláírása, melyet hazánkban a 2004. évi LXXIX. törvény hirdetett ki. Figyelemmel az információs technológiákat, a virtuális teret érintő bűncselekmények határokon átnyúló jellegére, a szerződés többek közt egységes fogalommeghatározásokat és közös eljárásjogi célkitűzéseket fektet le, kategorizálja a releváns deliktumokat, továbbá rendelkezik a részes államok közötti hatékony nemzetközi együttműködés kereteiről, így különösen egy a nap 24 órájában elérhető kapcsolattartási hálózat kialakításáról.

Az elektronikus technológiák hatékony állami kiaknázása terén fontos lépés volt az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény, azaz az E-ügyintézési törvény megalkotása és hatályba lépése, összhangban az Európai Parlament és a Tanács 910/2014/EU rendeletével, röviden az eIDAS (electronic identification and trust services) rendelettel; az elektronikus ügyintézés részletszabályait a 451/2016. (XII. 19.) Korm. rendelet rögzíti.

A bíróságokat érintően ki kell emelni a 2017-ben indult Digitális Bíróság Projektet, amely az ügyfélbarát elektronikus ügyintézés megkönnyítése és az adminisztratív terhek csökkentése érdekében három célt tűzött ki:

1) Az anonimizált bírósági határozatok közötti keresés megkönnyítése.
2) A BHGY rendszer továbbfejlesztése, a közhiteles nyilvántartások összekapcsolása a bírósági rendszerekkel.
3) Az E-Akta rendszer megteremtése révén a 2020. január 1. után indult ügyekben az iratbetekintés megkönnyítése (URL1).

Az elmúlt két évtizedben az elektronikus technológiák adaptálása terén a közigazgatás némileg előrébb járt az igazságszolgáltatásnál. A büntető ítélkezésben más jogterületekhez képest is lassabban zajlott le a digitális átállás folyamata, az elektronikus ügyintézés sokáig csupán kiegészítő jellegű lehetőség volt. A szabályozás átfogó reformálására a 2017. évi XC. törvény elfogadását követően, de még a régi Be. hatálya alatt került sor; eszerint a 2018. január 1. napján és az azt követően indult ügyekben kötelező az elektronikus kapcsolattartás az eljárásban érintett valamennyi állami szerv, illetve a védők, jogi képviselők számára. Az eljárás egyéb, elektronikus kapcsolattartásra nem kötelezett résztvevői bármikor bejelenthetik, hogy az E-ügyintézési törvényben foglaltak szerint – ez magánszemélyek esetén jellemzően Ügyfélkapun keresztül történő kézbesítést jelent – az elektronikus kapcsolattartás szabályait vállalva kívánnak eljárni. A jelenleg hatályos Be. tehát speciális jogszabály az E-ügyintézési törvényhez képest; a törvény XXVII. fejezete rendelkezik az elektronikus kapcsolattartásról, melyben általános jelleggel utal az E-ügyintézési törvény 17. § (1) bekezdésére (Róth, 2020).

A Be. 2022. március 1. napjától hatályos módosítása folytán a 132. § (6)–(8) bekezdése rögzíti az egyszerűsített elektronikus kapcsolattartás szabályait, mely szerint a bíróság, az ügyészség és a nyomozó hatóság az ügyiratot papíralapú kapcsolattartás esetén egyszerűsített elektronikus úton a címzett elektronikus levelezési címére vagy más elektronikus elérhetőségére kézbesítheti. A bíróság, az ügyészség és a nyomozó hatóság az egyszerűsített elektronikus úton való kézbesítéskor közli azt az elektronikus vagy hangkapcsolatot biztosító

elérhetőségét, amelyen a címzett az ügyirat hitelességét ellenőrizni tudja. A járványhelyzet alatt irányadó veszélyhelyzeti eljárási szabályok már lehetővé tették az e-mail útján történő kapcsolattartást; az alapvetően pozitív tapasztalatokra is figyelemmel a jogalkotó a Digitális Jólét Program keretében megfogalmazott javaslatok alapján megfelelően módosította a törvényt.

A távmeghallgatás, azaz a telekommunikációs eszköz használatának szabályait a Be. XX. fejezete fekteti le. Míg a régi Be. terminológiája szerinti zártcélú távközlő hálózat útján történő kihallgatásra csak viszonylag szűk keretek között volt lehetőség, addig a hatályos törvény a korábbiakhoz képest jóval szélesebb körben teszi lehetővé az ily módon történő részvételt az eljárási cselekményen. A Be. a távmeghallgatás elsődleges formájaként az audiovizuális összeköttetést rögzíti, míg kivételesen lehetséges a kizárólag hangkapcsolat útján történő meghallgatás (Róth, 2020). A szükséges technikai feltételek megteremtése érdekében 2018-ban vette kezdetét a ViaVideo rendszerek kiépítése a bíróságokon. 2019-re 184 végpont került kialakításra, azaz az ország valamennyi bíróságán legalább egy távmeghallgató helyiség elérhetővé vált (URL2).

A távmeghallgatás lehetősége jelentős mértékben hozzájárulhat az eljárás hatékonyságához, időszerűségéhez, illetve a költségek minimalizálásához, így különösen tehermentesítheti a büntetés-végrehajtási szervezetet a fogva tartásban lévő terheltek előállítása alól, vagy lehetővé teheti olyan, például külföldön tartózkodó személyek részvételét az eljárásban, akiket csak jelentős nehézségek árán lehetne személyesen meghallgatni. A telekommunikációs eszköz használatával járó előnyök ugyancsak a járványhelyzet idején kerültek előtérbe, amikor a személyes jelenlét minimalizálása kulcsfontosságú kérdéssé vált az igazságszolgáltatás működőképességének fenntartása érdekében. Az Országos Bírósági Hivatal elnökének éves beszámolói alapján rendelkezésre álló adatok szerint a távmeghallgatást, úgy tűnik, a veszélyhelyzet egyfajta sikertörténeteként könyvelhetjük el; míg 2019-ben országosan mindösszesen 6426 távmeghallgatást bonyolítottak le a bíróságok (URL3), addig 2020-ban, a járvány első évében ez a szám 20 569-re (URL4), majd 2021-ben 29 157-re emelkedett (URL5). Mindhárom említett évben az esetek túlnyomó többségében büntetőeljárásban, vádlottak meghallgatása céljából került sor távmeghallgatásra.

Az elektronikus ügyviteli jellegű, illetve az eljárás optimalizálását és modernizálását szolgáló szabályokon túl a digitalizáció hangsúlyos tényezőként jelenik meg a bizonyítás és a kényszerintézkedések körében is. A Be. a tárgyi bizonyítási eszköztől elkülönülő, önálló bizonyítási eszközként vezette be az elektronikus adat, és ehhez kapcsolódóan az értelmező rendelkezések közt az információs rendszer fogalmát. A régi Be. hatálya alatt az elektronikus adatok a tárgyi bizonyítási eszköz fogalmi körébe tartozó bizonyítékként voltak

felhasználhatók; ide tartozott az adatot tároló információs rendszeren, adathordozón túl maga az elektronikus, információs jel is. A hatályos Be. indokolása szerint a jogalkotó azért tartotta szükségesnek különálló kategória létrehozását, mert a hagyományos, fizikai valóságban megjelenő tárgyi bizonyítási eszközökre igazított szabályok nem minden esetben voltak alkalmazhatók az információs rendszerek tartalmára.

Ennek jegyében a törvény a vagyont érintő kényszerintézkedések körében nagyobb hangsúlyt fektet a digitális adatokra. A Be. 315. §-a a korábbi megoldással ellentétben speciális rendelkezéseket fektet le az elektronikus adat lefoglalására nézve, részletesen taglalva annak módjait. Lefoglalás tárgya lehet maga a tárolt adat, az adathordozó vagy az információs rendszer egésze. A fokozatosság jegyében a lefoglalás történhet elsődlegesen másolat készítésével vagy áthelyezéssel, míg az információs rendszer vagy adathordozó birtokának elvonására csak többletfeltételek mellett van lehetőség. A törvény ugyanezen cím alatt rendelkezik az elektronikus adat megőrzésére kötelezésről, mely az adat birtokosának rendelkezési jogosultságát korlátozza. E kényszerintézkedés lehetővé teszi, hogy az elrendelő az érintett adatok átvizsgálását követően megalapozott döntést hozhasson az esetleges lefoglalásról (Róth, 2019).

A fentieken túl az elektronikus adat, illetve az információs rendszer kategóriája a törvény számos további rendelkezésében visszaköszön, lényegében már a régi Be. egyes módosításaival bevezetett szabályoknak megfelelő tartalommal, melyek közül néhányra az alábbiakban mutatnék rá.

A kényszerintézkedések körében maradva például a kutatás kiterjedhet az információs rendszer vagy adathordozó átvizsgálására (egyúttal az intézkedés elnevezése a korábbi terminológia szerinti házkutatáshoz képest pontosabban tükrözi annak tartalmát).

Kifejezetten a Btk. 77. § (1) bekezdésében taglalt elektronikus adat végleges hozzáférhetetlenné tételének várható alkalmazása esetén, az online tartalmak közzétételével megvalósuló bűncselekmények megszakítása érdekében elrendelheti a bíróság az elektronikus adat ideiglenes hozzáférhetetlenné tételét, mely szintén az adat fölötti rendelkezési jogosultságot korlátozza.

A tágabb értelemben vett digitalizáció eredménye továbbá a távoltartás, illetve a bűnügyi felügyelet biztosítását szolgáló, a terhelt mozgását nyomon követő technikai eszköz.

Minthogy az utóbbi években a bűnözés, illetve annak esetleges nyomai is egyre szélesebb körben megjelentek a különféle digitális eszközökön, ehhez a leplezett eszközök alkalmazási körének is megfelelően igazodnia kell; e körben értelemszerűen a bírói engedélyhez kötött információs rendszer titkos megfigyelése bír különös jelentőséggel.

Az eljárás gyorsítását mozdítja elő és jelentős adminisztrációs tehertől mentesíti az eljáró szerveket az elektronikus adatkérés lehetősége, a különböző nyilvántartásokhoz való közvetlen hozzáférés.

Végül szintén a Be. 2022. március 31. napján hatályba lépett módosítása folytán a jogalkotó speciális joghatósági felhatalmazással ruházza fel a büntetőeljárásban eljáró szerveket a Magyarországról is elérhető digitális adatok, internetes tartalmak tekintetében, azzal, hogy az eljárási cselekmény nem terjedhet ki az információs rendszer védelmét szolgáló eszköz vagy informatikai megoldás megkerülésére vagy kijátszására, illetve nem érinti a nemzetközi bűnügyi együttműködés keretében vállalt kötelezettségeket. A korábban említett kibertér jelensége a büntetőeljárásban a joghatósági és illetékességi szabályok szempontjából jelent kihívást. A fizikai és a kibertér közt van átfedés, de az internethálózatot működtető és az online tartalmakkal rendelkezni jogosult gazdasági szereplők más-más államok honosságába tartoznak, így előfordulhat, hogy a magyar büntetőeljárás eredményessége az érintett hírközlési szolgáltató, vagy éppen a külföldi hatóságok együttműködési hajlandóságától függhet; a módosítás ezt a helyzetet hivatott orvosolni.

A digitalizáció megjelenése a büntető anyagi jogban

Dolgozatomban a digitalizáció egyes büntetőeljárás-jogi vetületeit kívánom feldolgozni, nem feledve ugyanakkor, hogy a büntetőeljárás és különösen a bizonyítás tárgyának kereteit, a büntetőjogi felelősség alapvető feltételeit a büntető anyagi jog szabályai rögzítik, így a következőkben erre térnék ki a téma szempontjából releváns körben.

A tételes általános részi rendelkezések közvetlenül csak egy helyen utalnak a digitális technológiákra, az elektronikus adat végleges hozzáférhetetlenné tételénél, melyet a Btk. az elkobzás mintájára, kifejezetten az online bűnözéshez kapcsolódó deliktumok visszaszorítását szolgáló intézkedésként vezetett be.

A digitális forradalom kihívást jelent az egyébként igen hagyománytisztelő büntetőjog-tudomány számára, tekintettel arra, hogy az újonnan tapasztalt technológiai és társadalmi jelenségek nem feltétlenül illeszthetők be az évszázadok alatt kialakult dogmatikai rendszerbe. A bűncselekménytan körében például – az elektronikus adat mint bizonyítási eszköz kapcsán kifejtettekhez hasonlóan – az elkövetési tárgy értelmezésének ma már tekintettel kell lennie az információs rendszerekben megjelenő adatokat érintő bűncselekményekre is. Többek között ezért javasolja Ambrus István az elkövetési tárgy fogalmának kiegészítését a személy, illetve dolog mellett a *„más speciális tárgy”* kategóriájával (Ambrus, 2021).

Az általános rész és a bűncselekménytan talaján maradva úgy tűnik, részben a digitalizációra visszavezethetően kialakulóban van a tevéssel és mulasztással is megvalósítható deliktumok egy újabb kategóriája, melyek a materiális nyitott törvényi tényállásokkal ellentétben nem tartalmaznak eredményt; ezeket Ambrus kvázi nyitott törvényi tényállásoknak nevezi. Az utóbbi évek bírói gyakorlatából erre példa lehet az állat életfeltételeiről való gondoskodás elmulasztásával megvalósított állatkínzás (EBD2014.B.8), vagy a Kúria újabb értelmezésében a rágalmazás, illetve a becsületsértés (EBH2017B.11) (Ambrus, 2021).

Különösen az online jelenlét kapcsán merül fel a törvényi tényálláson kívül álló előkészületi jellegű cselekményekért való büntetőjogi felelősség kérdése. Az interneten közzétett előkészületi szándéknyilatkozatok – így a felhívás, ajánlkozás, vállalkozás, közös elkövetésben megállapodás – például értelemszerűen előkészületi magatartásként büntethetők, ha annak egyéb feltételei fennállnak, azaz ha a törvény büntetni rendeli az előkészületet, és a bűncselekmény elkövetésére irányuló célzat ténylegesen megállapítható. Különösen ez utóbbi szubjektív elem fennállta igényel körültekintő mérlegelést, tekintettel arra, hogy az online platformokon a felhasználók köztudomásúan meggondolatlanabbul nyilvánulnak meg, mint akár a személyes vagy bármely egyéb fajta kommunikáció során (Ambrus, 2021).

A digitalizáció hatása talán némileg kézzelfoghatóbb a különös rész körében. Ahogy a technológia beférkőzött a 21. századi ember életének szinte minden mozzanatába, úgy az utóbbi évtizedekben a bűnözés mint társadalmi jelenség is számtalan új formát öltött.

Ahogy a mindennapi értelemben vett digitalizáció terminológiája is igen sokrétű, hasonlóképp számos különféle elnevezéssel találkozhatunk a technológiai fejlődés nyomán kialakult büntetendő magatartások leírására (kiberbűnözés, számítógépes bűnözés stb.), mindezek közül azonban a digitális bűnözés a leginkább technológiasemleges, így ez fedi le a deliktumok legszélesebb körét (Ambrus, 2021).

Az uralkodó szakirodalmi álláspont szerint a digitális bűncselekményeket két fő csoportra oszthatjuk fel. A szoros értelemben vett vagy sajátképi digitális bűncselekményeknek az információs rendszer az elkövetési tárgya, enélkül a törvényi tényállás fogalmilag nem valósul meg (cyber-dependent crimes – például hacking, azaz jogosulatlan belépésjellegű cselekmények, melyet a Btk. az információs rendszer vagy adat megsértésének tényállásával szankcionál). Tágabb értelemben a digitális bűncselekmények közé sorolhatunk minden olyan deliktumot, melyeknek nem szükségszerű feltétele a digitális elem; a technológia – jellemzően elkövetési eszközként – csupán elősegíti a cselekményt (cyber enabled crimes). Az utóbbi években nagy figyelem irányul

például a gyermekpornográfiára, az online zaklatásra, azaz cyberbullyingra, vagy a közösségi médiában, illetve egyéb internetes platformokon tett rágalmazó, becsületsértő kijelentésekre, de újfajta bűnözési formát jelenthetnek az úgynevezett deepfakek, melyek MI révén valós vagy fiktív személyek arcképét, hangját, beszédét képesek többé-kevésbé élethűen imitálni, többnyire audiovizuális formában (Ambrus, 2021).

Egyes szerzők megkülönböztetnek egy további kategóriát, a járulékos számítógépes bűnözést (incidental computer crime); itt az információs rendszer lényegében egy hagyományos eszközt vált ki (például könyvelés számítógéppel a papíralapú dokumentáció helyett) (Máté, 2017).

Garanciális szabályok a büntetőeljárásban; a közvetlenség elve

A digitális bűncselekmények elbírálása körében sem feledkezhetünk meg azokról az általános érvényű alapelvekről és eljárási garanciákról, amelyek a tisztességes eljáráshoz való jog érvényesülését szolgálják.

A büntető hatalom érvényesítése teszi lehetővé a legsúlyosabb állami beavatkozást az állampolgárok magánszférájába, ezért alapvető jogállami követelmény, hogy a terheltet mind a jogi szabályozás, mind a jogalkalmazás szintjén meg kell óvni az esetleges állami önkénytől. A jogalkotó a büntetőjog terén már az Alaptörvény szintjén általános érvényesülést követelő alapelveket fektetett le; a büntetőeljárásban a legalapvetőbb követelmény a tisztességes eljáráshoz való jog biztosítása. A tisztességes eljárás számos további részjogosultságot, alapelvet és eljárási garanciát foglal magába, melyek végső soron egyrészről azt szolgálják, hogy a terhelt, illetve védője aktív közreműködőként alakíthassák az eljárás menetét, másrészről pedig biztosítják az eljárás pártatlan, részrehajlástól mentes és időszerű lefolytatását (Tóth, 2021).

A büntetőeljárást érintő legfontosabb követelmények közül tehát az Alaptörvény XXVIII. cikke rögzíti többek közt a tisztességes eljáráshoz való jogot, az ártatlanság vélelmét és a védelemhez való jogot. A Be. első, *Alapvető rendelkezések* című fejezete tovább részletezi az eljárás egészét átható elveket, emellett alapelvi jellegű rendelkezéseket találunk az eljárás egyes szakaszaihoz vagy sarkalatos kérdésköreihez kapcsolódó szabályok között, például a kényszerintézkedések vagy a bizonyítás körében. Ahogy azonban a törvény miniszteri indokolása is utal rá, a tételesen rögzített alapelvek listája nem kimerítő jellegű; a jogalkotó szükségtelennek tartotta a nem kizárólag a büntetőeljáráshoz kapcsolódó elvek nevesítését, így a Be. – hasonlóan az 1998. évi XIX. törvényhez – nem tesz említést a bizonyítás során továbbra is meghatározó jelentőségű közvetlenség és szóbeliség elvéről.

A közvetlenség elve az akkuzatórius büntetőeljárási rendszer hagyományaiból eredő követelmény, melynek funkciója, hogy a bíróság személyesen észlelt, azaz a tárgyaláson lefolytatott bizonyítás eredménye alapján alakíthassa ki álláspontját a bizonyítás tárgyára, a releváns tényekre nézve. A közvetlenség elvéhez szorosan kapcsolódik a szóbeliség elve, mely lehetővé teszi, hogy a vádlott, illetve a védő kontradiktórius eljárás keretében a tárgyaláson, élőszóban fejthesse ki álláspontját a bizonyítás során. Mindez biztosítja a nyomozás eredményeinek, a vád által prezentált bizonyítékoknak az érdemi felülvizsgálatát az eljárás bírósági szakaszában. A közvetlenség elve tehát egyrészről azt szolgálja, hogy a bíróság lehetőleg az anyagi igazságnak megfelelően állapítsa meg a tényállást, másrészről elősegíti a védelemhez való jog érvényesülését.

Ugyanakkor az idők során a közvetlenség elve kétségkívül veszített jelentőségéből (Hati, 2015). Azon túl, hogy a jogalkotó továbbra sem tartotta szükségesnek a tételesen rögzített alapelvek közötti nevesítését, utalni kell arra, hogy a Be. egyik legfőbb célkitűzése a büntető ítélkezés időszerűségének és hatékonyságának előremozdítása, amely azonban rendszerint valamely garanciális követelmény rovására valósítható meg, mint amilyen a közvetlenség elve. A törvény számos olyan eljárási lehetőséget fektet le, melyek révén például a terhelt együttműködésére építve akár teljes egészében el lehet kerülni az adott esetben hosszadalmas és bonyolult bizonyítási eljárás lefolytatását. Mindez igen előnyös lehet a jogalkalmazó számára és az eljárás gyorsítása iránti társadalmi igénynek is megfelel, ugyanakkor az időszerű ítélkezés előmozdításával egyúttal talán lépésről lépésre eltávolodunk az alapvető garanciális szabályok által védeni hivatott értékektől. A közvetlenség elvének háttérbe szorulása azzal jár együtt, hogy a bíróságnak döntően a nyomozás irataira kell hagyatkoznia, azaz az eljárás hangsúlya a nyomozati szakra helyezkedik, míg a bíróság eljárása egyre inkább veszít jelentőségéből.

Az eljárás gyorsítása és a terheltet megillető garanciális szabályok szembenállása persze nem újkeletű jelenség, ellenkezőleg, a büntetőeljárásjog-tudomány egyik „örökzöld" témájaként tartjuk számon (Czédli, 2019). A digitális forradalom technológiai eredményei, illetve a digitális bűncselekmények sajátosságai, úgy tűnik, egy újabb terület, amely kevésbé egyeztethetők össze a közvetlenség elvén alapuló bizonyítással.

A digitalizáció egyes sarkalatos kérdései a bizonyításban

A Be. – mint láthattuk – számos ponton kifejezetten reflektál az információs társadalom igényeire és a digitális bűnözés kihívásaira. A bizonyítás körében

új elemként vezeti be az elektronikus adat fogalmát, amely azonban önmagában nem ad választ valamennyi, a digitális bűncselekmények, illetve a tágabb értelemben vett digitalizáció által felvetett bizonyítási kérdésre.

Az előző fejezetben kifejtettek szerint a közvetlenség elve értelmében a tárgyalás szolgál a bizonyítás helyszínéül, és a bírói meggyőződés is elvileg a tárgyaláson tapasztaltak alapján alakul ki a tényállást illetően. A digitális vonatkozású büntetőeljárások esetében ugyanakkor fokozottan igaz az – Finszter Géza szavaival élve –, hogy *„A kontinentális tárgyalási rendszer […] inkább tekinthető a nyomozási anyag felmondásának, mint a tényállás megállapításához szükséges eredeti bizonyítás felvételének…”* (Finszter, 2021), vagyis a bíróság nagyrészt rá van utalva a nyomozó hatóság felderítő tevékenységének eredményére.

A digitális bűncselekmények esetében a vádat alátámasztó bizonyítékok összegyűjtése és biztosítása több szempontból különösen nehéz feladat elé állítja a nyomozó hatóságot. Az internet igen nagyfokú anonimitást biztosít az online kriminalitás számára. A jogkövető világban is mindennapos VPN (virtual private network, azaz virtuális magánhálózat) szolgáltatások titkosítják a felhasználó teljes internetes tevékenységére vonatkozó adatokat, elfedik az IP-címét. A dark web olyan, a világhálón keresztül kapcsolódó, úgynevezett egymásra épülő, decentralizált hálózatokat takaró gyűjtőfogalom, amelyek eléréséhez valamilyen különleges szoftverre van szükség, és rendkívüli mértékben megnehezítik az online tevékenység nyomon követését; a legismertebb ilyen hálózat a TOR (The Onion Router) (Goodison, Woods, Barnum, Kemerer & Jackson, 2019). Az illegális tranzakciók lebonyolítása ezen felül gyakran a decentralizált és javarészt szabályozatlan kriptovalutákban történik, amely tovább nehezíti az ügyletek összekapcsolását az elkövetővel és a bűncselekménnyel (Polt, 2022).

A rejtett adathasználat és online kommunikáció veszélyeire reagálva az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Ektv.) 2016. július 17. napjától hatályos 3/B. §-a lehetővé teszi a titkosítást biztosító szolgáltatók kötelezését a titkosított tartalmak átadására; a részletszabályokat a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított együttműködésének rendjéről szóló 185/2016. (VII. 13.) Korm. rendelet rögzíti (Miskolczy & Szathmáry, 2018).

További kihívást jelent ugyanakkor az online bűnözés nemzetközi jellege. Az internetes térben fellelhető bizonyítékok, adatok összegyűjtésében a nyomozó hatóságok nagymértékben rá vannak utalva a különböző hírközlési, illetve tárhelyszolgáltatók által nyújtott információkra, a rendszerint külföldi illetőségű gazdálkodó szervezetek azonban nem mindig bizonyulnak hajlandónak az együttműködésre, illetve a megkeresés teljesítése is igen körülményesnek és

időigényesnek bizonyulhat. Ha a közvetlen adatkérés nem vezet eredményre, szükséges lehet az adott állam hatóságához fordulni nemzetközi bűnügyi együttműködés keretében, vagy az Európai Unió tagállama esetén európai nyomozási határozat útján, azonban a megkeresett állam együttműködési hajlandósága is változó, így a megkeresés teljesítésének elmulasztása akár a nyomozás elakadásához is vezethet. Az Európai Unió Bírósága, úgy tűnik, a szolgáltatók szabadsága, illetve a személyes adatok és a magánszféra védelme mellett foglalt állást (Digital Rights Ireland Ltd. kontra Írország-ügy, C-293/12 és C-594/12 egyesített ítélet, Tele2-ügy, C-203/15 és C-698/15 egyesített ítélet).

Mindezek mellett az említett deepfake-technológia a bizonyítás körében is nehézségeket okozhat a hatóságok számára. Habár a jelenleg elérhető (mozgó) képi, illetve hangimitációk még jellemzően kiforratlanok, így legtöbbször már viszonylag csekély fokú körültekintés mellett is felismerhetők, a digitális technológiák fejlődési ütemét ismerve ez várhatóan már a belátható közeljövőben változhat. Az utóbbi években többen aggodalmuknak adtak hangot arra nézve, hogy az MI-alapú deepfakek könnyedén válhatnak a hatóságok megtévesztésének eszközévé a büntetőeljárásban. Erre tekintettel a jövőben gyakrabban lehet szükséges a bíróság elé tárt, bizonyítékul szolgáló felvételeket további metaanalízis alá vetni (Gravett, 2020).

Az elektronikus, digitális bizonyítékok számos formában jelenhetnek meg a büntetőeljárásban. Egy kamerafelvétel bizonyító ereje például a felvételen látottakban rejlik, az adathordozó vagy a videófájl értékelése többnyire nem igényel különleges szakértelmet. Ahol azonban a büntetőeljárásban nagyobb hangsúlyt kap a digitális technológia, az elektronikus adatot vagy információs rendszert érintő eljárási cselekmények elvégzéséhez informatikai szakértő közreműködés válhat szükségessé. A Digital Forensic Sciecne, vagyis a bűnügyi informatika a digitális vonatkozású büntetőeljárásokra szakosodott, viszonylag rövid múltra visszatekintő bűnügyi segédtudomány, melynek feladata a bizonyítékok hiteles összegyűjtése, elemzése és bemutatása (Máté, 2017).

A digital forensic science tárgya a digitális bizonyíték, amely az elfogadott tudományos fogalommeghatározás szerint olyan bizonyító erejű információ, melyet bináris formában tároltak vagy továbbítottak. A definíció az elektronikus adat Be.-ben foglalt törvényi fogalmához képest tehát a bináris formára helyezi a hangsúlyt, míg a feldolgozó információs rendszernek nem tulajdonít jelentőséget. A digitális bizonyítékokat a szakirodalom elsősorban aszerint csoportosítja, hogy milyen formában, illetve milyen forrásból nyerhetők ki. Eszerint különbséget tehetünk az online tevékenység során keletkező, a kibertérben fellelhető adatok, valamint a hagyományos, fizikai adathordozókon tárolt adatok között. Továbbá megkülönböztethetünk olyan adatokat, melyek

az előbbi két kategóriára vonatkozó további információkat hordoznak, például az adatok keletkezésének, módosításának idejét vagy módját. Ilyenek lehetnek az információs rendszer vagy program használata során keletkező metaadatok, melyek révén például név, felhasználónév vagy IP-cím alapján a felhasználó személyére is következtetni lehet (Gyaraki, 2018).

Hazánkban az informatikai szakértői tevékenység általános jogszabályi kereteit az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény (Szaktv.) fekteti le, míg a részletszabályokat az igazságügyi szakértői működésről szóló 31/2008. (XII. 31.) IRM rendelet rögzíti. A 9/2006. (II. 27.) IM rendelet 6. melléklete határozza meg az informatikai szakértői szakterületeket. 2017-ben alakult meg a Magyar Igazsásügyi Szakértői Kamara Informatikai és Hírközlési Tagozata, amely elsődlegesen a magas szakmai színvonalú és egységes szakértői működést hivatott biztosítani.

Az igazságügyi szakértő tevékenysége a büntetőeljárásban igen sokrétű. Első lépésként már a potenciális digitális bizonyítékok azonosítása is informatikai szaktudást igényelhet. Az azonosítás keretében a szakértő elsősorban házkutatás, illetve annak előkészítése során feltárja és dokumentálja a releváns adathordozókat, információs rendszereket. A szakértő feladata az azonosított eszközök összegyűjtése, tárolása és megőrzése, valamint a releváns adatok kinyerése, azaz kimásolása, esetleg visszaállítása, melyre sor kerülhet a helyszínen vagy laboratóriumban. A szakértő ezt követően elemzi a digitális bizonyítékokat, végül szükség esetén prezentálja azokat a nyomozó hatóság, vagy adott esetben a bíróság számára (Máté, 2017).

A technológia nem csak a bizonyítás tárgyaként bírhat jelentőséggel a tényállás megállapítása során; digitális eszközök és források széles tárháza segíti az eljárásban részt vevő szervek munkáját.

Az online jelenlét nagy mennyiségű adatot, digitális lábnyomot hagy maga után az interneten, amely nyílt forrású adatgyűjtés (open source intelligence – továbbiakban: OSINT) révén rendkívül hasznosnak bizonyulhat a nyomozóhatóság számára a bűncselekmény felderítése során. Az OSINT, azaz a nyilvánosan, bárki számára korlátozás nélkül és jogszerűen hozzáférhető adatok összegyűjtése és elemzése gyakran, de nem kizárólag az önkéntesen, például közösségi média útján megosztott online információra irányul. Az adatgyűjtés történhet aktív vagy passzív formában; az előbbi esetén valamilyen kölcsönös interakció szükséges a vizsgált személlyel (például követési kérés jóváhagyása), míg utóbbi esetén kapcsolatfelvételre nem kerül sor, a célszemély közreműködése nem szükséges, és így nem is szerez tudomást arról, hogy vele szemben adatgyűjtés lehet folyamatban.

Jelentős mennyiségű digitális adatanyag áll rendelkezésre nemcsak az online térben, hanem a különféle hatósági, bűnügyi nyilvántartási rendszerekben is.

A Rasterfahndung, azaz raszternyomozás az 1970-es években a Német Szövetségi Köztársaságban kialakult felderítési módszer, a különböző, egymástól független adatbázisok automatizált elemzését és összehasonlítását jelenti, melynek révén a nyomozó hatóság úgynevezett raszterkritériumok alapján szűkíti le a lehetséges elkövetői kört, és szűri ki az érdektelen személyeket. Hazánkban a raszternyomozásnak nincs kiterjedt gyakorlata és a konkrét jogi szabályozás is hiányzik. A magyar bűnügyi hatósági adatbázisokra vonatkozó legfontosabb szabályokat 2009. évi XLVII. törvény, a Bnytv. fekteti le, melynek 3. § (1) bekezdése értelmében a bűnügyi nyilvántartási rendszer a személyazonosító adatok és fényképek nyilvántartásából, valamint a bűnügyi nyilvántartásokból áll; ez utóbbi részét képezi a 7. § szerint a bűntettesek nyilvántartása, a hátrányos jogkövetkezmények alatt álló, büntetlen előéletű személyek nyilvántartása, a büntetőeljárás hatálya alatt állók nyilvántartása és a külföldre utazási korlátozás hatálya alatt állók nyilvántartása. Mindezen adatbázisok tartalmát a büntetőeljárásban eljáró szervek, így a nyomozó hatóság is a Be. 263. §-ában foglalt felhatalmazás alapján akár közvetlen elektronikus hozzáférés útján is megismerhetik. Az automatizált bűnügyi adatelemzés azonban, ahogy arra a nemzetközi tapasztalatok is rávilágítanak, értelemszerűen alapjogi aggályokat is felvet. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) 5. § (7) bekezdése értelmében bűnügyi személyes adat csak szűk körben, a különleges adatokra vonatkozó szabályok szerint kezelhető, ezen felül a törvény a bűnüldözési célú adatkezeléshez is további speciális feltételeket határoz meg. A Bnytv. 8. § (1) bekezdése pedig kimondja, hogy a fenti bűnügyi nyilvántartások egymással nem kapcsolhatók össze. Az Alkotmánybíróság bűnügyi célú adatkezeléshez kapcsolódó álláspontja (lásd például 144/2008. [XI. 26.] AB határozat), valamint a nemzetközi gyakorlat, különösen a Német Szövetségi Alkotmánybíróság releváns gyakorlata alapján megállapítható, hogy a raszternyomozás alkalmazására csak a célhoz kötöttség elvének megfelelően, törvényi szintű szabályozás mellett és a szükségesség-arányosság elvére figyelemmel kerülhet sor (Jámbor, 2022).

A technológia által támogatott felderítés direktebb formája lehet a hatósági hacking, amely az érintettek tudtán vagy akaratán kívül végzett, a digitális kommunikáció tartalmának vagy titkosított adatoknak a megismerésére irányuló, nyílt vagy titkos tevékenység. Ennek végrehajtása többféle módszerrel történhet, például a brute force (nyers erő) a titkosítás feltörését, az információs rendszer sebezhetőségeinek kihasználását jelenti, de jellemzően ide tartozik a hatósági kémprogramok alkalmazása, melynek a hazai jogszabályi alapját a büntetőeljárásban a Be. a leplezett eszközök körében, az említett információs rendszer titkos megfigyelésére vonatkozó rendelkezésekkel fekteti le. A hatósági hacking áttörést hozhat különösen a dark weben folytatott, rendkívül nehezen nyomon

követhető és bizonyítható tevékenység felderítése során, ugyanakkor e körben is felmerül a célhoz kötöttség és az arányosság sérelmének veszélye (például ha a megszerzett adatok köre vagy az érintett személyi kör túlmutat a büntetőeljárás célján), ezen felül joghatósági aggályok is felmerülnek, ha az érintett szerver más államban található (Mezei, 2019).

Az MI lehetséges felhasználása a bizonyításban

A fentiekben röviden bemutatott OSINT, a raszternyomozás és a hatósági hacking emberi mércével beláthatatlannak tűnő adatmennyiség feldolgozását igényelheti. A bűnfelderítési célú, Big Data jellegű adatelemzés ideális alkalmazási terület lehet az MI számára, amely az időigényes, de különösebb mérlegelést nem igénylő emberi tevékenység kiváltása, a nyomozó hatóság tehermentesítése révén jelentős mértékben hozzájárulhat a nyomozás optimalizálásához. Hasonlóan a korábban kifejtettekhez, egyelőre még nem született jogalkotói válasz az MI-rendszerek alkalmazásának lehetőségére a nyomozás során, de a kérdéssel foglalkozó szakirodalom egységesnek tűnik abban, hogy elengedhetetlen a megfelelő garanciális szabályok, mindenek előtt az emberi felülvizsgálat lehetőségének lefektetése (Miskolczi & Szathmáry, 2018).

Az MI büntetőeljárásban betöltött szerepét illetően azonban talán a legtöbb kérdőjelet felvető téma az érdemi mérlegelést – legalábbis egyelőre –, a kizárólag az emberre jellemző értelmet igénylő feladatok, így különösen a bíróság ítélkező tevékenységének az MI általi kiváltása. Az állami feladatok digitalizációjával a hazai jogrendszerben az elmúlt évtizedekben a különféle, döntően közigazgatási jellegű eljárások is nagyfokú automatizáción estek át, így például a 2015 óta működő VÉDA intelligens kamerarendszer és az ahhoz kapcsolódó Közlekedésbiztonsági Automatizált Feldolgozó és Információs Rendszer (KAFIR) révén a szabálysértési eljárást algoritmusok sora – adott esetben – bármiféle emberi beavatkozás nélkül folytatja le, és állapít meg joghátrányt az eljárás alá vont személlyel szemben (Ződi, 2018).

A „robotbíró" koncepciója kétségkívül megmozgatta a jogtudomány fantáziáját. A korai kísérletek azt mutatják, hogy az MI egészen megbízható eredménnyel lehet képes megjósolni egy adott eljárás kimenetelét; egy 2016-os kutatásban alkalmazott algoritmus például az Emberi Jogok Európai Bírósága előtt folyamatban levő ügyek vizsgálata során 79%-os pontossággal jelezte előre a testület döntését (Aletras, Tsarapatsanis, Preoţiuc-Pietro & Lampos, 2016).

A gyenge MI a programozása és a rendelkezésre álló adatanyag korlátai közt elvileg szinte bármilyen kiszámítható logikai művelet, illetve műveletek

sorozatának végrehajtására képes lehet. A büntető ítélkező tevékenység egyes elemeiben tartalmaz matematikai, logikai számításokhoz hasonlatos vonásokat; így különösen a büntetéskiszabás körében, ahol a relatíve határozott szankciórendszer jegyében a Btk. 80. § (2) bekezdése határozott idejű szabadságvesztés kiszabása esetén az irányadó büntetési tételkereteken túl a bírói mérlegelés kiindulópontjaként a középmérték alkalmazását írja elő, figyelemmel az (1) bekezdésben foglalt büntetéskiszabási elvekre is.[3] Nem meglepő tehát, hogy a büntetéskiszabás az MI-ben rejlő lehetőségek kiaknázásának egyik elsődleges területe a büntetőeljárás bírósági szakaszában. Az Egyesült Államok területén már különféle döntéstámogató rendszerek segítik a bírákat a megfelelő szankció kiválasztásában a rendelkezésre álló információk, különösen az elkövető személyi körülményei, bűnügyi előélete alapján. Az MI általi adatelemzés elsődleges szempontja a bűnismétlés veszélyének kiszűrése, ennek érdekében az eszköz az elkövetőt egy kockázati értékelés alapján, általában egy háromfokú skálán, alacsony, közepes vagy magas kockázati kategóriába sorolja be (Harmati & Szabó, 2020).

Az erős MI azonban ennél is továbbmegy; az elképzelések szerint képes lehet értékelni az emberi döntéshozatalt befolyásoló, kevésbé kézzelfogható tényezőket is, mint amilyenek a bírói meggyőződés kialakulásában szerepet játszanak. A teljes gépi igazságszolgáltatás lehetősége tehát, habár az ehhez szükséges technológiát még nagyfokú bizonytalanság övezi, elvi szinten nem zárható ki.

A jogászság óvatosan közelíti meg az ítélkező MI koncepcióját. A leginkább kézenfekvő aggályok szerint a jogi munkától elválaszthatatlan emberi értékelő mozzanatban közreható pszichológiai folyamatok nem reprodukálhatók mesterséges úton (Nagy, 2020). Ennek ellenére, vagy talán éppen ezért az igazságszolgáltatás a deep learning-kutatás egyik kiemelt területe. Említést kell tenni ezen felül egy további aggályról az MI ítélkezési alkalmazása kapcsán, nevezetesen, hogy a gépi tanulás folyamatában könnyedén „porszem kerülhet a gépezetbe", amely a program döntési mechanizmusának rendellenességéhez vezethet. Közismert példa erre Tay, a Microsoft MI-alapú chatbotja, melyet 2016. március 23-án mutattak be a Twitteren, majd kevesebb mint 16 órán belül el is távolították, miután a program – internetes trollok közrehatására – közel százezer sértő, többek között rasszista tartalmú üzenetet tett közzé (Neff & Nagy, 2016). Az USA-ban az említett szankcionálási döntéstámogató rendszerek kapcsán ugyancsak felmerült az afroamerikai terheltekkel szembeni hátrányos megkülönböztetés veszélye. Az ilyen hibákat utólag rendkívül nehéz megállapítani

3 Nem feledve természetesen az 56/2007. BK vélemény iránymutatását, amely szerint a büntetési tényezőket nem szabad mechanikusan alkalmazni

és kiszűrni, tekintettel arra, hogy a programozóknak az algoritmus működésbe lépését követően gyakran nincs rálátásuk az automatizmus minden egyes lépésére. Nem hagyható figyelmen kívül továbbá az emberi tényező, vagyis az MI megalkotója; a legnagyobb jóhiszeműséget is feltételezve elkerülhetetlennek tűnik, hogy a programozó szubjektuma, előfeltevései valamilyen formában befolyásolják a program működését (Gravett, 2020).

Konklúzió

Bár a digitalizáció megítélése a büntető ítélkezésben nem újkeletű téma, az olyan technológiai fejlemények, mint az MI előretörése, valamint a COVID–19-járványhelyzet, az utóbbi években új megvilágításba helyezték azt. Az elektronikus ügyvitel, az egyre sokoldalúbb digitális eszközök jelentős mértékben hozzájárulnak a büntetőeljárás hatékonyságához, egyúttal az újfajta bűnözési formák felderítése, bizonyítása sajátos kihívások elé állítják az eljáró hatóságokat, de a téma kapcsán a jelen tanulmányban írtakat meghaladóan is számos további kérdés merül fel, melyeket a jogtudomány is kiemelt figyelemmel kísér (például prediktív rendészet). *„A prediktív rendészet az elemző – főleg kvantitatív módszerek – technikáknak egy olyan alkalmazása, amelyek beazonosítják a rendőrségi beavatkozás, a bűnmegelőzés, illetve a bűncselekményre adott válasz lehetséges célpontjait statisztikai és adatbányászati módszerekkel."* (Harmati & Szabó, 2020).

Ahogy Róth Erika rámutat, az informatikai eszközök térnyerése kifejezetten elősegítheti a terheltet megillető jogosultságok érvényesülését, mint a jelenlét joga vagy a védelemhez való jog (Róth, 2021). A digitális világ kihívásainak kezelése során, az útkeresés jelenlegi, átmeneti időszakában sem szabad azonban szem elől tévesztenünk azokat az elveket, amelyek az évszázadok alatt kialakult és a tisztességes eljárást biztosító modern büntetőeljárás jellegét adják, és talán az időszerűség és hatékonyság iránti igény fényében is indokolt az óvatosság az olyan kérdések megítélésében, mint akár az embert kiváltó, ítélkező mesterséges intelligencia.

Felhasznált irodalom

Aletras, N., Tsarapatsanis, D., Preoţiuc-Pietro, D. & Lampos, V. (2016). Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective. *PeerJ Computer Science, 2*(e93). https://doi.org/10.7717/peerj-cs.93

Ambrus I. (2021). *Digitalizáció és büntetőjog.* Wolters Kluwer Kft.

Berecz A., Karácsony P., Kónya L., Peck T., Szász G. & Vári-Kakas I. (2019). *Informatikai alapok*. Gábor Dénes Főiskola.

Czédli G. (2019). A bírósági eljárást gyorsító és fékező rendelkezések az új büntetőeljárási törvényben. *Büntetőjogi Szemle, 8*(1), 15–34.

Finszter G. (2021). A rejtőzködő bűn és a büntető hatalom. *Belügyi Szemle*, *69*(10), 1691–1707. https://doi.org/10.38146/BSZ.2021.10.1

Goodison, S. E., Woods, D., Barnum, J. D., Kemerer, A. R. & Jackson, B. A. (2019). *Identifying Law Enforcement Needs for Conducting Criminal Investigations Involving Evidence on the Dark Web.* RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2704/RAND_RR2704.pdf

Gravett, W. (2020). The dark side of artificial intelligence: Challenges for the Legal System. *Southern African Public Law, 35*(1), 13–27.

Grech, V. (2001). Publishing on the WWW. Part 5 – A brief history of the Internet and the World Wide Web. *Images in Paediatric Cardiology*, *3*(3), 15–22. https://www.researchgate.net/publication/221864858_Publishing_on_the_WWW_Part_5_-_A_brief_history_of_the_Internet_and_the_World_Wide_Web

Gyaraki R. (2018). *A számítógépes bűnözés nyomozásának problémái.* Doktori disszertáció. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola.

Harmati B. & Szabó I. (2020). A prediktív rendészet és az automatizált igazságszolgáltatás. *Belügyi Szemle, 68*(5), 23–37. https://doi.org/10.38146/BSZ.2020.5.2

Hati Cs. (2015). Egy eltűnt alapelv: a közvetlenség a büntetőeljárásban. In Elek B. & Miskolczi B. (Szerk.), *Úton a bírói meggyőződés felé. A készülő büntetőeljárási törvény kodifikációja* (pp. 159–177). Printart-Press.

Jámbor G. (2022). Raszternyomozás a kábítószer-bűncselekmények felderítésében. *Magyar Rendészet, 22*(3), 33–50. https://doi.org/10.32577/mr.2022.3.2

Máté I. Zs. (2017). *Az igazságügyi informatikai szakértő a büntetőeljárásban*. Doktori disszertáció. Pécsi Tudományegyetem Állam és Jogtudományi Kar Doktori Iskola.

Mezei K. (2019). *A kiberbűnözés egyes büntetőjogi szabályozási kérdései*. Doktori disszertáció. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola.

Miskolczi B. & Szathmáry Z. (2018). *Büntetőjogi kérdések az információk korában. Mesterséges intelligencia, Big Data, Profilozás*. HVG-ORAC.

Molnár Sz. (2018). A negyedik ipari forradalom nem várt hatásai. *Új Magyar Közigazgatás, 11*(3) 43–51. https://kozszov.org.hu/dokumentumok/UMK_2018/3/06_Negyedik_ipari_forradalom.pdf

Nagy A. (2020). Digitalizáció és mesterséges intelligencia a magyar igazságszolgáltatásban. *Miskolci Jogi Szemle, 15*(3), 105–111.

Neff, G. & Nagy, P. (2016). Talking to Bots: Symbiotic Agency and the Case of Tay. *International Journal of Communication, 8*(10), 4915–4931. https://ora.ox.ac.uk/objects/uuid:613f7303-8a07-4f5a-ada2-b495c9a449af/download_file?file_format=pdf&safe_filename=Neff_Nagy_2016_Talking%2BTo%2BBots.pdf&type_of_work=Journal+article

Polt P. (2021). A 21. század kihívásainak hatása a büntetőeljárásra. Kriptovaluták, azaz az új vagyoni értékek büntetőjogi kérdései. In Barabás, A. T. & Christián, L. (Szerk.), *Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére: Navigare necesse est* (pp. 419–428). Ludovika Egyetemi Kiadó.

Róth E. (2019). Az elektronikus adat mint új bizonyítási eszköz megjelenése a büntetőeljárási törvényben. *Miskolci Jogi Szemle*, *14*(2/2), 341–350.

Róth E. (2020). A digitalizáció hatása a büntetőeljárásra. *Miskolci Jogi Szemle, 15*(3), 165–174.

Tóth J. Z. (Szerk.) (2021). *A tisztességes eljáráshoz való jog.* Wolters Kluwer.

Ződi Zs. (2002). Az információs társadalom és a jog. *Gazdaság és Jog, 10*(7-8), 25–29.

Ződi Zs. (2018). A digitalizáció hatása a jogászi szakmára. *Gazdaság és Jog, 26*(12), 3–9.

Ződi Zs. (2020). A járvány, a jogi szféra és a technológia. *In Medias Res, 9*(2) 339–355.

A cikkben található online hivatkozások

URL1: *E-akta – Digitális Bíróság Projekt.* https://birosag.hu/birosagokrol/digitalis-birosag/e-akta

URL2: *Jelentős segítséget nyújt a veszélyhelyzet idején a bíróságok működésében a Via Video rendszer.* https://fovarositorvenyszek.birosag.hu/hirek/20200422/jelentos-segitseget-nyujt-veszelyhelyzet-idejen-birosagok-mukodeseben-video-rendszer

URL3: *Az Országos Bírósági Hivatal Elnökének 2019. évi beszámolója.* https://birosag.hu/sites/default/files/2020-11/obhe_2019_eves_beszamolo-1.pdf

URL4: *Az Országos Bírósági Hivatal Elnökének 2020. évi beszámolója.* https://birosag.hu/sites/default/files/2022-01/obhe_2020_eves_beszamolo.pdf

URL5: *Az Országos Bírósági Hivatal Elnökének 2021. évi beszámolója.* https://birosag.hu/sites/default/files/2023-04/obh_elnokenek_2021_evi_beszamoloja.pdf

Alkalmazott jogszabályok

Magyarország Alaptörvénye

A büntetőeljárásról szóló 1998. évi XIX. törvény

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény

Az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről szóló 2004. évi LXXIX. törvény

A bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról szóló 2009. évi XLVII. törvény

A Büntető Törvénykönyvről szóló 2012. évi C. törvény

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény
Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény
A büntetőeljárásról szóló 2017. évi XC. törvény
Az egyes büntetőjogi tárgyú és ehhez kapcsolódóan egyéb törvények módosításáról szóló 2021. évi CXXXIV. törvény
Az igazságügyi szakértői szakterületekről, valamint az azokhoz kapcsolódó képesítési és egyéb szakmai feltételekről szóló 9/2006. (II. 27.) IM rendelet
Az igazságügyi szakértői működésről szóló 31/2008. (XII. 31.) IRM rendelet
A titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről szóló 185/2016. (VII. 13.) Korm. rendelet
Az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet
Az Európai Parlament és a Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről
Az Európai Bizottság 2021/0106(COD) számú Javaslata
Alkotmánybírósági, bírósági határozatok
144/2008. (XI. 26.) AB határozat egyes bűnügyi nyilvántartási rendelkezések alkotmányellenességéről
56/2007. BK vélemény a büntetéskiszabás során értékelhető tényezőkről
EBD2014.B.8.
EBH2017.B.11.
Az Európai Unió Bíróságának C-293/12. és C-594/12. számú egyesített ítélete
Az Európai Unió Bíróságának C-203/15. és C-698/15. számú egyesített ítélete

A cikk APA szabály szerinti hivatkozása

Tóth M. M. (2024). A digitalizáció egyes kihívásai a büntetőeljárásban. *Belügyi Szemle*, *72*(2), 185-210. https://doi.org/10.38146/BSZ.2024.2.1

Nyilatkozatok

Összeférhetetlenség

A szerző nem jelentett összeférhetetlenséget.

Finanszírozás

A szerző nem kapott pénzügyi támogatást a kutatáshoz, a szerzőséghez és/vagy a cikk publikálásához.

Etikai nyilatkozat

Jelen cikkhez nem kapcsolódik adatkészlet.

Levelező szerző

A cikk levelező szerzője Tóth Marcell Máté, aki a tothmm@birosag.hu e-mail címen érhető el.