

ACTA UNIVERSITATIS SZEGEDIENSIS

FORVM

Acta Juridica et Politica

XII. évfolyam
1. szám

SZEGED
2022

Redigunt

TAMÁS ANTAL, ZSUZSANNA JUHÁSZ, KRISZTINA RÚZS MOLNÁR,
ZSOLT SZOMORA, NORBERT VARGA

Collegium scientiae actorum:

ATTILA BADÓ, MÁRTA DEZSŐ, ZSUZSANNA FEJES, KLÁRA GELLÉN,
ATTILA HARMATHY, JÓZSEF LICHTENSTEIN, BARNA MEZEY,
GÁBOR ROKOLYA, ARNDT SINN, BÉLA SZABÓ, ISTVÁN SZABÓ,
GERHARD THÜR

Redigit

MÁRIA HOMOKI-NAGY

Nota

FORVM Szeged

Szerkesztőbizottság:

ANTAL TAMÁS, JUHÁSZ ZSUZSANNA, RÚZS MOLNÁR KRISZTINA,
SZOMORA ZSOLT, VARGA NORBERT

A folyóirat tudományos testülete:

BADÓ ATTILA, DEZSŐ MÁRTA, FEJES ZSUZSANNA, GELLÉN KLÁRA,
HARMATHY ATTILA, LICHTENSTEIN JÓZSEF, MEZEY BARNA,
ROKOLYA GÁBOR, SINN ARNDT, SZABÓ BÉLA, SZABÓ ISTVÁN,
THÜR GERHARD

Főszerkesztő

HOMOKI-NAGY MÁRIA

Műszaki szerkesztő

MARVANEK JUDIT

Kiadja

GÖRÖG MÁRTA

dékán

Kiadványunk rövidítése

FORVM Szeged

ISSN 0324-6523 Acta Universitatis Szegediensis
ISSN 2063-2525 FORVM Acta Juridica et Politica

TARTALOMJEGYZÉK

BLUTMAN LÁSZLÓ Jogértelmezési módszerek és irányok az Alkotmánybíróságon.....	5
BODA ZOLTÁN – BAGOSSY MÁRIA Vitaindító a bírák és a bíróságok tekintélyének védelme érdekében történő fellépésről.....	31
FANTOLY ZSANETT Mesterséges intelligencia a büntetőeljárás nyomozási szakaszában.....	49
FARKAS CSABA – IVÁN DÁNIEL A koncessziós szerződés helye a honi kötelmi jog rendszerében.....	63
GÁL ANDOR Az elektronikus bizonyítéktranszfer megvalósítási lehetőségei az Európai Unió bűnügyi együttműködésében.....	81
GYÉMÁNT RICHÁRD Az Egyesült Államok „legveszélyesebb” tagállamai a kriminálgeográfiai és kriminálstatisztikai adatok tükrében, különös tekintettel a személy elleni erőszakos bűncselekményekre.....	95
JUHÁSZ ZSUZSANNA Mesterséges intelligencia és börtönkörnyezet?.....	125
MEZEI PÉTER Digitális felsőoktatás, szerzői jog és COVID-19 pandémia.....	141
NAGY ZSOLT A jogszociológia poszt- <i>weberi</i> perspektívája.....	157
TELEGDY GERGELY Gyakorlati észrevételek egy elméleti problémához – A hagyatékából kivont vagyon elemek.....	175

GÁL ANDOR*

Az elektronikus bizonyítéktranszfer megvalósítási lehetőségei az Európai Unió bűnügyi együttműködésében**

I. Bevezetés

A digitalizáció térnyerése életünk valamennyi területét, a gazdasági-társadalmi kapcsolatunkat, magán- és közjogi jogviszonyainkat egyaránt befolyásolja, így természetesen nem hagyja érintetlenül az állami büntetőigény érvényesítésének jogi teret adó büntetőeljárás lefolytatását sem. A büntetőjogi felelősségre vonás nézőpontjából a digitalizációs kihívások kétféleképpen jelentkeznek. Egyrészt a technológiai újításokban rejlő innováció nem maradhat kiaknázatlanul a bűnüldöző szervek tevékenységének ellátása során, alkalmazásuk révén ugyanis a büntetőeljárás időszerűbbé, hatékonyabbá, és gazdaságosabbá tehető, illetve ezáltal javítható az igazságszolgáltatáshoz való hozzáférés (*access to justice*) jogállami elvárása is.¹ Másfelől a bűnözés modernizálódása, részbeni digitális térbe helyeződése, és határokon átívelő jellege mind olyan tényezők, amelyek szükségképpen a büntetőeljárás jogi szabályozásának és infrastrukturális hátterének – az információs társadalom igényeihez igazodó – korszerűsítését követelik meg.² Ennek jegyében

* adjunktus, Szegedi Tudományegyetem Állam- és Jogtudományi Kar

** A kutatást a Szegedi Tudományegyetem Interdiszciplináris Kutatásfejlesztési és Innovációs Kiválósági Központ (IKIKK) Humán és Társadalomtudományi Klaszterének IKT és Társadalmi Kihívások Kompetenciaközpontja támogatta. A szerző a Mesterséges Intelligencia és a jogrend kutatócsoport tagja. The research was supported by the ICT and Societal Challenges Competence Centre of the Humanities and Social Sciences Cluster of the Centre of Excellence for Interdisciplinary Research, Development and Innovation of the University of Szeged. The author is a member of the Artificial Intelligence and the Legal Order (AILO) research group.

¹ Ehhez lásd ELEK BALÁZS: *Költség és időtartalékok a büntetőeljárásban*. Büntetőjogi Szemle 2015/1-2. 10. p.

² A kriminológiai kutatási eredmények rávilágítanak, hogy a bűnözés múltbeli alakulását és jövőbeni változásait a makrogazdasági és a demográfiai tényezők befolyásolják elsődlegesen. Ezen túlmenően azonban már harmadik befolyásoló szempontként veendő figyelembe a *technológia* fejlődése. KEREZSI KLÁRA – PAP ANDRÁS LÁSZLÓ: *A bűnözés és a bűnözéskontroll jövője*. In: Finszter Géza – Sabjanics István (szerk.): Biztonsági kihívások a 21. században. Budapest, Dialog Campus, 2017. 545. p. E tendenciák figyelembevételével alakult ki a nemzetközi szakirodalomban a *digitális kriminalitás* fogalma. Erre lásd SMITH, GAVIN J. D. – MOSES, LYRIA BENNETT– CHAN, JANET: *The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-Driven Approach*. The British Journal of Criminology Volume 57, Issue 2, 1 March 2017, 259–260. pp.

a büntetőeljárás digitalizációjára irányuló törekvések egyes törvényalkotási eredményei már a hazai büntetőeljárás törvényben is megtalálhatók.³

A fentiekben részletezett digitalizációs kihívások nem ismernek országhatárokat, így az azoknak való megfelelés igénye sem szűkülhet le a nemzeti jogalkalmazás szintjére, hanem az az Európai Unió tagállamai közötti bűnügyi együttműködés keretrendszerében is kiemelten jelentkezik.

Mindezekre figyelemmel indította el az Európai Bizottság a *Digital Criminal Justice* elnevezésű projektet, amely az alábbi elvek érvényre juttatása útján kívánja javítani az igazságszolgáltatáshoz való hozzáférést:⁴

- a határokon átnyúló igazságügyi együttműködésben résztvevő szervezeteknek biztonságosan kell kommunikálniuk és információt cserélniük digitális eszközökön keresztül (*biztonságos kommunikáció és a bűnügyi személyes adatok bizalmas kezelésének elve*);⁵
- biztosítani kell a tagállami bűnüldöző hatóságok és uniós szervek, illetve ügynökségek által használt informatikai rendszerek közötti átjárhatóságot (*interoperabilitás elve*);
- az érdekelt feleknek hatékonyan és a minőségbiztosítás követelményének szem előtt tartásával kell kezelniük az adatokat (*minőségi adatkezelés elve*);
- az európai digitális büntető igazságszolgáltatási térben résztvevő szervek által használt platformnak alkalmasnak kell lennie a határon átnyúló, és egymással személyi és/vagy tárgyi összefüggésben álló bűnelkövetések egymással való összekapcsolására (*büntetőügyek összekapcsolhatóságának elve*);
- a közös nyomozócsoportok létrehozásának és működtetésének folyamatát digitálisan támogatni, és ezáltal egyszerűsíteni kell;
- biztosítani kell az együttműködésben résztvevők számára a szükséges digitális eszközökhöz való hozzáférést (*digitális infrastruktúra biztosításának elve*).⁶

Megjegyzendő, hogy e modernizációs törekvések sikeressé tétele nem képzelhető el a *mesterséges intelligencia* alkalmazásában rejlő bűnüldözési előnyök kihasználása nélkül. Így értelemszerű, hogy a közeljövőben a tagállamok közötti bűnügyi együttműködés

³ Ezek bemutatására lásd HERKE CSONGOR: *A digitalizáció szerepe a büntetőeljárásban*. In: Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika*. PTE-ÁJK, MTA TK, Budapest-Pécs, 2019. 104–124. pp.; BARTKÓ RÓBERT: *Elektronikus kapcsolattartás a büntetőeljárásban*. In: G. Karácsony Gergely (szerk.): *Az elektronikus eljárások joga*. Gondolat Kiadó, Budapest, 2018. 73–98. pp.

⁴ Cross-border Digital Criminal Justice Final Report, 2020. [a továbbiakban DCJ Report]. Elérhető itt: <https://op.europa.eu/en/publication-detail/-/publication/e38795b5-f633-11ea-991b-01aa75ed71a1/language-en> (letöltés ideje: 2022.09.30.).

⁵ A kommunikációs csatornák biztonságának garantálása tehát nemcsak a bűnüldözés sikerét kívánja elősegíteni, hanem az adatvédelmi követelményeknek való megfelelés is csak ezáltal szavatolható. A rendvédelmi szervek jogszerű adatkezelése pedig a működésük számonkérhetősége szempontjából jelentős. VADÁSZ PÁL – ZÓDI ZSOLT: *A nemzetbiztonsági szolgálatok és a rendvédelmi szervek információkereséshez kapcsolódó számonkérhetősége*. Jogtudományi Közlöny, 2020/11. 519–520. pp.

⁶ DCJ Report 3-4.

hatékonyságának növelésében a mesterséges intelligenciának is meghatározó szerepe lesz. Ezen fejlesztési lehetőségek vizsgálata pedig jelen dolgozatnak is tárgya.

A bűnügyi együttműködés digitalizációjának egy külön területét jelenti az *elektronikus bizonyítékok* tagállamok közötti megosztása. Erre figyelemmel az Európai Tanács már a 2018. október 18-i következtetéseiben rámutatott arra, hogy megoldásokat kell találni az elektronikus bizonyítékokhoz való, határokon átnyúló gyors és hatékony hozzáférés biztosítására a terrorizmus, valamint a súlyos és szervezett bűnözés más formái elleni hatékony uniós, illetve nemzetközi szintű küzdelem érdekében, ennek keretében a jogalkotási ciklus végéig meg kell állapodni az elektronikus bizonyítékokra, a pénzügyi információkhoz való hozzáférésre, valamint a pénzmosás elleni hatékonyabb küzdelemre vonatkozó bizottsági javaslatokról.⁷

Az Európai Tanács álláspontja szerint az említett bizonyítéktranszfer azonban csak akkor lehet sikeres, ha a tagállami bűnüldöző hatóságok, illetve a velük közvetlen kapcsolatban álló Europol és az Eurojust megfelelő erőforrásokkal ellátása időközben megtörténik, mert csak így lehet szembenézni a technológiai fejlődésből, illetve a biztonsági fenyegetések folyamatosan változó természetéből eredő új kihívásokkal.⁸

Felismerve ezeket a követelményeket az Európai Bizottság már az említett következtetések publikálását megelőzően, 2018. április 17-én két jogalkotási javaslatot terjesztett elő az elektronikus bizonyítékok határokon átnyúló gyűjtésének fokozása érdekében. Ezek a következők: a büntetőügyekben az elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról rendeletről⁹ (a továbbiakban: Javaslát) és a büntetőeljárásban bizonyítékok összegyűjtése céljából a jogi képviselők kinevezéséről szóló irányelvről¹⁰ szóló javaslatok.

Így tehát az elektronikus bizonyítékok tagállamok közötti megosztására vonatkozó jogi szabályozás kialakítása előrehaladott állapotban van, a jogalkotási javaslatok elfogadása a közeljövőben várható.¹¹

⁷ Az Unió Tanácsa ezzel kapcsolatban 2018.12.13-i következtetéseivel pedig arra kérte fel a tagállamokat és a Bizottságot, hogy sürgősséggel hozzák létre az elektronikus bizonyítékok digitális cseréjére szolgáló rendszert, amelyben biztonságosan továbbíthatók az európai nyomozási határozatok, valamint a kölcsönös jogsegéllyel kapcsolatos megkeresések és válaszok. Lásd A Tanács következtetése: kölcsönös elismerés büntetőügyekben „A kölcsönös elismerés előmozdítása a kölcsönös bizalom erősítése révén” (2018/C 449/02). Az Európai Unió Hivatalos Lapja 2018.12.13. C 449/6.

⁸ Az Európai Tanács ülése (2018.10.18.) – II.9. számú következtetés. Brüsszel, 2018.10.18. EUCO 13/18.

⁹ A büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról szóló, az Európai Parlament és a Tanács rendeletére vonatkozó javaslat. Strasbourg, 2018.4.17. COM(2018) 225 final 2018/0108(COD) Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52018PC0225&from=EN> (letöltés ideje: 2022.09.26.).

¹⁰ A jogi képviselőknek a büntetőeljárásban bizonyítékok összegyűjtése céljából történő kinevezéséről szóló harmonizált szabályok meghatározásáról szóló európai parlamenti és tanácsi irányelvre vonatkozó javaslat. {SWD(2018) 118 final} {SWD(2018) 119 final} Elérhető itt: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52018PC0226&from=EN> (letöltés ideje: 2022.09.26.).

¹¹ Az Európai Parlament LIBE Bizottságának illetékes rapportőre jelentését már elkészítette, az Európai Unió Tanácsában az egyeztetések folyamata 2022. első félévében felgyorsult, így 2023-ban az említett instrumentumok elfogadása várható. A jelentésre elérhető itt: <https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-jd-cross-border-access-to-e-evidence-production-and-preservation-orders> (letöltés ideje: 2022.09.30.).

Mindezek alapján jelen tanulmány tárgya az elektronikus bizonyítékok tagállamok közötti cseréjét érintő végrehajtási kérdések vizsgálata, vagyis a bizonyítéktranszfer gyakorlati megvalósítási lehetőségeinek bemutatása. Éppen ezért nem céлом a szabályozástervezet kapcsán felmerülő büntetőeljárás, és elsősorban joghatósági dilemmák elemzése, hiszen azok önálló tudományos feldolgozást igényelnek, mint ahogy arra a jogirodalomban is találunk már példákat.¹²

II. Az elektronikus bizonyítékok közlésére és megőrzésére kötelező európai határozatokról szóló rendelettervezet szabályozási irányvonalai

Az elektronikus bizonyíték fogalma álláspontom szerint két irányból nyerhet értelmezést. Egyfelől értjük alatta az eleve elektronikus formában létrejövő valamennyi bizonyító erejű információt és adatot, amelyeket bináris formában tároltak vagy továbbítottak (pl. IP-címek, e-mailek, kép- és videófelvevételek stb.).¹³ Másrészt ezen ismérv alá vonandók azok az információk és adatok is, amelyek ugyan nem elektronikus formátumban jöttek létre, azonban később elektronizálásukra került sor, és ily módon digitális továbbításuk már lehetségessé vált. E felfogással egyébként a Javaslat legáldefiníciója is egybevág.¹⁴

De lege lata az ilyen formában rendelkezésre álló bizonyítékok cseréjére a büntetőügyekben kibocsátott európai nyomozási határozatról szóló 2014/41/EU irányelv (a továbbiakban: ENYH irányelv) lehet megfelelően alkalmazandó azzal, hogy az ENYH irányelv konkrét rendelkezést nem tartalmaz a bizonyítékok e típusához kapcsolódó bűnügyi együttműködést érintően. Az Európai Unió által készített hatásvizsgálatok azonban rámutattak arra, hogy ez az eszköz nem felel meg az időszerűség követelményének, hiszen átlagosan 10 hónap alatt történik egy ilyen típusú jogsegélykérelem teljesítése.¹⁵

Éppen erre figyelemmel a Javaslat be kívánja vezetni az uniós jogba a közlésre kötelező európai határozat és a megőrzésre kötelező európai határozat intézményét. A tervezet felfogásában *közlésre kötelező európai határozat* valamely tagállam kibocsátó hatóságának olyan kötelező határozata, amely azt írja elő az Unióban szolgáltatásokat nyújtó és más tagállamban letelepedett vagy képvisellel rendelkező szolgáltató számára, hogy

¹² KARSAI KRISZTINA: *Locus/Forum Regit Actum – a Dual Principle in Transnational Criminal Matters*. Hungarian Journal of Legal Studies, 2019/2. szám 155–172. pp.; ÁBRAHÁM MÁRTA: *A bizonyítékok gyűjtése és értékelése az EU-ban határokon átnyúló bűnözés esetén*. Miskolci Jogi Szemle, 2019/2. különszám. 1. kötet. 21–31. pp.; DORNFELD LÁSZLÓ: *A határokon átnyúló elektronikus bizonyítékgyűjtés szabályozása az EU-ban*. Infokommunikáció és Jog, 2019/2. 37–43. pp.; RÓTH ERIKA: *Az elektronikus adat megszerzését, megőrzését szolgáló büntetőeljárás kényszerintézkedések*. Infokommunikáció és Jog, 2021/2. 10–15. pp.

¹³ MEZEI KITTÍ: *Az elektronikus bizonyítékokkal kapcsolatos kihívások és szabályozási újdonságok*. Belügyi Szemle, 2019/10. 26. p.

¹⁴ A Javaslat 2. cikk (6) bekezdése szerint „elektronikus bizonyíték”: a szolgáltató által vagy nevében a közlésre vagy megőrzésre kötelező európai határozatra vonatkozó tanúsítvány átvételének időpontjában elektronikus formában tárolt bizonyíték, amely tárolt előfizetői adatokból, hozzáférési adatokból, tranzakciós adatokból és tartalmi adatokból áll.

¹⁵ Lásd a LIBE Bizottság rapportőrének jelentését: <https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-jd-cross-border-access-to-e-evidence-production-and-preservation-orders> (letöltés ideje: 2022. 09. 30.)

elektronikus bizonyítékot közöljön; míg a *megőrzésre kötelező európai határozat* valamely tagállam kibocsátó hatóságának olyan kötelező határozata, amely azt írja elő az Unióban szolgáltatásokat nyújtó és más tagállamban letelepedett vagy képvisellel rendelkező szolgáltató számára, hogy őrizzen meg elektronikus bizonyítékot a közlésre irányuló későbbi megkeresés érdekében.¹⁶

A Javaslat szerint mindkét határozatot valamely tagállam igazságügyi hatóságának kell kibocsátania. A határozat olyan, másik joghatósági területen található szolgáltató által tárolt adatok megőrzése vagy közlése érdekében bocsátható ki, amelyek nyomozások vagy büntetőeljárások során bizonyítékként szükségesek. Feltétel továbbá, hogy az eljárási cselekmény foganatosítása a kibocsátó tagállam nemzeti joga szerint is elvégezhető, és az egyben a szükségesség követelményének is megfelel.

A szabályozástervezet azt kívánja lehetővé tenni, hogy az egyik tagállam illetékes hatósága közvetlenül egy másik tagállamban letelepedett vagy képviselt szolgáltatótól kérhessen közlést vagy megőrzést a rendelet hatálya alá tartozó bűncselekmények kivizsgálásához és büntetőeljárás alá vonásához szükséges elektronikus adatokról.

A Javaslat messzemenőig meg kíván felelni az észszerűség és a hatékonyság követelményének azáltal, hogy a szolgáltató teljesítési határidejét 10 napban – kivételesen sürgős adatszolgáltatások esetében 6 órában – határozza meg [9. cikk (1)-(2) bekezdés].

A javaslat az egy vagy több tagállamban működő szolgáltatókra vonatkozik, függetlenül attól, hogy hol található a székhelyük vagy hol tárolják az információkat. E szabályozás lehetőséget biztosít a szolgáltató számára, hogy meghatározott indokok alapján – például technikai okokból, vagy nyilvánvalóan visszaélészerű vagy az Alapjogi Chartát sértő megrendelés esetén – a beérkezett határozat felülvizsgálatát kérje.¹⁷

A Javaslat koncepciója szerint a határozat címzettjének országában található társhatóságnak nem kell részt vennie közvetlenül a határozat kézbesítésében és végrehajtásában, kivéve, ha a címzett szolgáltató a határozatot nem teljesíti.¹⁸ Ebben az esetben a tagállami hatóságnak kell a végrehajtás iránt intézkednie a nemzeti jog irányadó szabályai szerint.

Mindezek alapján úgy tűnik, hogy a Javaslat szerint az elektronikus bizonyítékot kezelő szolgáltatónak a közlésre kötelező európai határozatban foglalt kötelezettség teljesítése érdekében a bizonyítékot közvetlenül, a végrehajtással érintett tagállam hatóságának bevonása nélkül kell a megkereső tagállami hatóságnak kiadnia. Álláspontom szerint ez a szabályozási koncepció kifogásolható tekintettel arra, hogy az nem felel meg az alapvető információbiztonsági követelményeknek.¹⁹ Ehhez képest szükséges lenne a Javaslatban kifejezetten szabályozni, hogy elektronikus bizonyíték továbbítására csak interoperábilis, biztonságos, decentralizált és egyben megfelelő autentikációs eljárást alkalmazó kommunikációs eszközön keresztül legyen lehetőség. Az említett követelményeknek való megfelelés érdekében szükségesnek tartom annak előírását, hogy az elektronikus bizonyíték szolgáltatása a szolgáltató székhelye szerint illetékes tagállami hatóság útján

¹⁶ Javaslat 2. cikk (1) és (2) bekezdés.

¹⁷ Lásd Javaslat 15. cikk.

¹⁸ Ehhez lásd a Javaslat 14. cikk.

¹⁹ A Javaslat kapcsán a LIBE Bizottság rapportőre is élt hasonló jelzéssel, azonban annak elfogadására vonatkozó jelzés – egyelőre – a Tanácstól nem érkezett. Ezzel kapcsolatban lásd a rapportőri jelentést: <https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-jd-cross-border-access-to-e-evidence-production-and-preservation-orders>

történjen. A tagállami hatóságok rendelkezhetnek ugyanis csak olyan kommunikációs eszközökkel, amelyek a fentiekben részletezett elvárások teljesítésére alkalmasak.

Ezen kötelezettségek teljesítése során a tagállami hatósággal való hatékony és gyors elektronikus kapcsolattartás jogi képviselő bevonásával is történhet, mint ahogyan e lehetőséggel a javaslatcsomagban foglalt másik jogalkotási kezdeményezés – a jogi képviselőknek a büntetőeljárásban bizonyítékok összegyűjtése céljából történő kinevezéséről szóló harmonizált szabályok meghatározásáról szóló európai parlamenti és tanácsi irányelvre vonatkozó javaslat²⁰ – kifejezetten számol is.²¹

A következőkben az Európai Unió büntügyi együttműködésében alkalmazott egyes, biztonságos információcserét szolgáló platformokat – az elektronikus bizonyítéktranszferre vonatkozó alkalmasság szempontjából – vizsgálom meg, rámutatva arra, hogy jelenleg is rendelkezésre állnak azok a csatornák, amelyek felhasználásával az előzőekben ismertetett de lege ferenda javaslatom a gyakorlatban is megvalósítható.

III. A büntügyi együttműködést koordináló szervek működésének digitalizációja

A bűnüldöző szervek tevékenységét érintően *kétirányú*: adminisztratív-szervezési-koordinációs, valamint a jogalkalmazást érintő érdemi felhasználásuk között lehet differenciálni. Előbbi kategóriába tartozó megoldások valójában a rendvédelmi szervek megfelelő feladatellátása adminisztratív oldalának javítását szolgálják. A második csoportba a szolgálatok azon nyílt és a nyilvánosság elől elzártan kifejtett tevékenységei tartoznak, amelyek célja a bűncselekmények megelőzésével és felderítésével kapcsolatos feladatok megvalósítása.²²

1. Adminisztratív-szervezési-koordinációs tevékenységek digitális ellátása

A technológiai újítások használata az adminisztratív tevékenységekre vonatkozóan többféle formában jelentkezhet: a büntetőeljárásban részt vevő szervezetek közötti kommunikáció javítása (pl. a hatóságok közötti videokonferencia útján lebonyolított távoli kommunikáció), a szolgálatok által kibocsátott és feldolgozott iratok elektronikus áramlásának biztosítása (pl. kizárólag elektronikus formátumú iratkezelés), bizonyos rendészeti cselekményeket automatizáló eszközök bevezetése (pl. beadványok készítése vagy bűncselekményekről szóló bejelentések kezelése) egyaránt az említett tevékenységfajták ellátását segítik elő.

²⁰ Lásd 10. ljt.

²¹ Az irányelv szabályozási koncepciója alapján az illetékes nemzeti hatóságok büntetőeljárásokban folytatott bizonyítékgyűjtésre irányuló határozatainak átvételére, az azoknak való megfelelésre és azok végrehajtására jogi képviselőt jelölhetnek ki. A bizonyítéktranszferet érintő adminisztratív akadályok ezt követő csökkentése a belső piac jobb működését biztosítaná, amely összhangban van a szabadságon, a biztonságon és a jog érvényesülésén alapuló közös térség fejlesztésével is.

²² DYMITRUK, MARIA: *Legal Tech in the Law Enforcement Agencies*. In: Szostek, Dariusz – Zalucki, Mariusz (szerk.): *Legal tech. Information technology tools in the administration of justice*. Nomos, 2022. 259–261. pp.

A technológiai piacon elérhető jogi iratautomatizálási szoftverek könnyen alkalmazhatók a szolgáltatók adminisztratív munkájában, mivel alkalmasak a szabványos iratelemek gyors előkészítésére.²³ Hasonlóan ehhez, megkönnyítheti a rendvédelmi szervek munkáját az automatikus beszédfelismerő (ASR) és az optikai karakterfelismerő (OCR) rendszerek elterjedése,²⁴ amelyek jelentősen felgyorsíthatják a formális tevékenységeket (pl. egy tanúvallomás rögzítése). A mesterséges intelligencia alkalmazása ebben a körben (is) hasznosulhat, így például egyes nyomozó hatóságok munkáját már rendőri chatbotok segítik, amelyek lehetővé teszik a bűncselekmények nyomozó hatóság részére történő azonnali bejelentését.²⁵ Úgyszintén segítséget jelenthet a mesterséges intelligencia az egyes elektronikus bizonyítékok rendszerezése, ügyekhez való kapcsolása során.

Az adminisztratív tevékenységek területén a technológiai eszközök alkalmazásának célja voltaképpen az ügyek feldolgozásának észszerűsítése és felgyorsítása. A digitalizációs fejlesztések ebben a körben történő használata bár fontos a szolgáltatások működésének egyszerűsítése szempontjából, azonban az még önmagában nem forradalmasítja a bűnüldöző szervek feladatellátását, és önmagától ettől az igazságszolgáltatás működése – informatikai szempontból – nem válik különbözővé a más ágazatokban uralkodó általános technológiai trendektől.²⁶ Az igazságszolgáltatási szervek együttműködése terén akkor érhető el tényleges előrelépés, ha a digitális eszközök használata az érdemi bűnüldözési feladatok megvalósítása során is dominánssá válik.

2. Az érdemi bűnüldöző tevékenységhez kapcsolódó legal-tech eszközök

A büntetőeljárások sikerét érdemben elősegítő digitális eszközök kimerítő felsorolása nyilvánvalóan nem lehetséges, ugyanakkor annak főbb területei²⁷ a következők szerint határozhatók meg:

- a bűncselekmények elkövetésének előrejelzése;
- a bűncselekmények és elkövetők felderítésének automatizálása;
- a döntéshozatali folyamatok automatizálása;

²³ Az automatikus dokumentumkészítő (*document assembly*) szoftverek lényegében szövegsablonok és algoritmusok (feltételes összefüggéseket tartalmazó kódolt szabályok) kombinációi. Ezek az eszközök az igazságszolgáltatást érintő technológiai újítások második generációjába tartoznak, amelyeket a jogi szakma hamar elkezdett használni. ZÓDI ZSOLT: *A járvány, a jogi szféra és a technológia. Hogyan vészelték át a jogrendszerek a járványt, mekkora szerepe volt ebben a technológiának, és mennyire lesznek tartósak a változások?* In *Medias Res*, 2020/2. 343-344. A *document assembly* rendszerek osztályozására lásd LAURINTSEN, MARC: *Document Automation*. In: KATZ, Daniel Martin et. al. (szerk.): *Legal Informatics*. Cambridge University Press, 2021. 69–72. pp.; KERY-TYERMAN, JONATHAN – SHANKAR, A. J.: *The Core Concepts of E-Discovery*. In: KATZ, DANIEL MARTIN et. al. (szerk.): *Legal Informatics*. Cambridge University Press, 2021. 311–312. pp.

²⁴ Bemutatókra lásd BOMMARITO, MICHAEL J.: *Preprocessing Data*. In: Katz, Daniel Martin et. al. (szerk.): *Legal Informatics*. Cambridge University Press, 2021. 58–60. pp.

²⁵ DYMITRUK 2022, 261. p.

²⁶ DYMITRUK 2022, 262. p.

²⁷ A szakirodalomban KARSAI utal rá, hogy e területen nagy jelentősége van az algoritmizált megoldások felhasználásának, amelyek lehetnek leíró (preskriptív) vagy előrejelző (prediktív) jellegűek. KARSAI KRISZTINA: *Inkrimínált algoritmusok a büntető igazságszolgáltatásban*. In: Madai Sándor – Pallagi Anikó – Polt Péter (szerk.) *Sic itur ad astra: Ünnepi kötet a 70 éves Blaskó Béla tiszteletére*. Budapest, Ludovika Egyetemi Kiadó, 2020. 253. p.

- a bizonyítékok automatizált elemzése, és
- a bizonyítékok, illetve elemzési eredmények hatóságok közötti megosztása.²⁸

Utóbbi terület érinti elsődlegesen a tagállamok közötti bűnügyi együttműködést koordináló szervek²⁹ működését, amelynek megvalósítási háttéréül – a tervek szerint túlnyomórészt – az e-Codex és az abba beépülő e-EDES rendszerei szolgálnak majd. Az Európai Unió e platformokat szánja ugyanis a digitális információ-megosztás jövőbeni fő színtereinek. Ezzel összhangban az Európai Bizottság javaslatot dolgozott ki a polgári és büntetőügyekben történő határokon átnyúló kommunikációra szolgáló számítógépes rendszerről (e-Codex rendszer) és az (EU) 2018/1726 (ún. eu-LISA) rendelet módosításáról, amelyet 2020. december 2-án tett közzé.³⁰

E javaslatra épülnek rá a következő, a közelmúltban, 2021. december 1-jén publikált további jogalkotási kezdeményezések:

- az igazságügyi együttműködés és az igazságszolgáltatáshoz való hozzáférés digitalizálásáról a határokon átnyúló polgári, kereskedelmi és büntetőügyekben, valamint egyes jogi aktusok módosításáról az igazságügyi együttműködés területén;³¹
- a terrorista bűncselekményekre vonatkozó információcseréről és együttműködésről szóló 2005/671/IB tanácsi határozatnak a személyes adatok védelmére vonatkozó uniós szabályokkal való összehangolásával összefüggő módosításáról;³²
- együttműködési platform létrehozása a közös nyomozócsoportok működésének támogatására és az (EU) 2018/1726 rendelet módosítása.³³

Az említett jogalkotási kezdeményezések szabályozási irányára a következőkben még kitérek.

²⁸ DYMITRUK 2022, 262. p.

²⁹ Ebbe a körbe sorolandók az EU bel- és igazságügyi ügynökségei [EU Justice and Home Affairs (JHA) agencies], amelyek önálló hálózatot alkotnak, tagjai: CEPOL (European Union Agency for Law Enforcement Training – Az Európai Unió Bűntüldözési Képzési Ügynöksége), EASO (European Asylum Support Office – Európai Menekültügyi Támogatási Hivatal), EIGE (European Institute for Gender Equality – Nemek Közötti Egyenlőség Európai Intézete), EMCDDA (European Monitoring Centre for Drugs and Drug Addiction - A Kábítószer és a Kábítószer-függőség Európai Megfigyelőközpontja), eu-LISA (Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice – A Szabadságon, a Biztonságon és a Jog Érvényesülésén Alapuló Téréség Nagyméretű IT-rendszereinek Üzemeltetési Igazgatását Végző Európai Ügynökség), Eurojust (European Union Agency for Criminal Justice Cooperation – Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége), Europol (European Police Office – Európai Rendőrségi Hivatal), FRA (Európai Unió Alapjogi Ügynöksége) és Frontex (European Border and Coast Guard Agency – Az Európai Határ- és Partvédelmi Ügynökség). 2020-ban az Eurojust koordinálta a hálózat tevékenységét és látta el a titkársági funkciót. 2021-ben a Frontex vette át az irányítást.

³⁰ Javaslat a polgári és büntetőügyekben történő határokon átnyúló kommunikációra szolgáló számítógépes rendszerről (e-CODEX rendszer) és az (EU) 2018/1726 rendelet módosításáról (2020.12.02.). COM(2020) 712 final 2020/0345(COD) Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CEEX:52020PC0712&from=EN> (letöltés ideje: 2022. 09. 30.). A Tanács előkészítő anyagát és általános megközelítését a javaslatról 2021. május 28-án tette közzé. Elérhető: <https://data.consilium.europa.eu/doc/document/ST-9005-2021-INIT/en/pdf> (letöltés ideje: 2022. 09. 30.).

³¹ Elérhető itt: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CE-EX:52021PC0759&from=EN> (letöltés ideje: 2022. 09. 30.)

³² Elérhető itt: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52021PC0767&from=EN> (letöltés ideje: 2022. 09. 30.)

³³ Elérhető itt: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52021PC0756&from=EN> (letöltés ideje: 2022. 09. 30.)

IV. A tagállamok közötti büntügyi együttműködés érdemi feladatainak ellátását szolgáló digitális eszközrendszer

1. Az e-Codex

Az e-Codex lényegében egy olyan, különböző szoftverösszetevőkből álló csomag, amely lehetővé teszi a felhasználói – az illetékes igazságügyi hatóságok, a gyakorló jogászok és a polgárok – számára, hogy a dokumentumokat, jogi űrlapokat, bizonyítékokat és egyéb információkat gyorsan és biztonságosan, *elektronikus úton* küldjék és fogadják.³⁴ Ezáltal az e-Codex biztosítja egy, a polgári és büntetőügyekhez informatikai támogatást nyújtó, a nemzeti informatikai rendszereket összekötő interoperábilis, biztonságos és decentralizált kommunikációs hálózat létrehozását.³⁵

Az e-Codex szabályozását célzó rendelet javaslatának indokolása szerint a tagállamok tapasztalataira építve az e-Codexben megvan a potenciál arra, hogy az Unióban a határon átnyúló büntetőeljárásoknál az elektronikus adatok biztonságos továbbításának fő digitális megoldásává váljék.³⁶

Az Európai Bizottság „Az igazságszolgáltatás digitalizálása az Európai Unióban – A lehetőségek eszköztára” című közleményében az e-Codexet tekinti a fő eszköznek a nemzeti informatikai rendszerek közötti kommunikációs hálózat létrehozásához.³⁷ E platform kiemelt előnye az, hogy a tagállami nemzeti rendszerek interoperabilitását biztonságos csatornán keresztül biztosítja. A büntügyi együttműködés terén álláspontom szerint e fejlesztés leginkább az európai nyomozási határozatok, elektronikus bizonyíték közlését célzó határozatok és kölcsönös eljárási jogsegélykérelmek végrehajtása során bírhat jelentőséggel, növelve a tagállamok közötti büntügyi tárgyú információ- és adatcserék hatékonyságát.

2. Az e-EDES

Az elektronikus bizonyítékok digitális cseréjére szolgáló rendszer [*e-Evidence Digital Exchange System – e-EDES*] egy olyan informatikai eszköz, amelynek segítségével a tagállamok hatóságai biztonságosan, digitális formában oszthatnak meg egymással európai nyomozási határozatokat, kölcsönös jogsegély iránti kérelmeket, valamint egyéb elektronizált vagy már elektronikus formában létrejött bizonyítékokat.

Jelenleg a hatóságok e célból postai, illetve elavultnak tekinthető elektronikus módszereket használnak, amelyek egyrészt lassúak, másrészt nem is rendelkeznek megfelelő

³⁴ Az e-Codexről mint a digitális igazságszolgáltatás meghatározó eszközéről szól OSZTOVITS ANDRÁS: *Online bíróságok és az igazságszolgáltatáshoz való jog – esély vagy veszély?* Magyar Jog, 2020/11. 631. p.

³⁵ <https://www.consilium.europa.eu/hu/press/press-releases/2021/06/07/digitalisation-of-justice-council-approves-its-mandate-for-negotiations-on-the-e-codex-system/> (letöltés ideje: 2021.11.10.)

³⁶ Javaslat a polgári és büntetőügyekben történő határon átnyúló kommunikációra szolgáló számítógépes rendszerről (e-CODEX rendszer) és az (EU) 2018/1726 rendelet módosításáról (2020.12.02.). COM(2020) 712 final 2020/0345(COD) Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52020PC0712&from=EN> (letöltés ideje: 2021.11.08.).

³⁷ Az Európai Bizottság 2020. december 2-i „Az igazságszolgáltatás digitalizációja az Európai Unióban Lehetőségek eszköztára” c. közleménye. COM(2020) 710 final. 3.5.

biztonsági szabványokkal. Éppen ezért az e-EDES létrehozásának célja az volt, hogy az említett adattípusok cseréjének biztonsága garantálható legyen, valamint a továbbított dokumentumok hitelességének és sértetlenségének ellenőrzési lehetősége mellett növelje a meglévő együttműködési eljárások hatékonyságát és gyorsaságát. Kialakítása egyúttal a nemzeti ügyviteli rendszerekkel való interoperabilitást is szolgálja.³⁸

Az e-EDES fejlesztésébe bevont tagállami szakértők határozottan decentralizált architektúrát kértek a rendszerhez, ami azt jelenti, hogy működése minden tagállamban egy biztonságos – nemzeti nyelven elérhető – portál üzemeltetését feltételezi. Kommunikációs csatornaként – az információcsere biztosítására – az internetet, valamint az eCodex Connector és az eDelivery átjárókat választották.³⁹

A DCJ Report meghatározott dokumentumoknak – *így különösen az elektronikus bizonyítékoknak* – a tagállami hatóságok közötti továbbítására kifejezetten az e-EDES-t ajánlja.⁴⁰ Az eszközt ugyanis az Európai Bizottság eleve az európai büntető igazságszolgáltatási tér igényeire szabta: az e-EDES közös nyílt szabványokon és nyílt forráskódú implementációkon (pl. e-Codex csatlakozó és Domibus Gateway) alapul.

Megjegyzendő azonban, hogy az e-EDES további fejlesztésre szorul, amely jelenleg – a 2020. október 1. és 2022. szeptember 30. közötti időszakban – az EXEC II projekt keretében valósul meg.⁴¹ Az EXEC II túlmutat a kezdeti digitalizációs törekvéseken, és lehetőséget ad a projektpartnereknek, hogy integrálják az e-EDES-környezetet nemzeti megoldásaikba. E platform használatának célja ugyanis kettős: először is lehetőség van az e-EDES környezet integrálására a nemzeti ügykezelési rendszerekbe az adatok cseréje és újrafelhasználása érdekében, másrészt ez viszont is igaz, vagyis a projektpartnerek integrálhatják nemzeti hitelesítési megoldásaikat a e-EDES rendszerbe, elkerülve ezzel a redundáns és hibára hajlamos felhasználói adminisztrációt, és egyúttal a meglévő felhasználói adatok újrafelhasználásával erősíthetik a platform használhatóságát.

Az EXEC II projekt további céljai a következők:

- a nemzeti ügykezelési rendszereknek az e-EDES platformba történő integrálása, amelynek köszönhetően a tárolt adatok újra felhasználhatók lehetnek mind a nemzeti nyilvántartás, mind az e-EDES számára;⁴²
- azonnali kommunikáció lehetővé tétele az érdekelt felek között (hasonlóan az Európai SIENA alkalmazásához);
- Eurojust számára – kezdetben csak a nemzeti összekötőkön keresztül – közvetlen hozzáférés biztosítása az e-EDES-hez;⁴³

³⁸ Az Európai Bizottság 2020. december 2-i „Az igazságszolgáltatás digitalizációja az Európai Unióban Lehetőségek eszköztára” c. közleménye. COM(2020) 710 final. 3.5.

³⁹ Council of the European Union Brussels, 2 March 2020; 6429/20.

⁴⁰ DCJ Report 101.

⁴¹ Az Európai Bizottság 2020. december 2-i „Az igazságszolgáltatás digitalizációja az Európai Unióban Lehetőségek eszköztára” c. közleménye. COM(2020) 710 final. 3.5.

⁴² <https://www.e-codex.eu/EXECII> (letöltés ideje: 2021. 12. 20.)

⁴³ Jelenleg az Eurojust mint ügynökség önállóan nem kapcsolódik az e-EDES-en belüli információcseréhez, azonban az Eurojust nemzeti összekötői ügyészi minőségükben megkaphatnak egyes dokumentumokat (pl. kölcsönös jogsegély iránti megkeresések teljesítése). DCJ Report 102.

- az elektronikus aláírások kezelése;
- mesterséges intelligencia alapú, gépi fordításra képes modul kialakítása.⁴⁴

Ezen túlmenően a jövőbeni fejlesztési tervek között szerepel az is, hogy az e-EDES tartalmazza az EJM Atlasz-eszközét,⁴⁵ amelynek köszönhetően az e-EDES-hez kapcsolódó társszervek képviselői felhasználóbarát módon találhatnak az ügyben eljárni illetékes hatóságot egy másik tagállamban.

3. Az Eurojust ügykezelési rendszere (CMS – Case Management System)

Az Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége (Eurojust) számára a tagállamok kötelesek minden olyan információt megadni, amelyre szüksége van az igazságügyi együttműködés és koordináció elősegítésére irányuló feladatának végrehajtásához.⁴⁶ E kötelezettségek teljesítése kihívás elé állítja a tagállamokat, mivel a Eurojust által használt platform kifejezetten elavultnak tekinthető.

Erre figyelemmel jelenthető ki az, hogy a Digital Criminal Justice projekten belül az Eurojust CMS újratervezése a határokon átnyúló digitális büntető igazságszolgáltatás informatikai modernizálásának egyik kulcseleme. Az előzetes tervek szerint az új, Eurojust által kialakítandó adatbázis fő összetevői a következők lennének: a Core CMS, a Terror-elhárítási Nyilvántartás, a JIT Admin Portál, az Action Day Collaboration Platform és az Integration Layer.⁴⁷

A Core CMS komponens az újratervezett Eurojust CMS részeként az Eurojust nemzeti irodák napi tevékenységét, azaz az Eurojust által támogatott, határokon átnyúló igazságügyi együttműködés minden ügyének nyilvántartását, kezelését és rögzítését támogató fő operációs rendszer.

A 2005/671/IB tanácsi határozat⁴⁸ előírja a tagállamok számára, hogy terrorcselekményekkel kapcsolatos információkat nyújtsanak az Eurojustnak. Ezért 2019-ban elindították a *Terrorelhárítási Nyilvántartást*, amely segíti az ügyészeket az aktívabb koordinációban, valamint a különböző országokban nyomozás alatt álló elkövetők vagy hálózatok azonosításában. E platform azonban jelenleg korlátozott funkciókkal rendelkezik, amely kiterjedt manuális beavatkozást igényel.⁴⁹

⁴⁴ DCJ Report 102.

⁴⁵ <https://www.ejm-crimjust.europa.eu/ejm/AtlasChooseCountry/EN> (letöltés ideje: 2022. 09. 30.)

⁴⁶ Az Európai Parlament és a Tanács 2018. november 14-i (EU) 2018/1727 rendelete az Európai Unió Büntető Igazságügyi Együttműködési Ügynökségéről (Eurojust) és a 2002/187/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről 21. cikk (3) bekezdés.

⁴⁷ DCJ Report 116.

⁴⁸ A Tanács 2005/671/IB határozata (2005.09.20.) a terrorista bűncselekményekre vonatkozó információcseréről és együttműködésről.

⁴⁹ DCJ Report 120.

Ezen adatbázis fejlesztésére irányuló folyamatok felgyorsítása érdekében élt az Európai Bizottság e tárgykörben jogalkotási kezdeményezéssel.⁵⁰ Az irányelvtervezet célja a 2005/671/IB tanácsi határozatnak a bünyügyi adatkezelési irányelvben⁵¹ megállapított elvekkel való összehangolása. A hivatkozott terrorelhárítási nyilvántartásban ugyanis személyes adat kezelése – a célhoz kötöttség elvével összhangban – kizárólag terrorista bűncselekmények megelőzése, kivizsgálása, felderítése és üldözése céljából történhet. A pontosan körülírt adatkezelési jogalapnak a tanácsi határozatba történő beépítése tehát szükséges annak érdekében, hogy a fejlesztendő nyilvántartás – az említett bűnüldözési célok mentén – hatékonyan működhessen.

A jelenlegi *JIT Admin Portál* a JIT támogatások adminisztrációját támogató eszköz.

Az *Action Day Collaboration Platform* olyan együttműködések digitális támogatására szolgálna, amelyek még nem minősülnek közös nyomozócsoportnak, ugyanakkor a tagállami szervek aktív és rendszeres kooperációját feltételezik. A közös nyomozócsoportok néhány hónaptól néhány évig működhetnek, ehhez képest az akciónapokhoz kapcsolódó együttműködés legfeljebb néhány hónapig tart. Fontos különbség emellett, hogy az akciónapi együttműködést az Eurojust koordinálja, míg közös nyomozócsoport az Eurojust bevonása nélkül is létrejöhet. Mindezek alapján az akciónapi együttműködések támogató elektronikus rendszert célszerűbb az Eurojuston belül elhelyezni, míg a közös nyomozócsoportok részére önálló digitális platform létrehozása indokolt.⁵²

V. Összegzés

A határon átnyúló szervezett bűnözés elkövetői a legmodernebb telekommunikációs eszközök felhasználásával fejtik ki tevékenységüket. E bűncselekmények elleni fellépés hatékonyságának növelése érdekében a rendvédelmi szerveknek lépéselőnybe kell(ene) kerülniük a korszerű technológiák alkalmazása terén.⁵³

Ehhez képest a nemzetközi elemet tartalmazó büntetőügyek intézése tekintetében az állapítható meg, hogy a papíralapú adminisztráció változatlanul túlsúlyban van. Éppen ezért az uniós jogi eljárások esetében is nélkülözhetetlen a digitális ügyintézésre való átállás felgyorsítása.

Különösen igaz ez az elvárás az elektronikus formában rendelkezésre álló bizonyítékok cseréjére, hiszen ezen együttműködési forma esetében a tagállami hatóságok közötti kapcsolattartás kizárólag digitális úton elképzelhető.

Ennek ellenére a jelenleg hatályban lévő uniós jogi aktusok nem határozzák meg az ilyenfajta adatátvitel közvetítő eszközét, és nem adnak e kapcsolattartási formára nézve

⁵⁰ Lásd 32. lj.

⁵¹ Az Európai Parlament és a Tanács 2016/680 (EU) irányelve (2016.04.27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről.

⁵² DCJ Report 124.

⁵³ VADÁSZ-ZÓDI 2020, 518. p.

háttérszabályozást sem. Ennek következtében a tagállami hatóságok egymás közötti, illetve az uniós szervekkel folytatott kommunikációja továbbra is lassú, költséges és adatbiztonsági szempontból kifogásolható kapcsolattartás keretében valósul meg.⁵⁴

E korszerűsítési kívánalmak szem előtt tartásával az Unió is felismerte, hogy a büntetőügyekben folytatott igazságügyi együttműködés terén a digitalizációban rejlő előnyök kiaknázása nem halasztható: mind a jogi, mind az infrastrukturális háttérnek az azonnali fejlesztése indokolt. Ennek jegyében indította útjára az Európai Bizottság a Digital Criminal Justice elnevezésű projektet, amelynek egyes eredményeit jelen tanulmány is taglalja.

Ezzel áll összhangban azon javaslatcsomag is, amely az elektronikus bizonyítéktranszfer jogi szabályozását célozza az elektronikus bizonyítékok közlésére és megőrzésére kötelező határozatok jogintézményének bevezetésével. Sajnálatos módon azonban a rendelettervezet jelenlegi formájában nem rendezi az adatszolgáltatás végrehajtási kérdéseit.

Ahogy arról jelen dolgozatban részletesen szóltam, az Európai Unió célkitűzésként határozta meg egy digitális igazságszolgáltatási térség kialakítását. Ennek keretében több biztonságos adatátvitelt szolgáló platform egyidejű kialakítása van folyamatban, amelyek használatával a tagállami és uniós rendvédelmi szervek kapcsolattartása gyorsabbá, hatékonyabbá és bűnüldözési, illetve adatvédelmi szempontból biztonságosabbá válhat.

A fentiekben rámutattam arra, hogy az Európai Unió a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségen belül a büntetőügyeket érintő fő digitális kommunikációs csatornának az e-Codexet, az e-EDES-t és az Eurojust modernizált CMS-ét szánja. A közeljövő feladata e rendszereknek egymással, más uniós adatbázisokkal (pl. VOCU,⁵⁵ SIENA,⁵⁶ JIT online felület stb.), valamint a tagállami nyilvántartásokkal történő megfeleltetése.

Álláspontom szerint szükséges az elektronikus bizonyítékok cseréjét is ezen platformok keretében lebonyolítani. A tanulmányban írtak alapján erre az e-EDES adatbázis tűnik a legmegfelelőbb eszköznek. Ezzel együtt garanciális jelentőségű lenne, hogy a bizonyíték-továbbítás eszközeként az e-EDES-t az elfogadásra váró rendelet kifejezetten nevesítse.

⁵⁴ Ahogyan arra MEZEI KITTI a szakirodalomban az elektronikus bizonyítékok hatóságok közötti megosztása kapcsán rámutatott: „[...] az ilyen adatok beszerzéséhez igazságügyi együttműködésre és kölcsönös jogsegélyre van szükség, azonban az eljárás lassú és nehézkes. Ma az olyan bűncselekmények csaknem kétharmada esetén nem lehet megfelelően lefolytatni a nyomozást és a büntetőeljárást, ahol más országban tárolnak elektronikus bizonyítékokat. Ennek az a fő oka, hogy rendkívül időigényes az ilyen bizonyítékok begyűjtése, illetve széttagolt a jelenlegi jogi szabályozás kerete.” MEZEI 2019, 32. p.

⁵⁵ A „Virtual Operations Coordination Unit” az OLAF által kifejlesztett, a csalásellenes információs rendszer (Anti-Fraud Information System – AFIS) alá tartozó IT-alkalmazás- és nyilvántartási rendszer, amely a tagállamok illetékes hatóságai és az OLAF között a bűnüldözés szempontjából operatív jellegű információk cseréjét segíti elő.

⁵⁶ A Secure Information Exchange Network Application (SIENA) egy, az Europol által használt, korszerű platform, amely lehetővé teszi a bűnüldözési célból rendelkezésre álló adatok gyors és felhasználóbarát cseréjét az Europol összekötő tisztjei, a tagállamok nyomozó hatóságok, valamint azon harmadik felek között, amelyekkel az Europol együttműködési megállapodást kötött.

ANDOR GÁL

THE POSSIBILITIES OF TRANSMISSION OF E-EVIDENCE IN THE
COOPERATION IN CRIMINAL MATTERS IN THE EUROPEAN
UNION

(Summary)

Digitalisation of justice aims to facilitate access to justice, improve overall efficiency, and ensure the resilience of justice systems in times of crises, such as the COVID-19 pandemic. Regarding criminal proceedings, the need for digitalisation is made even clearer by the modernization of crime, its partial digitalisation and its cross-border nature. It also follows from the international nature of the digitalisation challenges that the need to meet them cannot be reduced to the level of national law enforcement but is also reflected in the framework of criminal cooperation between the Member States of the European Union.

In accordance with all these a new challenge for the digitalization of justice is the exchange of electronic evidence. Adoption of the proposal for a regulation on the exchange of electronic evidence between member states is underway in the European Union. However, the proposal does not regulate execution issues related to the transmission of electronic evidence. Thus, there is a risk that the service providers will carry out official requests through insecure communication channels, even though the European Union already has platforms that are suitable for the transfer of evidence. Therefore, the aim of this paper to present the specifics of the legal-tech platforms already used by the European Union in this field and to be introduced in the future. Also, the paper examines the relevant legal background related to the operation of these platforms.