Jog-Állam-Politika, 2026/2.95
DOI: 10.58528/JAP.2026.18-2.95

BARTKÓ RÓBERT[1] – KELEMEN ROLAND[2],[3]

A migráció digitalizációja és az állami kontroll átalakulása az Európai Unióban

ABSTRACT

In recent years, the dynamics of irregular migration in the EU have increasingly been mediated by digital infrastructures, primarily smartphones, social media platforms, and encrypted messaging apps. Embedding in cyberspace creates opportunities for obtaining information, maintaining contacts, and organizing at the irregular level of migration, thus institutionalizing the phenomenon, while also strengthening the control exercised by the authorities (e.g., through the development of biometric systems, surveillance). The aim of this study is to explore the relationship between irregular migration and cyberspace in the context of trends visible at the EU's external borders after 2020, and it examines three main research questions: (1) How can we interpret the digitalisation of irregular migration; (2) How do digital channels influence the human smuggling networks; and (3) How do the digitalization affect EU's border control tools and measures? Based on the results of the study, digital tools have become the operating system of migration, accelerating the flow of information and coordination, while increasing exposure to exploitation and surveillance. At the same time, the interoperable database ecosystem creates a concentrated risk in the area of cyber resilience.

Keywords: irregular migration ■ cybersecurity ■ interoperability ■ digital migration ■ EU border control

I. BEVEZETÉS

[1] Habilitált egyetemi docens, Széchenyi István Egyetem, Deák Ferenc Állam- és Jogtudományi Kar, Bűnügyi Tudományok Tanszék, bartko.robert@ga.sze.hu.
MTMT: 10033153 * ORCID: 0000-0002-3547-4252 * Scopus ID: 57208659673.

[2] Tanszékvezető egyetemi docens, Széchenyi István Egyetem, Deák Ferenc Állam- és Jogtudományi Kar, Modern Technológiai és Kiberbiztonsági Jogi Tanszék.
MTMT: 10050826 * ORCID: 0000-0002-5419-8425 * Scopus ID: 58283156900.

[3] A tanulmány elkészítéséhez a Kulturális és Innovációs Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott STARTING_25 pályázati program nyújtott támogatást

Az Európai Uniót érő migrációs – ideértve annak irreguláris formáját is – nyomás egyszerre geopolitikai, humanitárius, valamint egyre inkább technológiai kihívást is jelent. A digitális fejlődés visszavonhatatlanul változtatta meg a globális emberi mobilitás terrénumát, beleértve az irreguláris migráció összetett dinamikáját is. A kibertér – bár korábban perifériku s tényező volt –, ma már központi szerepet tölt be a migrációban, hiszen befolyásolja a migrációs útvonalak alakulását, valamint az embercsempészésre épülő szervezett bűnözői csoportok működését.

Az Európai Unió külső határait érintő irreguláris határátlépési trend elemzése és értelmezésekor a kibertér szerepe ezért megkerülhetetlenné válik. A kérdést vizsgáló nemzetközi szakirodalom is rámutat arra,[4] hogy a digitális eszköztár (így az okostelefon, a térképszoftverek, az üzenetküldő és közösségi platformok) a döntéstől az út közbeni kockázatelemzésen át egészen a célországban történő ügyintézésig végigkíséri a migrációs hullám tagjait,[5] ugyanakkor az *„empowerment-control"* elv[6] alapján az is jól látható, hogy a kibertérben rejlő lehetőségek nemcsak a migránsok, hanem az állami szereplők szolgálatában is állnak.

Ezért, amikor a két jelenség, azaz a kibertér és az (irreguláris) migráció kapcsolatát vizsgáljuk, rá kell mutatnunk ezen reláció sokszínűségére. Így vizsgálni szükséges, hogy a digitális eszközök, az interneten elérhető adatok milyen módon befolyásolják a migrációs útvonalak alakulását, az utazás megtervezését és az azzal kapcsolatos kockázatok kezelését. Szükségképpen ki kell térnünk az irreguláris migráció „motorjaként" értékelhető embercsempész-hálózatok digitalizálódására, platformizálódására, és természetesen harmadrészt a bevezetőben említett „empowerment-control" elv alapján a digitális határigazgatás működésére, annak irreguláris migrációra gyakorolt hatásaira. Az absztraktban említett kutatási kérdéseink megfogalmazását is ezen gondolatok, kiindulási pontok vezérelték. A tanulmány ezért alapvetően elméletvezérelt szintézist kíván teremteni a fenti kérdésekben, alapul véve a FRONTEX határrendészeti statisztikai adatait, valamint a témával foglalkozó releváns európai szakirodalmat. Itt azonban fontos kiemelni, hogy számos nemzetközi tanulmány a „menekült" kifejezést használja, és ezen kategória vonatkozásában végzi el elemzését. Témánk szempontjából azonban ezen írások is alapul szolgálhattak kutatásainknak.

Ugyanakkor jeleznünk szükséges, hogy a telekommunikációs eszközök a migrációnak nemcsak az irreguláris, hanem a reguláris formájához is kapcsolódnak, ezt elvitatni nem lenne megalapozott tudományos állítás. Azonban jelentős különbségek mutatkoznak a két hatásmechanizmus között. A reguláris migráció tagjai a digitális eszközöket elsősorban ügyintézésre, hivatalos kommunikációra, családtagokkal való kapcsolattartásra, integrációjuk elősegítésére használ-

[4] Eide, 2020, 67-81.; Netto, 2021, 542-559.
[5] Josipovic, 2023, 534-551.; Ponzanesi – Leurs, 2022, 103-121.
[6] Nedelcu – Soysüren, 2022, 1821-1837.

ják, főként annak köszönhetően is, hogy az ezen jelenséghez kapcsolódó alapvető állami folyamatok (pl. vízumkérelmek, időpontfoglalás, adminisztráció) sok területen már digitalizáltak. A migráció irreguláris formája esetén a személyek ezeket a hagyományos „útvonalakat, módszereket" kívánják elkerülni a digitális eszközök segítségével, esetükben a digitális eszközök a „túlélés eszközeivé" válhatnak és egyértelműen felerősítik az ahhoz kapcsolódva működő bűnözői hálózatok rugalmasságát és rejtettségét. A fent említett és a szakirodalomban kirajzolódó *„empowerment-control"* elv mentén pedig az is rögzíthető, hogy addig, amíg a reguláris migráció esetében a digitalizáció egyfajta kényelmi, adminisztratív előnyt jelent, addig az irreguláris migránsok esetén azok láthatóságát és így a könnyebb és eredményesebb detektálásuk esélyét növeli.

II. KIINDULÓ MEGÁLLAPÍTÁSOK

Az Európai Unió migrációs – ideértve az irregulárist is – térképének mikénti alakulására alapvetően két tényezőcsoport van releváns hatással. Egyrészt a kibocsátó államokban kialakult geopolitikai instabilitások, politikai konfliktusok, gazdasági válsághelyzetek, melyek nagy sebességgel képesek átrendezni az egyes útvonalakat, azok terheltségét – és ezek kiválasztásában tud a kibertér jelentős segítséget nyújtani –, másrészt pedig a migráció „digitális közvetítettsége", amelyhez mind az uniós szintű, mind pedig a tagállami szintű szabályozás nehezen tud igazodni. Az első tényezőt egyértelműen alátámasztják a FRONTEX éves jelentései is, melyek a trendek változását, ezzel összefüggésben az irreguláris migráció és az azt kísérő embercsempészet rezilienciáját mutatják. Bár a FRONTEX adatai nem azonosak az egyedi irreguláris migrációt meghatározó személyszámmal, az eseményszintű mutatók azonban meghatározók. Addig, amíg 2021-ben[7] nagyságrendileg 200.000 volt a detektált jogellenes határátlépések száma, addig 2022-ben[8] ez már 330.000, 2023-ban[9] már 380.000 volt. A számok az elmúlt két évben mutattak csökkenést a 2024-es[10] becsült 239.000 fővel, valamint a 2025-ös[11] 178.000 fővel. A számok visszaesést mutatnak, mely főként a határőrizeti rendszer hatékonyságának fokozásával magyarázható, melyben a digitalizációnak szintén fontos szerep jut. A csökkenésnek tehát egyik, de nem kizárólagos oka, hogy az EU, de más tranzitország is szigorította a fizikai és operatív határőrizeti intézkedéseit, amellyel eredményesebben tudnak fellépni az egyes embercsempész hálózatokkal szemben is.

[7] Frontex, 2022.
[8] Frontex, 2023.
[9] Frontex, 2024.
[10] Frontex 2025.
[11] Frontex, 2026.

A másik tényező a fentebb már említett digitalizáció, amely három értelmezhető szinten kapcsolódik a migrációhoz, valamint annak irreguláris formájához. Az első az úgynevezett alsó szint, a migrációs hullám résztvevőinek szintje, ahol az internetképes okoseszközök a migránsok közötti kapcsolattartás, a navigáció, az információszerzés, valamint a különféle pénzügyi tranzakciók elvégzésének eszközei.[12] Az (irreguláris) migránsok telefonhasználata mára empirikusan is alátámasztott jelenség, az aktív eszközhasználat pedig növeli ezen személyek „digitális lábnyomát". A második a középső szint, ami a tulajdonképpeni embercsempészet síkja. A csempészet a tapasztalatok, valamint az Európai Bizottság összefoglaló munkaanyaga alapján „platformizálódik", egyre inkább digitális, végpontok között titkosított csatornákon kerül sor a hirdetések közzétételére, a csempészet menedzselésére, valamint a fizetési műveletek koordinációjára. Ezzel a piac jóval rugalmasabb, és nehezebben felderíthető.[13] A harmadik az ún. felsőszint, vagy állami szint, ami tulajdonképpen az EU digitális határigazgatási megoldásait foglalja magában, amely az ún. „retrospektív határkontroll" eszközévé vált. Az így lehetővé vált adatszerzések természetesen számos adatvédelmi és emberi jogi dilemmát is felvetnek, ugyanakkor ezen kérdések vizsgálata jelen tanulmány terjedelmi kereteit feszítené szét, így azokkal kutatásunkban csak érintőlegesen, a probléma jelzése szintjén foglalkozunk.

A fentiek alapján tanulmányunk központi tézise, hogy az irreguláris migráció és a kibertér kapcsolata egyszerre kétirányú, ugyanakkor ambivalens is. A titkosított kommunikáció, a digitális és okoseszközök, a modern technológia nemcsak szolgálják és támogatják az irreguláris migrációt, hanem egyben növelik is az állami kontrollt és annak hatékonyságát, ezáltal pedig a jogellenesen az Unió területére belépni szándékozók detektálásának esélyét, sérülékenységük kockázatát.[14]

III. A DIGITALIZÁCIÓ ÉRTELMEZÉSI SÍKJAI AZ IRREGULÁRIS MIGRÁCIÓVAL ÖSSZEFÜGGÉSBEN

1. Az irreguláris migráció digitális eszközhasználata

A digitális technológiák, különösen az internetkapcsolattal rendelkező okostelefonok alapvető eszközök azoknak a kezében, akik irreguláris migrációs útvonalakat terveznek, szerveznek, vagy éppen követnek. Ezek az eszközök bőséges információval tudják őket ellátni, kommunikációs csatornákat nyitnak, létfontosságú navigációs képességeket kínálnak számukra.[15] Ezen személyek gyakran online platformokat,

[12] Eide, 2020, 72-75.
[13] European Commission, 2021.
[14] Geirgiou – d'Haenens – Zaki – Donoso – Bossens, 2024, 277-285.
[15] Eide, 2020, 67-81.; Lintner, 2025.

közösségimédia-felületeket, végpontok közötti titkosítást biztosító üzenetküldő alkalmazásokat használnak, közülük is Lintner 2025-ös kutatása szerint a WhatsApp mobilapplikáció népszerű. Gursky és Woolley megállapításai szerint pedig a Signal és a Telegram is ilyennek tekinthető, egyéb közösségi platformok mellett.[16] Ezekkel az irreguláris migránsok képessé válnak arra, hogy megfelelő célországokat találjanak, megértsék és adott esetben megkerüljék a határellenőrzési eljárásokat, mások által dokumentált tapasztalatokat gyűjtsenek. Kutatások ugyanakkor alátámasztották azt is, hogy a migránsok körében a mobiltelefon egyfajta „társas támasz" és az utazással járó nehézségekkel történő gyakorlati megküzdés eszköze is egyben. Azonban a gyakori, hálózati lefedettség hiányosságából eredő problémák, vagy éppen a félrevezető információk komoly kockázatokat hordoznak magukban számukra. A metaadatok, az egyes okoseszközökön tárolt adatok pedig digitális bizonyítékként szolgálnak az egyes idegenrendészeti eljárásokban, hiszen egyre több ország vezette be az ún. adatkinyerés módszerét.[17] Ennek alkalmazása során a határrendészeti hatóságok a migránsok személyes digitális eszközeiről adatokat másolnak le és elemzik annak megállapítására, honnan érkeztek, milyen útvonalat követtek, vagy éppen, hogy van-e kapcsolatuk bármilyen embercsempész hálózattal. Ez természetesen súlyos adatvédelmi, akár személyiségi jogi kérdéseket is felvet, azonban jelen tanulmánynak nem tárgya ezekkel foglalkozni, mert túlmutatna a kutatás fókuszán. Összefoglalva elmondható, hogy az okoseszközök és az end-to-end titkosított üzenetküldő fórumok nemcsak a magánélet védelme szempontjából, hanem gyakorlati okokból is népszerűek az irreguláris migránsok körében is. Azonban ezen eszközök alkalmazása egyben súlyos kitettséget is okoz esetükben, hiszen a telefon által tárolt metaadatok egyfajta digitális nyomként szolgálnak a hatóságok számára.

2. Az embercsempészet digitalizációja

Az EU szakpolitikai jelentése szerint az irreguláris határátlépések jelentős része csempészhálózatok segítségével valósul meg.[18] A digitális infrastruktúrában rejlő lehetőségeket a bűnözői csoportok is kiaknázzák, akik jellemzően az embercsempészetben és az emberkereskedelemben érdekeltek. Egyes útvonalakon – ilyen például a közép-mediterrán útvonal – egyre inkább elmosódnak a határok a csempészek és a kereskedők között.[19] Ezek a szervezetek a digitális eszközöket működésük szinte minden szegmensében használják, tágítva ezzel földrajzi lefedettségüket, rugalmasságukat és a bűnüldöző hatóságokkal szembeni ellenálló képességüket. A csempészek és kereskedők az internetet és internetalapú technológiákat használnak összetett logisztikai feladataik megtervezésére, a migránsok mozgásának koordinálására, illegális szolgáltatásaik hirdetésére, toborzásra,

[16] Gursky – Woolley, 2021.
[17] Jagerovic, 2025, 179-198.
[18] European Commission, 2021.
[19] Bish – Cockbain – Walsh – Borrion, 2024, 70-94.

útvonalaik és módszereik gyors adaptálására a változó határrendészeti intézkedésekre reagálva, valamint a fizetések megszervezésére is.[20] Utóbbi tekintetben kiemelendő, hogy olyan kriptovalutákat, mint a Bitcoin, a Tether vagy éppen a Monero, egyre gyakrabban alkalmaznak a fent megjelölt bűnözői csoportok.[21] Ezek mellett általában a stabilabb árfolyam, az azonnali utalhatóság, valamint a titkosított jelleg szól. Látható tehát, hogy a csempészek és kereskedők a digitális kommunikációt a személyes kapcsolatok csökkentésére, a tettenérési kockázat minimalizálására használják, ezzel kiépítve egy önállóan működő, egymástól elválasztható, de mégis összekapcsolt modulokra épülő rendszert. A digitális csatornák hozzájárulnak a csempészet fent jelzett „modularizálódásához", valamint gyorsítják annak önálló piaccá válását.[22] A titkosított kommunikációs lehetőségeket a bűnözői csoportok is kihasználják, ami egyszerre nehezíti és segíti a felderítést a különféle digitális nyomok segítségével.[23] A hálózatok *„interconnected and digital"* működési szisztémája a kiberteret a szolgáltatáskínálat szélesítésére, profitmaximalizálásra használja, amely tudományos nézőpontból összekapcsolható a tanulmányunk induló tézisével, hiszen ugyanazok a csatornák, amelyek az irreguláris migránsokat segíthetik, csempészoldalon a kizsákmányolás és akár az erőszak infrastruktúrái is lehetnek. Összességében második kutatási kérdésünk kapcsán látni kell, hogy a csempészet – illetve egyes esetekben az emberkereskedelem – digitális csatornákon történő szerveződése növeli a bűnözői hálózatok alkalmazkodási képességeit és csökkentheti közvetlen kitettségüket, egyben a hatóságok számára új, digitális nyomokat is létrehoz, amely uniós szinten is felveti a kiberbiztonság, a határvédelem és a platformszabályozás metszéspontjainak vizsgálati kényszerét.

3. Az EU digitális határigazgatása – a „digitális határrezsim" modellje

Az Európai Unió célja az elmúlt években nagy adatbázisainak összekapcsolása, a migráció hatékonyabb kezelése érdekében. Az egyes információs rendszerek interoperabilitása olyan adatállomány előállítására alkalmas, amely egyrészt képes biztosítani a határellenőrzések hatékonyságát, ugyanakkor komoly alapjogi kockázatokat is magában hordoz, hiszen ez alapot adhat arra, hogy a határigazgatási, azaz a kifejezetten migrációs célú adatbázisok a rendészeti célzatúakkal összemosódjanak. Ezzel pedig sérülhetnek adatvédelmi szempontok, és veszélybe kerülhet az adatkezelés és az emberi jogi szempontok metszetében a szükségesség-arányosság elve is.[24] A szakirodalomban szintén éles támadások kereszttüzében van a migránsoktól lefoglalt okostelefonokról történő adatki-

[20] Europol, 2024.
[21] TRM Team, 2025.
[22] European Commission, 2021; Nedelcu – Soysüren, 2022.
[23] Case Note, 2022.
[24] Bredström – Krifors – Mesic, 2022, 68-81.; Blasi, 2021, 433-457.

nyerési eljárás is, mely alapját képezi annak a retrospektív szemléletű elemzésnek és határellenőrzésnek, melyek révén a hatóságok szenzitív adatokhoz tudnak hozzájutni határrendészeti célokra, hatósági feladatokra hivatkozással.[25] Ezt a módszert tulajdonképpen az európai határellenőrzés intelligenssé és digitálissá válása eredményezte, az EURODAC, a SIS és a VIS rendszerek adatbázis bővítésével és a fentiekben már említett interoperabilitásával. Összességében tehát az a megállapítás tehető, hogy az EU digitális kontrollrendszerei a láthatóság és a bizonyítás egy egészen új rezsimjét hozták létre, amelyek alapjogi és kiberbiztonsági kockázatokat egyaránt hordoznak, ugyanakkor a szintén a kibertérben aktív irreguláris migráció digitális adaptációját is eredményezik.

Az uniós szintű kiberbiztonsági kockázatot csak tovább fokozza, hogy az Európai Unió Migrációs és Menekültügyi Paktuma[26] 2026. június 12. napjától van érvényben, míg az ún. „uniós okos határok" szempontjából fontos EES (Entry/Exit System)[27] teljeskörű implementációjának végső határideje 2026. április 10. Az új rendszerek indulása mellett a 2019/817 (EU) rendeletben nevesített informatikai struktúrák és adatbázisok (EES, VIS, ETIAS, EURODAC, SIS, ECRIS-TCN) összekapcsolása – bár kétségkívül vannak operatív előnyei, de – a kiberbiztonsági kockázatot is összekapcsolttá teszi. Ha a rendszer egy pontja valamilyen incidens miatt sérül, a horizontális terjedés szinte elkerülhetetlenné válik. Ráadásul ezek a rendszerek rendkívül szenzitív adatokat (pl. biometrikus azonosítók, személyazonosító adatok, utazási mintázatok) tárolnak, amely a jövőben az EU-ban is rendszerszintű kockázatértékelést fog igényelni. Akár az adatlopás vagy adatszivárgás, akár egy terheléses támadás vagy rendszerleállás is komoly rizikófaktor. A rendszerek összekapcsolásával előálló okos határvédelem magában hordozza a *„function creep"*,[28] azaz a kezdeti céloktól elmozduló, azokon jelentősen túlterjeszkedő használat lehetőségét, amely csak tovább fokozhatja a jövőben az alapjogi problémákat. A Paktum, valamint a fentiekben említett okosrendszerek 2026-os élesítésével az európai határellenőrzés egy erősen digitális alapokon szerveződő ökoszisztémává válik, amely egyszerre válik majd adatintenzívvé, interoperabilisabbá, digitáliskontroll-centrikusabbá. Kiberbiztonsági nyelvre lefordítva a problémát: az Európai Unió határigazgatásának teljes digitalizálásával nő a támadási felület, a rendszerkomplexitás, valamint a koncentráltan kezelt adatállomány, amely komoly kibertámadási ok lehet. Annak eredményessége esetén pedig a következmények kiszámíthatatlanok.

[25] Josipovic, 2023, 534-551.; Josipovic, 2024, 1831-1854.
[26] European Commission, 2024.
[27] European Union, 2026.
[28] A koncepcióval kapcsolatban lásd: Koops, 2021, 29-56.

IV. FELHATALMAZÁS ÉS KONTROLL DINAMIKÁJA A DIGITÁLIS KÖRNYEZETBEN

A digitális migrációs ökoszisztéma elemzése a korábbi fejezetekben azt mutatta meg, hogy az egyéni migránsok digitális praxisai, a platformizált csempészhálózatok működése és az uniós interoperábilis határrendszerek nem elszigetelt jelenségek, hanem egymást kölcsönösen alakító folyamatok részei. E kölcsönhatások eredményeként a közigazgatási eljárások, a biztonsági racionalitások és a digitális infrastruktúrák egyre szorosabban fonódnak össze, miközben a határ nem csupán térbeli, hanem adat- és döntési architektúrák mentén is újratermelődik. Ezt az állami működési logikát ragadja meg a *cyberfare state* fogalma, amely nem önálló államelméleti modellként, hanem analitikus keretként értelmezi azt a folyamatot, amelyben a mindennapi igazgatási gyakorlatok fokozatosan biztonsági funkciókkal telítődnek, és technológiailag közvetített döntési láncokba ágyazódnak.[29]

Ebben a megközelítésben a cyberfare state nem a kritikai *border studies* irodalmát váltja fel, hanem kiegészíti és továbbgondolja azt. Míg a kritikai határkutatások elsősorban azt mutatják meg, hogy a határ mint gyakorlat miként oszlik szét társadalmi, technológiai és intézményi folyamatokban, addig a cyberfare state koncepció az ezekből összeálló állami szintű konszolidációra helyezi a hangsúlyt. Arra irányítja a figyelmet, hogy a digitális rendszerek révén a mindennapi közigazgatási eljárások egyre inkább biztonsági funkciókkal telítődnek, és az állami hatalomgyakorlás nem csupán a fizikai határokon, hanem az interoperábilis adatarchitektúrákon keresztül is érvényesül.[30]

A koncepció többletértéke a kapcsolódó fogalmakkal – így a digitális szuverenitás vagy a total security environment – szemben abban ragadható meg, hogy nem pusztán az adatkontroll vagy a biztonsági logikák kiterjedését írja le, hanem azok kormányzási következményeit vizsgálja. A cyberfare state perspektívája azt emeli ki, miként alakul át a jogi felelősség, a diszkréció és a legitimáció akkor, amikor a biztonsági célkitűzések automatizált és interoperábilis rendszerekbe ágyazódnak.[31] E nézőpontból a központi kihívás nem kizárólag a megfigyelés intenzívebbé válása, hanem egy olyan állami működési modell megjelenése, amelyben a politikai és jogi döntések egyre inkább technikai rendszereken keresztül közvetítődnek – és részben el is fedődnek –, új típusú algoritmikus diszkréciót és intézményi átláthatatlanságot eredményezve.[32]

A tanulmány az irreguláris migráció digitális átalakulását három szinten szintetizálta: az egyéni migráns, a csempészhálózatok és az EU állami apparátusa felől. E perspektívák integrálása feltárja, hogy a kibertér és a migráció kapcsolata nem pusztán technikai evolúció, hanem egy dinamikus, kölcsönös alkalmazkodási folyamat. Az eredmények arra utalnak, hogy az „*empowerment–control*

[29] Kelemen, 2026.
[30] Trauttmansdorff, 2024; Martins – Lidén – Jumbert, 2022.
[31] Musco Eklund, 2024.
[32] Leese – Ugolini, 2024.

nexus"[33] rekurzív spirálként működik a totális biztonsági környezetben.[34]

Ez a dinamika leginkább a technológiai adaptációs versenyben érhető tetten. Az embercsempészet platformizációja azt mutatja, hogy az illegális hálózatok a „szürke zónában" működve használják ki a technológiai aszimmetriát.[35] A titkosított alkalmazásokat és decentralizált „beszállítói munkaerőt" alkalmazó hálózatok a „hálózati alapú partizán" logikáját követik:[36] nem a nyílt konfrontációt, hanem a rejtőzködést és a rugalmasságot választják az EU digitális szuverenitásra irányuló törekvéseivel szemben.[37] Az állam válasza – a helyzetismeret javítása és az interoperábilis rendszerek kiépítése – szükségszerű reakció a biztonsági környezet komplexitására, ugyanakkor e lépések a hálózatokat még kifinomultabb titkosítási és elrejtési módszerek felé terelik, fenntartva a technológiai fegyverkezési versenyt.

Az egyéni migráns szintjén mindez a digitális kormányzás és az adatkezelés új dilemmáit veti fel. Az okostelefon kettős szerepet tölt be: a migráns számára a navigáció és az identitásmegőrzés személyes digitális archívuma,[38] az állam számára viszont nélkülözhetetlen információs forrás a jogszerű eljárások lefolytatásához. Ez a dinamika jól példázza a cyberfare state működési logikáját, ahol az igazgatási eljárások és a biztonsági szűrés funkcionálisan összekapcsolódnak.[39] Az EU kontextusában az adatok kinyerése nem pusztán rendészeti kényszer, hanem a modern államigazgatás hatékonyságának egyik feltétele:[40] ugyanaz az adatbázis egyaránt szolgálhatja a jogosultság megállapítását és a közbiztonság védelmét. Ebben a keretben a migráns szükségszerűen adattalanyná válik, ami lehetővé teszi az állam számára, hogy a tömeges mobilitás kihívásait jogállami keretek között, ugyanakkor a technológia nyújtotta precizitással kezelje.

Az EU „digitális határrezsimjének" kiépítése a jogállamiság és a társadalmi legitimitás alapvető kérdéseit veti fel. Az automatizált kockázatelemzés és az algoritmikus diszkréció alkalmazása növeli ugyan a határellenőrzés hatékonyságát, az átláthatóság hiánya azonban rendszerszintű kockázatot hordoz.[41] Amennyiben a technológiai rendszerek – például az ETIAS – működése ellenőrizhetetlen „fekete dobozzá" válik, vagy ha a funkciókúszás révén az adatfelhasználás céljai önkényesen bővülnek, az aláássa azt a társadalmi felhatalmazást, amelyre a hatékony és legitim állami fellépésnek támaszkodnia kellene.[42]

[33] Nedelcu – Soysüren, 2022.
[34] Farkas – Vikman, 2026.
[35] Farkas – Vikman, 2026.
[36] Childs – Bernot, 2025.
[37] Martins – Lidén – Jumbert, 2022.
[38] Georgiou – Leurs, 2022.
[39] Kelemen, 2026.
[40] Scheel, 2023.
[41] Musco Eklund, 2024.
[42] Leese – Ugolini, 2024; Kelemen – Farkas – Bučko – Jordan, 2024.

Az EU migrációs ökoszisztémájának digitalizációja nem szüntette meg a fizikai határokon zajló küzdelmet, hanem kiterjesztette azt a kibertérre, ahol az irreguláris migráció és a csempészhálózatok működése hatékonyabbá vált. Ebben a dinamikus környezetben az állam technológiai eszközökkel igyekszik növelni a határellenőrzés hatékonyságát, miközben folyamatos lépéskényszerben van a gyorsan adaptálódó bűnözői csoportokkal szemben. A cyberfare state demokratikus modelljében a fő kihívás éppen az egyensúly megtalálása: a hatóságoknak úgy kell növelniük műveleti képességeiket a biztonsági kockázatokkal szemben, hogy közben fenntartják a jogállami garanciákat és az intézményi bizalmat. E dilemmák kezelése ezért nem csupán technológiai vagy rendészeti kérdés, hanem a digitális kormányzás jogállami kereteinek újragondolását igénylő, strukturális kihívás.

V. ZÁRÓ GONDOLATOK

A digitális eszközök a migráció operatív rendszerévé váltak, meghatározó szerepet játszva az információáramlásban, a koordinációban és a döntéshozatalban. Amint azt a tanulmány bemutatta, az okostelefonok és a titkosított kommunikációs csatornák nélkülözhetetlen támogatást nyújtanak a migránsok számára a szigorú határrezsimek közötti eligazodásban és az utazások túlélésében. Ugyanezek a technológiák azonban a rugalmasság, a rejtőzködés és a gyors alkalmazkodás infrastruktúrájává váltak az embercsempész-hálózatok számára is. A digitalizáció így nem csupán erősíti az irreguláris migrációt, hanem új, minőségileg eltérő kihívásokat teremt a határigazgatás és a bűnüldözés számára.

Az alkalmazkodó digitális határigazgatási rendszerek – különösen az interoperábilis uniós adatbázisok – növelik a felderíthetőséget, ugyanakkor egyidejűleg adatvédelmi és jogállami kérdéseket vetnek fel, mindenekelőtt a célhoz kötöttség elvének fokozatos eróziója kapcsán. A 2026-tól működésbe lépő új uniós rendszerek tovább erősítik ezt az adatintenzív ökoszisztémát. Ezzel párhuzamosan a digitális platformok jogállami keretek közötti hatékonyabb szabályozása és felügyelete érdemben növelheti az állami fellépés hatékonyságát a szervezett bűnözői csoportokkal szemben. A jövőbeli stratégiák ezért szükségszerűen a c*yberfare state* rendszerszintű egyensúlyának megteremtésére kell, hogy irányuljanak: az operatív hatékonyság növelésére anélkül, hogy sérülne a közbizalom és az alapvető jogok védelme.

A kibertér és az irreguláris migráció összefonódása arra világít rá, hogy a technológiai fejlődés egyszerre kínál megoldásokat és ró összetett felelősséget a nemzetállamokra és a nemzetközi közösségre. A központi kihívás nem pusztán technológiai természetű, hanem kormányzási és jogállami kérdés: annak biztosítása, hogy a digitális ellenőrzés megerősítse, és ne aláássa a jogállamiság intézményi és társadalmi alapjait.

HIVATKOZÁS (MLA)

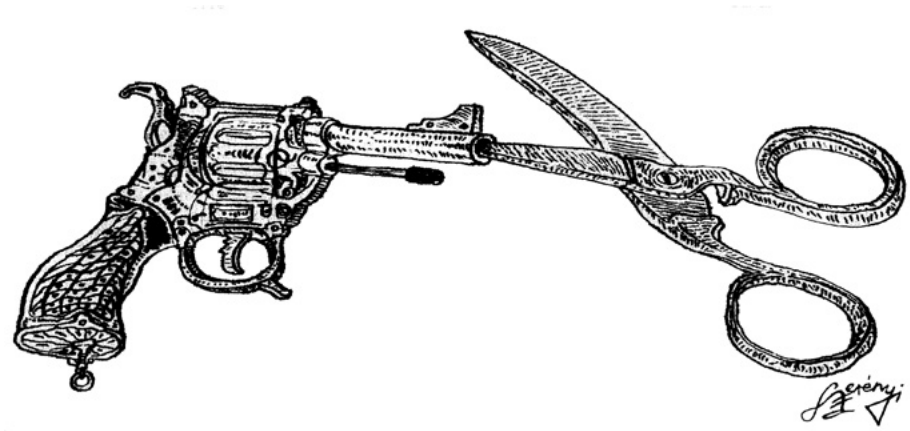
- Bartkó, Róbert, and Roland Kelemen. „A migráció digitalizációja és az állami kontroll átalakulása az Európai Unióban." *Jog–Állam–Politika: Jog- és politikatudományi folyóirat*, vol. 18, no. 2, 2026, pp. 95-107. https://doi.org/10.58528/JAP.2026.18-2.95.

IRODALOM

- Bish, A., et al. "Exploring the 'Blurred Boundary': Human Smuggling and Trafficking on the Central Mediterranean Route to Europe." *Journal of Illicit Economies and Development*, vol. 5, no. 1, 2024, pp. 70–94. https://doi.org/10.31389/jied.214.
- Blasi Casagran, C. "Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU." *Human Rights Law Review*, vol. 21, no. 2, 2021, pp. 433–457. https://doi.org/10.1093/hrlr/ngaa057.
- Bredström, A., et al. "Border Reconfiguration, Migration Governance, and Fundamental Rights: A Scoping Review of EURODAC as a Research Object." *Social Inclusion*, vol. 10, no. 3, 2022, pp. 68–81. https://doi.org/10.17645/si.v10i3.5398.
- "Intercepted Communications as Evidence: EncroChat." *The Journal of Criminal Law*, vol. 86, no. 4, 2022, pp. 271–276. https://doi.org/10.1177/00220183221113455.
- Childs, A., and A. Bernot. "The Platformisation of Illicit Drug Markets: How Datafication, Technological Affordances, and Platform-Mediated Labour Practices Shape Illicit Drug Markets." *Crime, Media, Culture*, vol. 21, no. 2, 2025, pp. 149–168. https://doi.org/10.1177/17416590241254519.
- Dewey, M., and A. Buzzetti. "Easier, Faster and Safer: The Social Organization of Drug Dealing Through Encrypted Messaging Apps." *Sociology Compass*, vol. 18, no. 1, 2024, e13175. https://doi.org/10.1111/soc4.13175.
- Eide, E. "Mobile Flight: Refugees and the Importance of Cell Phones." *Nordic Journal of Migration Research*, vol. 10, no. 2, 2020, pp. 67–81. https://doi.org/10.33134/njmr.250.
- European Commission. *A Renewed EU Action Plan Against Migrant Smuggling (2021–2025)*, COM(2021) 591 final, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0591.
- European Commission. *Pact on Migration and Asylum*, 2024. https://home-affairs.ec.europa.eu/policies/migration-and-asylum/pact-migration-and-asylum_en. Accessed 21 Jan. 2026.
- European Union. *Entry/Exit System (EES)*, 2026. https://travel-europe.europa.eu/ees. Accessed 21 Jan. 2026.
- Europol. "Interconnected and Digital: How Migrant Smugglers and Human Traffickers Operate." 2024. https://www.europol.europa.eu/media-press/newsroom/news/interconnected-and-digital-how-migrant-smugglers-and-human-traffickers-operate. Accessed 20 Jan. 2026.
- Farkas, A., and L. Vikman. "From Totality to Hybridity and Beyond: The Challenges of State Security Systems in the Context of the Info-Communication Revolutions." *Frontiers in Political Science*, vol. 7, 2026, 1749077. https://doi.org/10.3389/fpos.2025.1749077.
- Frontex. "Irregular Border Crossings Down 26% in 2025, Europe Must Stay Prepared." 2026. https://www.frontex.europa.eu/media-centre/news/news-release/frontex-irregular-border-crossings-down-26-in-2025-europe-must-stay-prepared-lyKpVb. Accessed 15 Jan. 2026.
- Frontex. *Risk Analysis 2022/2023*, 2022. https://www.frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/ARA_2022_Public_Web.pdf.

- Frontex. *Risk Analysis 2023/2024*, 2023. https://www.frontex.europa.eu/assets/Publications/General/ARA_2023.pdf.
- Frontex. *Risk Analysis 2024/2025*, 2024.
- Frontex. *Risk Analysis 2025/2026*, 2025.
- Georgiou, M., et al. "Digital Skills of and for Lives Marked by Vulnerability." *European Journal of Communication*, vol. 39, no. 3, 2024, pp. 277–285. https://doi.org/10.1177/02673231241245321.
- Georgiou, M., and K. Leurs. "Smartphones as Personal Digital Archives? Recentring Migrant Authority as Curating and Storytelling Subjects." *Journalism*, vol. 23, no. 3, 2022, pp. 668–689. https://doi.org/10.1177/14648849211060629.
- Gursky, J., and S. Woolley. *Countering Disinformation and Protecting Democratic Communication on Encrypted Messaging Applications*, 2021. https://www.brookings.edu/wp-content/uploads/2021/06/FP_20210611_encryption_gursky_woolley.pdf. Accessed 20 Jan. 2026.
- Herraiz Jagerovic, V. "Smartphone Data Extraction in the Context of Asylum." *European Journal of Migration and Law*, vol. 27, no. 2–3, 2025, pp. 179–198. https://doi.org/10.1163/15718166-12340199.
- Josipovic, I. "What Can Data Justice Mean for Asylum Governance? The Case of Smartphone Data Extraction in Germany." *Journal of Refugee Studies*, vol. 36, no. 3, 2023, pp. 534–551. https://doi.org/10.1093/jrs/fead049.
- Josipovic, I. "Digitalising Asylum Procedures: The Legitimisation of Smartphone Data Extraction for Retrospective Border Control." *Geopolitics*, vol. 29, no. 5, 2024, pp. 1831–1854. https://doi.org/10.1080/14650045.2023.2288162.
- Kelemen, R., et al. "Public Trust in National Security Institutions as a Key to Sustainable Security." *Connections: The Quarterly Journal*, vol. 23, no. 4, 2024, pp. 49–62. https://doi.org/10.11610/Connections.23.4.03.
- Kelemen, R. "The Cyberfare State: Divergent Models of Digital Governance and Control." *Frontiers in Political Science*, vol. 8, 2026, 1748562. https://doi.org/10.3389/fpos.2026.1748562.
- Koops, B.-J. "The Concept of Function Creep." *Law, Innovation and Technology*, vol. 13, no. 1, 2021, pp. 29–56. https://doi.org/10.1080/17579961.2021.1898299.
- Leese, M., and V. Ugolini. "Politics of Creep: Latent Development, Technology Monitoring, and the Evolution of the Schengen Information System." *European Journal of International Security*, vol. 9, 2024, pp. 340–356. https://doi.org/10.1017/eis.2024.5.
- Lintner, C. "Connected Journeys: Exploring Refugee Lives Through Digital Tools and Mobile Research." *Qualitative Research Journal*, 2025. https://doi.org/10.1108/QRJ-01-2025-0011.
- Martins, B. O., et al. "Border Security and the Digitalisation of Sovereignty: Insights from EU Borderwork." *European Security*, vol. 31, no. 3, 2022, pp. 475–494. https://doi.org/10.1080/09662839.2022.2101884.
- Morgan, H. "Living Digitally Like a Migrant: Everyday Smartphone Practices and the (Re)mediation of Hostile State-Affects." *Progress in Human Geography*, vol. 47, no. 3, 2023, pp. 409–426. https://doi.org/10.1177/03091325231174311.
- Musco Eklund, A. "Limits to Discretion and Automated Risk Assessments in EU Border Control: Recognising the Political in the Technical." *European Law Journal*, vol. 30, no. 1–2, 2024, pp. 103–121. https://doi.org/10.1111/eulj.12513.

• Nedelcu, M., and I. Soysüren. "Precarious Migrants, Migration Regimes and Digital Technologies: The Empowerment-Control Nexus." *Journal of Ethnic and Migration Studies*, vol. 48, no. 8, 2022, pp. 1821–1837. https://doi.org/10.1080/1369183X.2020.1796263.
• Netto, G., et al. "Resilience, Smartphone Use and Language Among Urban Refugees in the Global South." *Journal of Ethnic and Migration Studies*, vol. 48, no. 3, 2021, pp. 542–559. https://doi.org/10.1080/1369183X.2021.1941818.
• Oubad, I., and R. Ghaffari. "The Digital Infrastructures of Illegal Border Crossings: Solidarity Actors and Networks in the Arabic and Persian Speaking Virtual Spheres." *Critical Criminology*, vol. 33, 2025, pp. 71–88. https://doi.org/10.1007/s10612-025-09824-5.
• Ponzanesi, S., and K. Leurs. "Digital Migration Practices and the Everyday." *Communication, Culture & Critique*, vol. 15, no. 2, 2022, pp. 103–121. https://doi.org/10.1093/ccc/tcac016.
• Scheel, S. "'Request Denied': Some Elements of a Sociology of Translation and Treason for Border and Migration Studies." *Geopolitics*, vol. 28, no. 2, 2023, pp. 739–765. https://doi.org/10.1080/14650045.2021.1973436.
• Trauttmansdorff, P. "Against Interoperability? Terrains of Technopolitical Contestation and the Remaking of EU Border Infrastructure." *Big Data & Society*, 2024, pp. 1–15. https://doi.org/10.1177/20539517241307909.
• TRM Team. "Blockchain Intelligence and Border Security." 2025. https://www.trmlabs.com/resources/blog/blockchain-intelligence-and-border-security. Accessed 20 Jan. 2026.



Szerényi Gábor grafikája