Doktori (PhD) értekezés

Tóth Tamás

2024.

NEMZETI KÖZSZOLGÁLATI EGYETEM

Hadtudományi Doktori Iskola

Tóth Tamás:

Az IKT környezet változásainak hatásai az információgyűjtés 21. századi fejlődésére

Doktori (PhD) értekezés

Témavezető:
Dr. habil. Dobák Imre

……..

Budapest, 2024.

„A gonosz diadalához csak annyi kell, hogy a jók tétlenek maradjanak!”

Edmund Burke
(1729.01.12. – 1797.07.09)
ír író, filozófus, politikus

TARTALOM

1. BEVEZETÉS

1.1. Témaválasztás és a kutatás aktualitásának indoklása

Napjainkban a biztonsági környezet dinamikus változása, a technológiák intenzív fejlődése, valamint a rendelkezésre álló információ mennyiségének folyamatos növekedése az információgyűjtő szervezetek[1] vonatkozásában szervezeti és műveleti területen egyaránt gyorsan alkalmazkodni képes, hatékony információszerző és -feldolgozó képességgel bíró szervezeteket követel meg. A külső – az értekezés szempontjából elsősorban Európában érvényesülő – biztonsági környezetet negatív irányú dinamikus spirál jellemzi, amelyre aktuális példák az orosz és ukrán állam között zajló fegyveres konfliktus, valamint a gázai (Izrael állam és a Hamász[2] terrorszervezet) konfliktus, azok összetett, ágazatokon átívelő regionális, globális hatásai. További példa az éghajlatváltozás, az Afrikából és Ázsiából az Európai Unió felé irányuló tömeges illegális migráció és annak eltérő vallási, kulturális kihívásai, a migrációs hátterű belső európai zavargások, illetve akár a Sars-CoV-2 világjárvány, és az azt megelőző nyugat-európai iszlám fundamentalista terrortámadások. Tapasztalható az egyes kihívások, kockázatok, és fenyegetések, valamint a tényleges konfliktusok fokozódó hibrid, aszimmetrikus jellege, amely mára a nyílt reguláris katonai konfliktusoktól kiterjed az információs műveleteken keresztül, a terrorizmuson, a szervezett bűnözésen át, egészen a politikai, gazdasági nyomásgyakorlásig, befolyásolásig.[3]

A társadalom normál működése, a nemzeti szuverenitás biztosítása érdekében a modern államhatalom védelmi és biztonsági funkciójából adódó alkotmányos feladata az egyetemleges biztonság érvényesülésének garantálása, valamint az abban való közreműködése nemzetközi szövetségesei szintjén. Ezen elköteleződést, vállalást állapítja meg Magyarország Alaptörvénye (a továbbiakban: Alaptörvény) a Nemzeti Hitvallás fejezetében, miszerint „*Valljuk, hogy a polgárnak és az államnak közös célja a jó élet, a biztonság, a rend, az igazság, a szabadság kiteljesítése.*” Amennyiben pedig a nemzetközi jog, azon belül is az Európai Unió jogának

[1] Az értekezésben a titkos információgyűjtésre, a leplezett eszköz alkalmazására és annak végrehajtására jogosult szerveztek köre értendő.

[2] Hamász: Ḥarakat al-Muqāwama al-Islāmiyya - Iszlám Ellenállási Mozgalom

[3] DR. RESPERGER ISTVÁN (2018): *A válságkezelés és a hibrid hadviselés*. Budapest: Dialóg Campus Kiadó. 21-35. Online: https://nbi.uni-nke.hu/document/nbi-uni-nke-hu/Resperger%20Istv%C3%A1n_A%20v%C3%A1ls%C3%A1gkezel%C3%A9s%20%C3%A9s%20a%20hibrid%20hadvisel%C3%A9s.pdf (Letöltés ideje: 2023. július 16.); HOFFMAN, Frank (2007): *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies. Online: https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf (Letöltés ideje: 2024. március 30.)

terrénumára tekintünk az Európai Unióról (a továbbiakban: EU, Unió) szóló Szerződés[4] (a továbbiakban: EUSZ) 3. cikk (2) bek. kimondja, hogy az Unió „*egy belső határok nélküli, a szabadságon, a biztonságon és a jog érvényesülésén alapuló […] térséget kínál polgárai számára […]*”. Az EUSZ és az Alaptörvény szerinti (kötelezettség)vállalások egyes olyan alkotmányos alapvető jogok érvényesülését is hivatottak biztosítani, mint például a szabadsághoz, a személyi biztonsághoz, a magánélet, és az információs önrendelkezési jog védelméhez fűződő alapvető jogok.[5] A magyar állam polgárai számára ezen alapvető jogokat elsősorban a hon- és rendvédelmi ágazat – az értekezés szempontjából kiemelten a nemzetbiztonsági szolgálatok[6], igazságügyi[7] és bűnüldöző szervek[8] (a továbbiakban együtt: bűnüldöző szervek) – hatékony és törvényes működtetése által kívánja biztosítani[9], indokolt esetben törvényi garanciális szabályok mellett például a jogosult szervezetek által végzett titkos információgyűjtés[10], valamint leplezett eszközök[11] alkalmazása (a továbbiakban együtt értsd: titkos információgyűjtésként) által. Ezen állami monopóliummal és a végrehajtással szemben támasztott alkotmányossági kritérium[12] a törvényességnek, valamint a szükségesség és arányosság alapelveinek való megfeleltetés, hiszen ezen „speciális eszközök” alkalmazása a tevékenységgel érintett személy alkotmányos alapvető és személyiségi jogait korlátozhatja[13]. Az információgyűjtés szempontjából releváns adatok, információk legnagyobb hányada jelenleg valamely információ és kommunikáció technológiai (a továbbiakban: IKT[14]) eszközhöz, rendszerhez, eljáráshoz kapcsolódik. Már erőteljesen zajlik az olyan diszruptív, azaz „felforgató” technológiák térnyerése, mint például a mesterséges intelligencia (a

[4] Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata, OJ C 202, 7.6. 2016, 1–388.

[5] Alaptörvény IV. cikk (1) bek. „*Mindenkinek joga van a szabadsághoz és a személyi biztonsághoz*.” Lásd: Európai Unió Alapjogi Chartája (2012/C 326/02) OJ C 326, 26.10.2012, 391–407. 7. cikk

[6] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 1. § szerinti hazai nemzetbiztonsági szolgálatok.

[7] Az ügyészségről szóló 2011. évi CLXIII. törvény vonatkozó rendelkezései alapján a titkos információgyűjtésre, leplezett eszköz alkalmazására jogosult ügyészségi szervezetek.

[8] Alaptörvény 45 - 46. cikk

[9] A rendőrségről szóló 1994. évi XXXIV. törvény 4. § (2) bekezdésében felsorolt, titkos információgyűjtésre és a büntetőeljárásról szóló 2017. évi C. törvény szerinti leplezett eszköz alkalmazására jogosult szerveken túl beleértendők a Nemzeti Adó- és Vámhivatalról szóló 2010. évi CXXII. törvény vonatkozó rendelkezései alapján jogosult adó- és vámügyi szervek.

[10] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról 53. §

[11] 2017. évi C. törvény a büntetőeljárásról 214. §

[12] Alaptörvény I. cikk (3) bek.

[13] Ezen jogviszonyokban a titkos információgyűjtéssel érintett személy alapvető jogai közvetlenül konkuráló viszonyban állhatnak más személy, például biztonsághoz fűződő alapvető jogával, egy vagy több általános közérdek védelmével [GDPR 23. cikk (1) a) - e) pontja], illetve az ilyen érdekekkel kapcsolatos közhatalmi feladatok ellátásával, például az állam védelmi és biztonsági alkotmányos kötelezettségével, így azok össztársadalmi érdek érvényesülése érdekében arányos és szükséges módon korlátozhatók.

[14] IKT: Információ- és kommunikáció technológia – ICT: Information and Communication Technology

továbbiakban: MI), az autonóm robotika, az „Internet of Things" (a továbbiakban: IoT[15]), a virtuális valóság (a továbbiakban: VR[16]), a kiterjesztett valóság (a továbbiakban: AR[17]), az újgenerációs rendkívül nagysebességű hírközlési, infokommunikációs hálózatok, az űrtechnológia fejlődése stb. Ezek fokozott ütemben alakítják át, digitalizálják a korábban megszokott ipari, közigazgatási, gazdasági, szociális, egészségügyi, hírközlési és persze a biztonsági környeztet. Így elengedhetetlen az információgyűjtő szervezetek technikai képességeinek folyamatos fejlesztése, alkalmazkodása az aktuális és várható biztonsági, technológiai kihívások, kockázatok, veszélyek kezelése érdekében.[18] A jövőt illetően valószínű, hogy az információgyűjtő szervezetek technikai képességeit, infrastruktúráját a biztonsági fenyegetések változása, valamint a technológiai környezet fejlődése formálja majd a továbbiakban is.[19] A fentiek okán a biztonság szektoriális elméletének[20] megfeleltetett szintek és dimenziók komplex szemléletmódú elemzése elengedhetetlen, melyeket alapjaiban sző át a technológiai, azon belül is az IKT környezet változása. Az értekezés az IKT környezet változásának egyes hatásait hivatott vizsgálni az információgyűjtés 21. századi fejlődésére, a későbbiekben konkretizálva a kutatás tárgyát, a témaválasztás indoklásával.

Az értekezés során az IKT környezet változásának vizsgálata magával hozza a kommunikációt érintő információgyűjtés elemzésének szükségszerűségét, központi szerepét. A kommunikációs közlemények forrása lehet ember vagy gép, formája lehet szó- és írásbeli, valamint adatalapú, továbbításuk történhet személyesen köz- vagy magánterületen, illetve valamely szolgáltatás, technikai, vagy elektronikus információs rendszer igénybevételével. Napjainkra az utóbbiak keretében legyakrabban a csomag- és postaküldemény mellett a földi, légi vagy világűr infrastruktúrán üzemelő elektronikus hírközlő hálózatra gondolunk csatornaként, az eszközök tekintetében pedig az olyan IKT eszközök jutnak eszünkbe, mint az okostelefon, okosóra, táblagép vagy laptop. A kommunikáció, így a hálózati infrastruktúra és a szolgáltatás tipizálható továbbá kormányzati, ipari, és publikus (azaz lakossági célú) felhasználás szerint.
Az IKT piacon intenzív változás, fejlődés figyelhető meg, amely magában foglalja az infokommunikációval és az információs társadalommal összefüggő egyéb szolgáltatásokat, a

[15] IoT: Internet of Things – dolgok internete
[16] VR: Virtual Reality – virtuális valóság
[17] AR: Augmented Reality – kiterjeszte5tt valóság
[18] DR. RESPERGER 2018: 4-5
[19] DR. BODA József – DR. DOBÁK Imre (2016): Titkosszolgálatok fejlődése – technikai szemmel. *Nemzetbiztonsági Szemle*, 4(4), 23. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1879/1168 (Letöltés ideje: 2024. március 3.)
[20] BUZAN, Barry (1983): *People, states, and fear: the national security problem in international relations*. Brighton: Wheatsheaf Books.

kapcsolódó technológiákat, valamint a szoftver és hardveres infrastruktúrákat is. 2020-tól az infokommunikációs ágazat az IKT piac legnagyobb bevételt realizáló szegmense, míg az új, diszruptív technológiák a legdinamikusabban bővülő kategóriák. A piac vezető részesedését a következő néhány évben elsősorban a big data[21] és elemzése, a közösségi média, a mobil és a felhőalapú IKT – köztük kommunikációs – szolgáltatások fogják meghatározni.[22] A digitális jövő alapvetően az IKT termékek és szolgálatások konnektivitásának, azaz összekapcsoltságának, konvergenciájának, interoperabilitásának, autonómiájának, multimodalitásának színtere lesz, melyben a személyközi kommunikáció mellett kiemelt szerepe lesz a gép-gép, azaz a machine-to-machnie (a továbbiakban: M2M[23]) kommunikációnak. Az Ipar 4.0[24], az okos városok komponenseiben kulcsszerepet betöltő IoT eszközök biztonságos vezérlését lehetővé tevő M2M adatkommunikáció az eddigi hálózatokon csak korlátozottan biztosítható paramétereket követel meg.[25]

Az IKT alapú termékek és szolgáltatások alapján a 21. századra kialakult információs társadalomnak köszönhetően a kibertér[26] teljesen átszövi a polgárok mindennapjait, interakciójuk elsődleges színterévé vált, „*a tömegesen terjedő infokommunikációs eszközök a kommunikáció jellegét is megváltoztatják.*”[27] Kovács László kutatási eredményeivel egyetértve megállapítható, hogy „*Azok az infokommunikációs eszközök jellemzik igazán a 21. századot, amelyeknek egyik legszemléletesebb példái az okostelefon vagy a mobilizálható számítógépek – tabletek, laptopok –, illetve az ezek működését lehetővé tevő forradalmi technológiák, mint*

[21] A big data fogalma alatt azon összetett technológiai környezetet értendő, amely biztosítja olyan adatállományok feldolgozását, melyek annyira nagy méretűek és komplexek, hogy feldolgozásuk a hagyományos adatbázis-menedzsment technológiákkal jelentős nehézségekbe ütközik.

[22] *Global ICT market share 2013-2022, by selected country*. Statista Research Department. 2023. Online: https://www.statista.com/statistics/263801/global-market-share-held-by-selected-countries-in-the-ict-market/ (Letöltés ideje: 2023. július 8.)

[23] M2M: machine-to-machnie – gép-gép

[24] Az ipar 4.0 a termelési folyamatok olyan szervezési modellje, amelyben a hálózatba kapcsolt okos eszközök autonóm módon szenzoriak által érzékelnek, adatot gyűjtenek, kommunikálnak egymással és adatalapú döntéseket hoznak, így MI által vezérelt gyártási folyamatokat hoznak létre. A rendszerek nyomon követik a fizikai folyamatokat és decentralizált döntéseket hoznak adatcsere alapján. Lásd: SCHWAB, Klaus (2017): *The Fourth Industrial Revolution*. London: Penguin

[25] Az információgyűjtés szempontjából merőben új lehetőségeket, adatforrásokat teremt az IoT, azonban tekintettel annak önálló kutatási területére – már csak az egyes összetevői vonatkozásában is – a témakör az értekezésben nem képezi elmélyült vizsgálat tárgyát, csak a komplex trend, tendenciaelemzés, az elektronikus adatvédelem során kerül részlegesen feldolgozásra.

[26] SIMON László – DR. MAGYAR Sándor (2017): A terrorizmus és indirekt hatása a kibertérben. *Nemzetbiztonsági Szemle*, 5(3), 96-97. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1685/991 (Letöltés ideje: 2023. július 9.)

[27] KOVÁTS Ildikó (2006): Információs társadalom, emberi tényező, civil társadalom, média – Adalékok a magyarországi digitális műsorszórás előrejelzéséhez. *Jel-kép*, 26(29, 19-36. Online: http://real-j.mtak.hu/5612/2/JelKep 2006 2.pdf (Letöltés ideje: 2023. július 9.)

például az 5G[28] *mobilkommunikáció.*"[29] Néhány éve egyre több titkosított online kommunikációt biztosító „csevegőalkalmazás", mobil applikáció, azaz a hazai jogszabályi fogalomhasználat szerinti alkalmazásszolgáltatás[30] jelent meg, amelyek biztonságos kommunikációt ígértek. Ezek körében a végpont-végpont titkosítási kriptográfiai eljárás (a továbbiakban: E2EE[31]) egyre elterjedtebbé vált. Az E2EE a gyakorlatban azt jelenti, „*hogy a küldő (egyik végpont) és a fogadó (másik végpont) között titkosítva valósul meg az adatátvitel, a tartalmát még a csevegőalkalmazást működtető vállalat sem látja.*"[32] A feldolgozott szakirodalom alapján az alkalmazásszolgáltatások a 21. század legelterjedtebb online infokommunikációs szolgáltatásaivá váltak, amelyeket jogsértő cselekmények megvalósítása során például a terror-, bűnszervezetek is alkalmaznak kommunikációs csatornaként. Ezt támasztja alá a francia terrorelhárítás vizsgálata is, miszerint 2016 augusztusában az Iszlám Állam (a továbbiakban: ISIS[33]) terrorszervezet Jacques Hamel atya, az Észak-franciaországi Saint-Étienne-du-Rouvray-i plébánia beosztott papja elleni terrortámadás során E2EE-t biztosító Telegram alkalmazáson kommunikált.[34] A terrortámadásokat követően egyes nyugati sajtóorgánumok a Telegramot "*dzsihádi üzenetküldő alkalmazásának*" minősítették.[35] Az ISIS Telegram használata már 2015-ben újraindította az E2EE titkosítás vitáját.[36] A szervezett bűnözés kapcsán az Europol[37]által készített 2021 évi SOCTA[38] jelentése megállapítja, hogy „*Gyakorlatilag minden bűncselekmény megvalósítása tartalmaz néhány online komponenst,*

---

[28] 5G: 5. generáció: A cellarendszerű mobiltávközlés legújabb generációja, amelynek jellemzői a magas adatsebesség, a kevesebb késleltetési idő, az energiamegtakarítás, a kevesebb költség, a magasabb rendszerkapacitás és az eszközökre vonatkozó jobb hálózati összekapcsoltság, azaz a konvergencia. Lásd: *Digital Single Market: Political agreement on the rules shaping the telecommunication markets in the 5G era*. European Commission. 2018. 1. Online: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_18_4084/MEMO_18_4084_EN.pdf (Letöltés ideje: 2024. február 18.)

[29] KOVÁCS László (2023): *Hadviselés a 21. században: kiberműveletek*. Budapest: Ludovika Egyetemi Kiadó. 25.

[30] Az értekezés során alkalmazásszolgáltató alatt az Ekertv. 2. § m) pontja szerinti szolgáltatók körén belül a titkosított online kommunikációt biztosító szolgáltatók értendők.

[31] E2EE: End-to-End Encryption – végpont-végpont közötti titkosítás: csak a küldő és fogadó készüléken teszi lehetővé a rejtjelezett üzenet értelmezhető formában történő visszafejtését, applikációk tekintetében azonos szolgáltatáson belül.

[32] BÁNYÁSZ Péter – TÓTH András – MAGYAR Sándor – KOLLER Marco (2022): A videókonferencia-alkalmazások biztonsági kockázatai. *Acta Humana*, 10(4), 26. Online: https://folyoirat.ludovika.hu/index.php/actahumana/article/view/6731/5286 (Letöltés ideje: 2024. február 16.)

[33] ISIS: Islamic State of Iraq and Syria – Iraki és Szíriai Iszlám Állam

[34] HADDAD, Margot - HUME, Tim (2016): *Killers of French priest met 4 days before attack*. CNN. Online: http://edition.cnn.com/2016/08/01/europe/france-church-attack-telegram/index.html (Letöltés ideje: 2023. július 8.)

[35] CAMPBELL, Scott (2016): *ISIS warn London 'next to be attacked' as UK churches put on terror alert after French priest murder*. Daily Mirror. Online: https://www.mirror.co.uk/news/world-news/isis-warn-london-next-attacked-8500399 (Letöltés ideje: 2023. július 8.)

[36] SANGER, David - PERLROTH, Nicole (2015). *Encrypted Messaging Apps Face New Scrutiny Over Possible Role in Paris Attacks*. The New York Times. Online: https://www.nytimes.com/2015/11/17/world/europe/encrypted-messaging-apps-face-new-scrutiny-over-possible-role-in-paris-attacks.html (Letöltés ideje: 2023. július 8.)

[37] Europol - Bűnüldözési Együttműködés Európai Uniós Ügynöksége

[38] Serious And Organised Crime Threat Assessment - Szervezett bűnözés európai uniós fenyegetettségértékelése

például olyan digitális megoldásokat, amelyek megkönnyítik a bűncselekmények során végbement kommunikációt."[39]

A külső biztonsági környezet negatív irányú változásának tendenciája, valamint a digitalizáció, a technológiai környezet rohamos fejlődése átfogó biztonsági stratégiaalkotást is eredményezett mind nemzetközi, mind állami szinten. A hazai 2020-2030 időszakra szóló hatályos Nemzeti Biztonsági Stratégia[40] (a továbbiakban: Stratégia) 126. pontja alapján *„Magyarország stratégiai célkitűzése, hogy 2030-ra kialakítsa azokat a nemzeti ellenálló, elrettentési, védelmi, válságkezelési és koordinációs képességeket, amelyek a változékony nemzetközi környezetben előfeltételei a nemzet fejlődéséhez szükséges stabilitásnak és biztonságnak. Magyarország nemzetközi összehasonlításban is magas szintű közbiztonsági helyzetét meg kell őrizni és tovább kell javítani."* A Stratégia 165. pontja ezen törekvés megvalósításának alapvető elemeként azonosítja a hazai nemzetbiztonsági szolgálatokat és azok nemzetközi együttműködésének fokozását, továbbá kimondja, hogy „*Hazánk biztonsági környezetének romlása miatt szükséges a nemzetbiztonsági szolgálatok képességeinek továbbfejlesztése, különös tekintettel a titkos információgyűjtés koncentrált eszközrendszerére."*[41] A digitalizáció hatására előtérbe kerülő, kialakuló új titkos információgyűjtő módszereknek a hagyományos információgyűjtő módszerekkel – katonai NATO[42] terminológia[43] szerint elsődlegesen a HUMINT[44]-tal – történő hatásait vizsgáló kutatás szerint „*A jövőre kitekintve már most látható, hogy az emberi viselkedés és kapcsolattartás virtuális platformokon megjelenő digitalizált adatai a humán és a technikai alapú ismereteket igénylő új információgyűjtő megoldásokat eredményeznek.*"[45]
Az infokommunikációs ágazat biztonsági szempontú elemzése során két fő tevékenységi kör határolható el állami szinten. Az egyik a nemzetbiztonsági szolgálatok, egyéb hon- és rendvédelmi szerezetek feladat- és hatáskörével érintett infokommunikációs rendszerek, hálózatok információvédelme, míg a másik a nemzetbiztonsági, bűnüldöző szervek által

[39] *European Union Serious and Organised Crime Threat Assessment* (SOCTA) 2021. Europol, 32. Online: https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf (Letöltés ideje: 2023. július 8.)
[40] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 1. sz. melléklet
[41] Magyarország további nemzetközi együttműködésen alapuló (NATO, EU stb.) védelmi célú fejlesztési-beruházási kötelezettségeinek vizsgálat nem képezi az értekezés tárgyát.
[42] NATO: North Atlantic Treaty Organisation – Észak-atlanti Szerződés Szervezete
[43] *NATO Glossary of Terms and Definitions AAP-06 (2021)*. NATO Standardization Office. 2021. 65.
[44] HUMINT: Human Intelligence – Emberi erőforrás alapú hírszerzés: Azon információgyűjtő módszerek és eszközök összessége sorolható a HUMINT körébe, amelyek során az információk emberi erőforrás által kerülnek beszerzésre és elsősorban humán forrásokból származnak.
[45] DOBÁK Imre – TÓTH Tamás (2022): Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering). *Belügyi Szemle*, 69(2), 195-212. Online: https://ojs.mtak.hu/index.php/belugyiszemle/article/view/5345/4209 (Letöltés ideje: 2024. február 15.)

folytatott titkos információgyűjtéssel érintett személyek kommunikációjának ellenőrzése, azaz annak taralmának és az ahhoz kapcsolódó kísérő- és metaadatok[46] leplezett megismerése. Az értekezés szempontjából a második tevékenységi kör bír relevanciával. A köz- és nemzetbiztonságot negatívan befolyásoló jogellenes tevékenységek – így például a nemzetközi szervezett bűnözés, a terrorizmus, az illegális fegyverkereskedelem, a nemzeti szuverenitást veszélyeztető állami és nem kormányzati törekvések – megelőzése, felderítése és elhárítása érdekében jelentős szerepe van az ezekkel összefüggő kommunikáció törvényes ellenőrzésének (a továbbiakban: LI[47]).

Az értekezés tudományos vizsgálatának elsődleges tárgyát az információs társadalommal összefüggő infokommunikációs szolgáltatások körén belül a személyközi online kommunikációt megvalósító titkosított alkalmazásszolgáltatások nemzetbiztonsági célú LI tevékenysége képezi, természetesen vizsgálva a kommunikációs csatornaként alkalmazott elektronikus hírközlési, valamint az egyéb információs társadalommal összefüggő szolgáltatások kapcsolódó vetületeit, továbbá egyfajta összehasonlító jelleggel a bűnüldözési célú LI -t. A disszertációs kutatómunka fő tárgya a később ismertetésre kerülő egyes LI módszereken belül a passzív, mély csomagátvizsgálás, azaz a DPI[48], annak is a hírközlőhálózati oldalon megvalósuló központi monitoring alrendszer típusú formája, természetesen vizsgálva a többi LI módszert, például a szolgáltatói együttműködést. A szakirodalom alapján indokolt az LI szabályozási és technológiai környezetének vizsgálata is,[49] a biztonsági környezet változásainak és a társadalmon belüli IKT trendek, tendenciák elemzése mellett.

---

[46] A kísérő- és metaadatok fogalomköre mára a köznapi nyelvezetben összeolvadt, azonban az értekezés szempontjából lényeges ezen fogalmak, szakterminológiák elkülönítése és nem összevonása, melynek első sorban a titkos információgyűjtés, azon belül is az LI szempontjából van jelentősége. Elektronikus hírközlés során beszélhetünk kísérőadatról, amely körét általános fogalmi szinten az elektronikus hírközlésről szóló 2003. évi C. törvény hatálya alá tartozó tevékenységeknél az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről szóló 180/2004. (V.26.) Korm. rendelet 2. § e) pontja rendezi. Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 2. § 1. pontja, illetve 3/B §-a szerinti titkosított online kommunikációt biztosító alkalmazásszolgáltatás tekintetében pedig metaadatról beszélhetünk, amely köre a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről szóló 185/2016. (VII.13.) Korm. rendelet 1. § d) pontja alapján a 2001. évi CVIII. törvény 13/B. § (2) bekezdésében meghatározott adatok. Ezek a későbbiekben részletesen kifejtésre kerülnek.

[47] LI: Lawful Interception – törvényes „lehallgatás", törvényes kommunikációellenőrzés. Az értekezés során az LI tágabb fogalomköre kerül alkalmazásra, azaz a tartalomellenőrzés mellett beleértendő a kommunikációra vonatkozó kísérő- és metaadatokhoz való hozzáférés. Ezt a fajta értelmezést az IKT környezet fejlődése teszi indokolttá, hiszen a hírközlő hálózatokon, információs rendszereken ezek ellenőrzésére is lehetőség nyílik.

[48] DPI: Deep Packet Inspection – mély csomagátvizsgálás

[49] SZABÓ Hedvig – DOBÁK Imre (2021): Az információs társadalom nemzetbiztonsága. *Nemzet és Biztonság – Biztonságpolitikai Szemle*, 14(2), 96. Online: https://folyoirat.ludovika.hu/index.php/neb/article/view/5781/4819 (Letöltés ideje: 2023. július 9.)

A fentiek alapján a témakör tudományos vizsgálata indokolt, amelyet az alábbi konkrét szakirodalmi megállapítások is alátámasztanak. A Nemzeti Közszolgálati Egyetem katonai műszaki doktori képzésének keretében 2013-2016 között tudományos kutatómunka során vizsgálatra került az alkalmazásszolgáltatások törvényes kommunikációellenőrzése.[50] Ennek főbb következtetései szerint az alkalmazásszolgáltatások LI-jével kapcsolatos akkori elsődleges kihívások a szolgáltatókkal történő együttműködés jogszabályi rendezésének hiánya, az LI képesség egy szervezetben történő koncentrált kialakításának hiánya, valamint a szélesebb adatforrási bázison történő információgyűjtés – különös tekintettel a kísérő- és metaadatokra – továbbá a fúziós elemzés-értékelés lehetőségének vizsgálatai voltak. 2013-ban megjelent a „*Hírközlési-szabályozás, hírközlési-igazgatás hazánkban és az Európai Unióban*"[51] című könyv, amely jogtudományi jelleggel a felhőkommunikációs szolgáltatások, így az értekezés vizsgálatának tárgyát képező alkalmazásszolgáltatások tipikus szabályozási problémái között tárgyalja a jogszabályi előírások és a hatósági intézkedések érvényre juttatásának témakörét. A vizsgált szakirodalom következtetései alapján a szolgáltatások helyfüggetlensége és ebből adódóan azok globális jellege sok esetben jogi kollízióhoz vezet, mely okán fennáll az alkalmazandó nemzeti jog és az eljáró külföldi hatóság joghatóságának vitája is.[52] Mind a fenti szakmai tudományos, mind a jogtudományi következtetések akkoriban helyesnek bizonyultak, hiszen a Nyugat-Európát ért iszlamista terrortámadások hatására, a hatékony megelőzés, elhárítás, felderítés érdekében „lépéskényszerbe" került uniós tagállamok, így Magyarország is jogalkotásba kezdett, mely eredményeképpen 2016. július 17-én hatályba lépett a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló 2016. évi LXIX. törvény. A normamódosítás hatására például az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvényben (a továbbiakban: Ekertv.) hatálya kiterjed az alkalmazásszolgáltatókra, mint

[50] Lásd: KOVÁCS Zoltán (2013): Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. *Hadmérnök,* 8(3), 184-197. Online: http://hadmernok.hu/133_18_kovacsz_2.pdf (Letöltés ideje: 2023. július 8.); KOVÁCS Zoltán (2013): Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II. *Hadmérnök,* Hadmérnök. 8(3), 198-210. Online: http://hadmernok.hu/133_19_kovacsz_3.pdf (Letöltés ideje: 2023. július 8.); DR. KOVÁCS Zoltán (2016): Az alkalmazásszolgáltatók törvényes ellenőrzésének jövője – a technológiák konvergenciájának tükrében. *Nemzetbiztonsági Szemle*, 4(1), 79-99. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1815/1105 (Letöltés ideje: 2023. július 8.); KOVÁCS Zoltán (2015): *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai.* Doktori (PhD) értekezés. Budapest: NKE KMDI. Online https://adoc.tips/az-infokommunikacios-rendszerek-nemzetbiztonsagi-kihivasai.html (Letöltés ideje: 2023. július 8.)

[51] LAPSÁNYSZKY András (szerk.) (2013): *Hírközlési-szabályozás, hírközlési-igazgatás hazánkban és az Európai Unióban.* Budapest: Wolters Kluwe CompLex Kiadó.

[52] DR. BARTOLITS István (2013): Az over-the-top (OTT) szolgáltatások. In LAPSÁNYSZKY András (szerk.): *Hírközlési-szabályozás, hírközlési-igazgatás hazánkban és az Európai Unióban.* Budapest: Wolters Kluwe CompLex Kiadó. 803.

nevesített közvetítő szolgáltatókra[53], egyben definiálva is annak fogalmát, továbbá LI célú együttműködési kötelezettséget állapított meg az alkalmazásszolgáltatók számára, tekintettel azok elterjedésének reális veszélyére a bűnszervezeteknél. 2016-ot követően a témakört érintő hazai tudományos publikációkat korlátozottan lehet fellelni, így elengedhetetlen annak aktuális vizsgálata olyan formális tudományos kutatás keretében, amely eredményei alkalmasak a gyakorlati alkalmazhatóságra, a jogalkotás támogatására, összhangban a Stratégia 165. pontja szerinti titkos információgyűjtés koncentrált eszközrendszerének fejlesztésére irányuló törekvések, azon belül is a hazai LI képességfejlesztés nyilvános, tudományos megalapozására.

A témakör vizsgálatának aktualitását továbbá indokolják a digitalizáció és annak kihívásait legalább középtávon kezelni kívánó EU-s jogalkotási és szakpolitikai törekvések, melyeket érdemes a személyes adatvédelem/biztonság szerinti értékduál mentén szemlélni. Az uniós szintű adatvédelmi előírások érvényesülése érdekében 2018. május 25-től alkalmazandó az Általános Adatvédelmi Rendelet (a továbbiakban: GDPR[54]).[55] 2022. december 15-én az EU vezetése aláírta a „*Digitális jogokról és elvekről szóló európai nyilatkozatot*”[56], amely célja a technológiai biztonság adatvédelmi szempontú zsinórmértékének kinyilatkoztatása.[57] Az Európai Tanács 2022. december 08-án elfogadta „*A digitális évtizedhez vezető út*”: uniós terv a digitális Európa 2030-ra történő megvalósításához szükséges programról szóló határozatát[58] (a továbbiakban: Digitális évtized 2030 szakpolitikai program), amely átrendezi az Unió digitális piacát/gazdaságát és komponenskeként a digitális adatvédelmet. A Program célkitűzései egyik alapjaként 2030-ra 100%-os 5G lefedettséget határoz meg az EU területén. Az újgenerációs hírközlési hálózatok tekintetében az EU már szabvány szintjén fokozta az elektronikus

[53] Ekertv. 2. § l) pont le) alpontja

[54] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), OJ L 119, 4.5.2016, 1–88.

[55] Kiemelendő, hogy az uniós adatvédelmi szabályozás, hasonlóan a technológiai oldalhoz lineárisan fejlődő és a korábbi megoldásokra épít. Azért is fontos ezen kérdést összefüggéseiben látni, mert a szabályozási keretrendszer fejlesztésére azért került sor, mivel a jogalkotó tudatosan törekedett arra, hogy adekvát normatív adatvédelmi választ adjon az új technológiai megoldásokra, illetve az uniós polgárok jogait hátrányosan érintő nemzetközi – elsődlegesen USA-beli – gyakorlatra. Lásd: SZŐKE Gergely László (2013): Az adatvédelem szabályozásának történeti áttekintése. *Infokommunikáció és jog*, 56(3), 107-112. Online: https://infojog.hu/wp-content/uploads/pdf/201356_SzokeGergelyLaszlo.pdf (Letöltés ideje: 2024. július 9.)

[56] The European Parliament, the Council and the Commission solemnly proclaim the following joint Declaration on Digital Rights and Principles for the Digital Decade. 15 December 2022. Online: https://ec.europa.eu/newsroom/dae/redirection/document/94370 (Letöltés ideje: 2023. július 9.)

[57] *Commission puts forward declaration on digital rights and principles for everyone in the* EU. Europea, Commission. 2022. Online: https://ec.europa.eu/commission/presscorner/detail/hu/IP_22_452 (Letöltés ideje: 2023. július 9.)

[58] Decision (EU) 2022/2481 of The European Parliament And of The Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance). Online: https://eur-lex.europa.eu/eli/dec/2022/2481/oj (Letöltés ideje: 2023. július 9.)

információbiztonság követelményeit, elsősorban a titkosság, az anonimizálás tekintetében. Az Europol 2019-ben felismerte, hogy az 5G jelentősen rontja a hírközlési LI hatékonyságát, így nélkülözhetetlen a képességfenntartó intézkedések megtétele.[59] EU-s jogalkotás van folyamatban a gyermekek szexuális bántalmazásának megelőzésére és az ellene folytatott küzdelemre vonatkozó szabályok megállapításáról szóló Európai Parlament és Tanácsi rendelet javaslatáról (a továbbiakban: CSAR)[60], mely egyik fő célja a személyes adatvédelmet garantáló E2EE kriptográfiát biztosító kommunikációs szolgáltatások LI-jének normatív biztosítása.[61] Tehát az IKT környezet változásainak az információgyűjtés 21. századi fejlődésére gyakorolt hatásinak, azon belül is az alkalmazásszolgáltatások nemzetbiztonsági célú LI-jének tudományos vizsgálatát az uniós jog- és szakpolitikai, nemzetközi együttműködési törekvések is indokolják, aktuálissá teszik, fokozva az új tudományos eredmények, és gyakorlati hasznosíthatóságuk szükségszerűségét.

1.2. Tudományos probléma megfogalmazása

A nemzetbiztonsági szolgálatok tevékenységével érintett nemzeti szuverenitást sértő magatartással, terrorizmussal, egyéb kimagasló társadalomra veszélyes bűncselekményekkel összefüggésbe hozható személyek, csoportok elleni hatékony, prognosztikus szemléletű fellépés érdekében elengedhetetlen a titkos információgyűjtés komplex eszközrendszerén belül a társadalmi, technológiai, normatív kihívásokkal szemben ellenálló LI képességek fenntartása. Az EU digitális piaci és adatvédelmi stratégiai célkitűzéseinek hatására tapasztalható a lakossági célú elektronikus hírközlési, valamint az információs társadalommal összefüggő egyéb internet alapú kommunikációs szolgáltatások piacainak átalakulása, így az értekezés szempontjából elsősorban az alkalmazásszolgáltatások iránti növekvő kereslet, mely a digitalizáció, a virtualizáció, a folyamatos online jelenlét iránti szükségletek kielégítése érdekében kiemelt összetevőként azonosítható. A diszruptív infokommunikációs termékekkel, szolgáltatásokkal kapcsolatban kialakult keresleti „dömping” egyfajta kínálati K+F+I „sokkot”

[59] Lawful Interception – Strengthening EU cooperation (Brussels, 5 November 2020), 11517/1/20 REV 1. 1-2. Online: https://data.consilium.europa.eu/doc/document/ST-11517-2020-REV-1/en/pdf (Letöltés ideje: 2023. július 9.)

[60] Proposal for a Regulation of The European Parliament and of The Council laying down rules to prevent and combat child sexual abuse COM/2022/209 final (Brussels, 11.5.2022). Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN (Letöltés ideje: 2023. július 9.)

[61] Written comments submitted by Member States Proposal for a Regulation laying down rules to prevent and combat child sexual abuse (9068/22) (Brussels, 12.4.2023) WK 10235/2022 ADD 10 REV 2. 65-66. Online: https://www.documentcloud.org/documents/23819681-law-enforcement-working-party-document-encryption (Letöltés ideje: 2023. július 9.)

okozott a 21. század IKT piacán, melynek következtében az infokommunikációs technológiák, az IKT környezet egyre dinamikusabb fejlődése tapasztalható, többek között az új adatátviteli megoldások, a kifinomultabb elektronikus információ-, kibervédelmi eljárások, valamint a normatív adatvédelmi előírások tekintetében egyaránt. A témaválasztás indoklása alapján ezen internet alapú, titkosított online kommunikációt biztosító alkalmazásszolgáltatások igénybevétele feltételezetten fokozódó ütemben azonosítható a nemzetbiztonsági szolgáltatok – és bűnüldöző szervek – tevékenységével értinett személyek, csoportok kommunikációs attitűdjében, mely tendencia egyben a piaci kereslet/kínálat szabályai szerint az „LI piacán" is feltételezetten növekedést eredményez, eredményezhet.

A témaválasztás indoklása alapján az elektronikus hírközlő hálózatokon megvalósuló személyközi kommunikáció hazai hatékony ellenőrzése tekintetében tudományosan vizsgálandó problémakörként azonosítom az IKT környezet fejlődéséből adódó kihívásokat, és azok hatásait az LI hatékonyságára, képességfejlesztésére. A szakirodalom alapján megállapítható, hogy 2015/16-ig bezárólag az alkalmazásszolgáltatások ellenőrzése állami szinten normatív, technológiai nehézségekbe ütközött. A témaválasztás indoklása alapján szükséges a témakör ezen időpontot követő tudományos alaposságú vizsgálata, mely során altémakör elsősorban az alkalmazásszolgáltatások hazai nemzetbiztonsági célú LI-je jogszabályi és technológiai környezetének hatékonysága, így az IKT környezet fejlődésével szembeni rezilienciája[62]. Az alkalmazásszolgáltatások LI-je kapcsán indokolt a legtöbb esetben kommunikációs csatornát biztosító elektronikus mobil (telefon, internet) hírközlési szolgáltatások és azok LI-jének tudományos vizsgálata is. Az LI hatékonysága szempontjából szükséges vizsgálni mind a hírközlő hálózatok, mind az alkalmazásszolgáltatások kriptográfiai környezetének fejlődését is. Ezen túlmenően nélkülözhetetlen a képességfejlesztési irányok meghatározásához a biztonsági környezet jellemzőinek, valamint a társadalom, azaz a felhasználók IKT szokásainak, trendjeinek vizsgálata. Megállapítható, hogy a technikai információgyűjtés, azon belüli résztevékenységként értelmezve az LI képesség hatékonyságát számos az IKT környezet folyamatos változásából, fejlődéséből adódó egymással összefüggő, igen összetett külső hatás befolyásolja direkt, indirekt módon, melyek közül a kutatómunka

[62] Reziliencia: Általános értelemben vett rugalmas ellenállási képesség, azaz valamely rendszernek azon reaktív képessége, amely keretében az erőteljes, megújuló, vagy akár sokkszerű külső negatív hatásokkal szemben sikeresen adaptálódjék.

során a szabályozási, technológiai, társadalmi, és a biztonsági környezet vizsgálata indokolt.[63] A technikai információgyűjtésre, azon belül értelmezve az LI képességekre az IKT környezet változásából adódó vizsgált hatástényezőket az alábbi 1. ábra hivatott szemléltetni.

1. ábra: A technikai információgyűjtésre, azon belül az LI képességre az IKT környezet változásából adódó vizsgált hatástényezők (Szerk.: A szerző)

A kutatómunka során tudományos következtetések levonására nyílik lehetőség az IKT környezet fejlődéséből adódó többlet LI lehetőségekről és kihívásokról, melyek hozzáadott értéket képezhetnek az LI hatékonyságára irányuló képességfejlesztés számára. Annak érdekében, hogy az alkalmazásszolgáltatásokat érintő LI tevékenység hazai viszonylatban a jövőben is eredményesen biztosítható legyen, nélkülözhetetlen prognosztikus szemléletű következtetéseket levonni:

- a digitális IKT piac globális és hazai trendjei, tendenciái, evolúciója tekintetében;
- az IKT piac fejlődéséből adódó LI szempontú kihívásokról/többlet LI lehetőségekről;
- az LI tevékenység hazai szervezetrendszeréről, szabályozásáról, azok evolúciójáról;
- a mobilhálózatok és az alkalmazásszolgáltatások LI szempontú egyedi jellemzőiről, a tevékenységek összefüggéseiről;
- a személyközi infokommunikációs szolgáltatások körén belül a mobil hírközlési hálózatok, valamint az alkalmazásszolgáltatások elektronikus információvédelmi környezetéről, azon belül is a kriptográfiai eljárások alakulásáról;

[63] A részkutatási cselekmények során természetesen vizsgálat tárgyát képezi a politikai, gazdaságpolitikai környezet hatásai is elsősorban uniós szinten, azonban azok nagyrészben indirekt módon a szabályozáson keresztül érvényesülnek. Környezeti tényezők vizsgálatára nem kerül sor, tekintettel annak indokolatlanságára.

- a személyközi hírközlés normatív adatvédelmi környezetének alakulásáról;
- az alkalmazásszolgáltatásokra irányló LI tevékenységgel érintett személyek, csoportok kommunikációs szokásainak alakulásáról;
- a globalizált IKT szolgáltatások okán a nemzetbiztonsági, bűnüldözési célú LI nemzetközi, uniós együttműködésének lehetőségeiről.

1.3. Hipotézisek

1. A prognosztizálható IKT trendek alapján feltételezhető, hogy a GSM alapú mobil kommunikáció hagyományos LI-jével szemben a mobilinternet alapú titkosított online kommunikációt biztosító alkalmazásszolgáltatások LI igényének fokozódása várható, amelyek szolgáltatói együttműködés alapú és technikai monitoring LI módszerei is innovatív technológiai, szabályozási és szervezeti környezetet követelnek meg.

2. A jövőben a légi, világűr infrastruktúrára épülő elektronikus hírközlő hálózatok várható elterjedése, valamint az újgenerációs mobilhálózatok LI-je forradalmasíthatja az összadatforrású titkos információgyűjtés technikai képességeit az egyre heterogénebb jellegű és forrású adatforgalom okán, amennyiben az információgyűjtő szervezetek képesek technológiai szempontból kiaknázni a lehetőségeket.

3. Az alkalmazásszolgáltatások globalizációja, a nemzetközi adatvédelmi normatív és technológiai környezet fejlődése hátrányosan érintheti az azokon végbement kommunikáció LI-jének hatékonyságát, valamint azok kriptográfiai fejlődésének hatására a kommunikációellenőrzést szabályozó hatályos hazai normarendszer hatékonysága erodálódhat, e téren az LI képesség rezilienciája korlátozódhat.

4. Valószínűsíthetően a jövőben a személyközi hírközlési szolgáltatások – beleértve az alkalmazásszolgáltatásokat is – keretében végbement kommunikáció nemzetbiztonsági célú LI-jének hatékonysága érdekében nélkülözhetetlen lesz a nemzetközi, uniós együttműködés fokozása, az információcserén túl a jövő LI képességei kialakításának lehetőségét is figyelembe véve, a nemzeti szuverenitás tiszteletben tartása mellett.

1.4. Az értekezés célja

Az 1.5. alfejezetben meghatározott tudományos kutatási módszertan alkalmazásával a hipotézisek igazolását tűzöm ki fő célul, egyben új tudományos eredményként az LI jövőbeli hatékonyságát elősegíteni képes javaslatok megalkotásával. A definiált általános tudományos problémakörön belül elsődlegesen tudományos jelleggel vizsgálni kívánom az alkalmazásszolgáltatások hazai LI-je jogszabályi és technológiai környezetének hatékonyságát, valamint a kriptográfiai eljárások fejlődésével szembeni rezilienciáját, és az egyes nemzetbiztonsági célú LI hatékonyságnövelő intézkedések lehetőségeit, összhangban a Stratégia 126. és 165. pontjaiban megfogalmazott átfogó célkitűzésekkel, vizsgálva az EU digitális piaci és adatvédelmi stratégiai célkitűzéseinek hatásait a témakört illetően.

Ennek érdekében mind a főbb személyközi IKT trendek, tendenciák elemzésére alapozva következtetéseket kívánok levonni a hagyományos mobil hírközlés és a mobilinternet alapú kommunikáció, valamint az ezeket érintő LI viszonyrendszerének alakulásáról, a hírközlés és a hazai LI tevékenység evolúciós folyamataik elemzésére alapozva. Az értekezés során össze kívánom hasonlítani a mobil hírközlésre, valamint az alkalmazásszolgáltatásokra irányuló LI tevékenység hazai normatív környezetét, majd következtetéseket kívánok levonni azok hatékonyságáról. Vizsgálni kívánom és következtetéseket kívánok levonni az IKT környezet fejlődéséből adódó többlet LI lehetőségekről.

Mind a mobilhálózatok, mind az alkalmazásszolgáltatások kriptográfiai környezetének általános vizsgálatára alapozva meg kívánom állapítani, hogy melyek a vizsgálat tárgyát érintő főbb kriptográfiai jellemzők, valamint, hogy ezek milyen hatékonyságkorlátozó jellemzőkkel bírnak az LI szempontjából. Következtetéseket kívánok levonni továbbá a kriptográfiai környezet fejlődésének és a felhasználók adatkezelési attitűdjét befolyásoló egyes globális eseményeknek az alkalmazásszolgáltatások keresletváltozására gyakorolt hatásaival kapcsolatban. Az alkalmazásszolgáltatások nemzetbiztonsági célú LI-jének hazai normatív környezetét elemezve, azt összevetve a kriptográfiai fejlődésével további következtetéseket kívánok levonni a közleményellenőrzés ellenállóképességéről, hatékonyságáról.

Az értekezés során célom kitekinteni az alkalmazásszolgáltatások jogszerűtlen célú felhasználási formáira, gyakorlati példákkal igazolva azok ellenőrzésének létjogosultságát, valamint az LI korlátozott hatékonyságának társadalomra veszélyességét. Tekintettel az

elektronikus hírközlés globalizációjára az értekezés során következtetéseket kívánok levonni az LI tevékenység egyes nemzetközi tapasztalatairól, az alkalmazásszolgáltatások értintő LI jellegű kihívásokról. Össze kívánom hasonlítani a nemzetbiztonsági és a bűnüldözési célú LI-re irányuló nemzetközi együttműködések rendszerét, mely alapján értékelni kívánom a nemzetbiztonsági célú LI nemzetközi együttműködésének aktualitásait, a két tevékenységi kör viszonyrendszerét. Továbbá nemzetközi kitekintést kívánok tenni elsősorban az alkalmazásszolgáltatások LI-jével kapcsolatos kihívásokra, gyakorlatra, illetve a nemzetközi együttműködés lehetőségeire. Következtetéseket kívánok levonni arra vonatkozóan, hogy az IKT környezet változása milyen konkrét hatásokkal bír a titkos információgyűjtésre, első sorban az LI aspektusából a stratégiaalkotás, a jogalkotás és a tényleges LI képességek tekintetében. Az értekezés prognosztikus jellegű vizsgálatának időtávja illeszkedik az EU Digitális évtized 2030 szakpolitikai program és a hazai Stratégia 2030-as időtávjához.

A doktori értekezés fő célja a fenti elemzések, vizsgálatok során elért tudományos következtetésekre alapozva olyan gyakorlatorientált, az alkalmazott kutatásokhoz integrálható nyilvános tudományos eredmények elérése, amelyek magukban hordozzák a hazai LI képességek hatékonyságfokozásában való közreműködés lehetőségét, elsősorban jogalkotási irányok, szemléletformálás, további részkutatási irányok meghatározása által. A kutatás a feldolgozott szakirodalom rendszerző jellegű áttekintésén túl, elsődlegesen az egyes vizsgált témakörök vonatkozásában új tudományos alaposságú összefüggések feltárására, következtetések levonására hivatott. A célkitűzéseket az alábbi kutatási, vizsgálati módszerek alkalmazásával kívánom elérni, egyben a nemzetbiztonsági célú LI kutatás új tudományos módszertanának megalkotásával, és az értekezés során való alkalmazásával.

1.5. Kutatási módszertan

Az értekezés során meghatározó kutatási módszerként kerülnek alkalmazásra a statisztikai adatelemzés, a trend és tendenciaelemzés, a szakmatörténeti kutatás, a jogszabályi elemzés és interpretáció, a dokumentum- és tartalomelemzés, valamint az azokon alapuló adatok és információk komplex szemléletű, egyes kvantitatív és kvalitatív szempontú elemzése, értékelése, illetve az esettanulmány jellegű feldolgozás. A szakirodalom feldolgozása, a források kritikai szemlézése során támaszkodok továbbá az elemzési munka komparatív elemzési módszerére. A kutatómunka során végig alapelvként érvényesül az észszerűség, a logika alkalmazása, az alapos és objektív „megfigyelés”, elemzés.

Az értekezés során a mobil hírközlési szolgáltatásokat és az alkalmazásszolgáltatásokat érintő egyes infokommunikációs trendekkel, tendenciákkal kapcsolatos szakirodalom feldolgozásán túl a nyíltan hozzáférhető aktuális, illetve prediktív statisztikai adatok kerülnek kvalitatív módon elemzésre és értékelésre. Kutatási kihívásként azonosítható a vizsgált tárgykört érintően a rendelkezésre álló források, statisztikai adatok megbízhatóságának, hitelességének kérdése, így azok széles körben, egymással összevetve kerülnek feldolgozásra a hiteles forráselemzés érdekében.

Vizsgálat tárgyát fogja képezni a nemzetbiztonsági – és összehasonlítási céllal a bűnüldözési – célú LI hazai normatív környezete a vonatkozó szakirodalom és jogszabályok dokumentum-, tartalomelemzés jellegű feldolgozásával, a hazai és nemzetközi, azon belül is az uniós jogforrások, a digitalizációval összefüggő uniós törekvések párhuzamos feldolgozásával. Az Emberi Jogok Európai Bíróságának (a továbbiakban: EJEB), az Európai Unió Bíróságának (a továbbiakban: EUB) és az Alkotmánybíróság ítélkezési gyakorlata is bemutatásra kerül a témához kapcsolódó egyes döntéseiknek ismertetése során. Továbbá az Európai Adatvédelmi Testület (a továbbiakban: EDPB[64]) és a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) egyes releváns döntései is feldolgozásra kerülnek az információs önrendelkezési jog korlátozását érintő jogvitákat illetően.

A hírközlést és az alkalmazásszolgáltatásokat érintő törvényes kommunikációellenőrzés hazai szervezetrendszerének, tevékenységének evolúciós vizsgálata során a fenti szempontrendszer mentén áttekintésre kerül a 21. századi hazai technológia és szabályozás fejlődése, egyfajta integrált, komplex módszertan alkalmazásával az LI-vel kapcsolatos szakmatörténeti dokumentumok, normák és jogszabályok, valamint statisztikai adatok összevetésével. Az értekezés gyakorlatorientált megközelítése érdekében esettanulmány jelleggel kerülnek feldolgozásra az alkalmazásszolgáltatások jogszerűtlen célú felhasználásával kapcsolatos nemzetközi példák, kihívások.

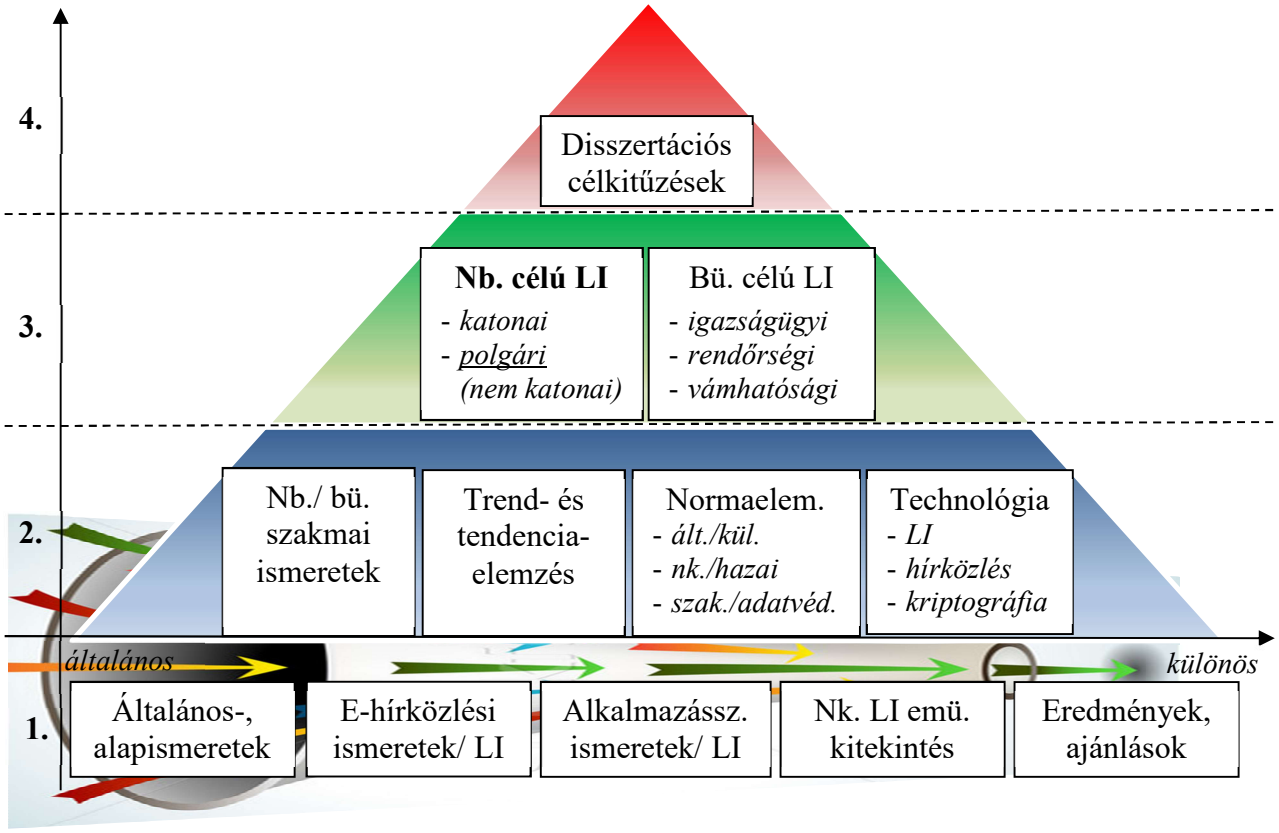
Az értekezés kutatási módszerei műszaki, technológiai elemzést, mérést nem tartalmaznak. A kutatási módszerek alkalmazása során a minősített adat védelméről szóló 2009. évi CLV. törvény szerinti minősített adat nem kerül feldolgozásra, kezelésre és nyilvánosságra hozatalra.

[64] EDPB: European Data Protection Board - Európai Adatvédelmi Testület

A témaválasztás és a kutatás aktualitása indoklásának átlagosnál hosszabb terjedelme, a tudományos probléma megfogalmazása, és a fenti módszertani leírás során láthatóvá vált a tudományos vizsgálatot igénylő igen komplex téma, amely komponensei alapján egy:

- szigorú logikai szerkezetű (általánostól halad és szűkül a különösig);
- integrált tartalmú (nemzetbiztonsági és bűnüldözési szakmai ismeretek; trend- és tendenciaelemzés; normaelemzés; technológiai és digitalizációs ismeretek);
- összefüggő tevékenységi célzat alapú (nemzetbiztonsági célzat, bűnüldözési célzat)

összetett kutatási módszertant tesz szükségessé a hipotézisek alátámasztása és az értekezés célkitűzéseinek megvalósítása érdekében. Ennek okán kidolgoztam a disszertációs kutatómunka során alkalmazott „*nemzetbiztonsági célú LI kutatás integrált interdiszciplináris tudományos módszertanát*”, amelyet az alábbi 2. ábra hivatott szemléltetni:



2. ábra: Nemzetbiztonsági célú LI kutatás integrált interdiszciplináris tudományos módszertana[65]
(Szerk.: A szerző)

[65] Rövidítések: E-hírközlési ismeretek – Elektronikus hírközlési ismeretek; Alkalmazássz. ismeretek – Alkalmazásszolgáltatási ismeretek; Nk. LI. emü. kitekintés – Nemzetközi LI együttműködési kitekintés; Nb./ bü. szakmai ismeretek – Nemzetbiztonsági és bűnüldözési szakmai ismeretek; Normaelem. – Normaelemzés; ált./kül. – általános és különös; nk./hazai – nemzetközi és hazai; szak./adatvéd. – szakági és adatvédelmi; Nb. célú LI – Nemzetbiztonsági célú LI; Bü. célú LI – Bűnüldözési célú LI.

A disszertációs kutatómunka keretében a kidolgozott kutatási módszertan alapján a szakirodalom[66] feldolgozása során, a hipotéziseknek megfelelően, az értekezés szerkezetéhez[67] illeszkedve az alfejezetekben integrált módon kerülnek elemzésre az egyes tartalmi szempontok, a tevékenység célzat alapú vizsgálatával egyetemben, melynek fő iránya a „polgári nemzetbiztonsági[68] célzat". Így vertikálisan kiteljesítve a piramis csúcsán elhelyezkedő disszertációs célkitűzéseket, horizontálisan pedig az új tudományos eredmények elérését, ajánlások megfogalmazását, végsősoron a doktori (PhD) értekezés elkészültét.

1.6. Szakirodalmi áttekintés

Az értekezés szakirodalmi forrásainak csoportosítása:

- eredet szerint: hazai, nemzetközi;
- téma szerint: nemzetbiztonság elméleti, bűnüldözés elméleti, jogtudományi és szakági jogi, ítélkezési és egyéb jogalkalmazói gyakorlat, hírközlési ismeretek, infokommunikációs ismeretek, kriptográfiai ismeretek, szakmatörténeti ismeretek;
- forrás szerint: mértékadó tudományos folyóiratok és publikációk, jogforrások, minisztériumok, állami szervek, kormányzati főhivatalok és önálló szabályozó szervek által publikált statisztikai adatok, tanulmányok, elemzések, levéltári gyűjtemények dokumentumai, továbbá a világhálón elérhető forráskritikával szemlézett sajtóközlemények és statisztikák;
- szerző szerint: tudományos kutatók, jogászok, politikusok, szakértők, szakújságírók;
- forrás nyelve szerint: magyar, angol, francia, német, spanyol nyelvű dokumentumok, eredeti nyelven vagy fordításban, illetve közvetítő nyelven.

A forráskiválasztás során a nyíltan hozzáférhető hazai és nemzetközi forrásokat kívánom vizsgálni, áttekinteni. Tekintettel arra, hogy a vizsgált témakör egységes, és szisztematikus feldolgozása korábban csak korlátozottan történt meg, a források felkutatása során a résztémakörök határterületeihez kapcsolódó szakirodalmat is elemzem. Az értekezésben, azon belül is az egyes összehasonlítások, következtetések levonása során alkalmazásra kerül a nemzetbiztonsági és bűnüldözési területen eltöltött évtizedes szakmai gyakorlat keretében

[66] Lásd: „1.6. Szakirodalmi áttekintés" című alfejezet
[67] Lásd: „1.7. Az értekezés szerkezete" című alfejezet
[68] Értsd: A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 2. § (1) bek. szerinti polgári nemzetbiztonsági szolgálatok (Információs Hivatal, Alkotmányvédelmi Hivatal, Nemzetbiztonsági Szakszolgálat, Nemzeti Információs Központ) tevékenységi célzata.

megszerzett látásmód, és ismeretek, így még gyakorlatorientáltabbá téve a kutatómunkát és az elért eredményeket, azok alkalmazott tudományos jellegét.

1.7. Az értekezés szerkezete

Az értekezés bevezető részében, azaz a 1. fejezetben ismertetésre kerül a témaválasztás és a kutatás aktualitásának indoklása, a tudományos probléma megfogalmazása, a hipotézisek, az értekezés célja, a kutatási módszertan, a szakirodalom áttekintése, jelen alfejezetben pedig az értekezés szerkezete, annak felépítése, és a további alfejezetek főbb tartalmának bemutatása.

Az értekezés érdemi tartalmi első része, azaz a 2. fejezet fő tárgyköre az LI garanciális, szervezetrendszeri, fogalmi és módszertani hátterének áttekintése egyfajta felvezetőként, a szükséges alapvető ismeretek tárgyalásaként, a további fejezetekben szereplő kutatási cselekmények előkészítése céljából. A fejezeten belül előkérdésként értelmezésre kerül a „nemzetbiztonsági cél” tartalma, majd vizsgálat tárgyát képezi az LI szabályozásának nemzetközi és hazai keretrendszere, az LI alapvető jogi és adatvédelmi garanciális hátterének áttekintése, az EU digitális piaci és adatvédelmi stratégiai célkitűzései hatásainak elemzése az LI aspektusából. Továbbá az LI hazai szervezetrendszerének és általános normatív háttérének ismertetése, információelméleti háttere és annak átültetése a normatív környezetbe, egyes főbb módszerei, eljárásai, a szükséges kriptográfiai alapismeretek és kihívásainak áttekintése. Valamint elvégzésre kerül az egyes alfejezetek kutatási cselekményei alapján megállapítható részkövetkeztetések levonása.

Az értekezés érdemi tartalmi második része, azaz a 3. fejezet fő tárgyköre a mobil hírközlési ellenőrzést érintő IKT trendek, tendenciák komplex és szisztematikus elemzése a meghatározott kutatási módszertan alapján, a hipotézisek alátámasztása és az új tudományos eredmények eléréséhez szükséges részkutatómunka elvégzése érdekében. A fejezeten belül vizsgálat tárgyát képezi az elektronikus digitális mobil hírközlőhálózatok evolúciója, fejlődési trendjei, a mobilhálózatok felhasználói tendenciái, a mobilhálózatok kriptográfiai környezetének evolúciója, trendjei, kitekintve az LI szabványosításra, a hazai hírközlési kommunikációellenőrzés normatív, szervezeti, technológiai evolúciója, trendjei. Valamint elvégzésre kerül az egyes alfejezetek kutatási cselekményei alapján megállapítható részkövetkeztetések levonása.

Az értekezés érdemi tartalmi harmadik része, azaz a 4. fejezet fő tárgyköre az alkalmazásszolgáltatások LI-jét érintő IKT trendek, tendenciák komplex és szisztematikus elemzése a meghatározott kutatási módszertan alapján, a hipotézisek alátámasztása és az új tudományos eredmények eléréséhez szükséges részkutatómunka elvégzése. A fejezeten belül vizsgálat tárgyát képezi az alkalmazásszolgáltatások felhasználói trendjei, az alkalmazásszolgáltatásokkal összefüggő adatvédelmi trendek, a biztonsági kihívási tendenciák és válaszintézkedések a nemzetközi térben, az alkalmazásszolgáltatások LI-jének hatályos hazai normatív, szervezeti evolúciója, trendjei. Valamint elvégzésre kerül az egyes alfejezetek kutatási cselekményei alapján megállapítható részkövetkeztetések levonása.

Az értekezésnek a végkövetkeztetések levonását, összefoglalását szolgáló befejező része az 5. fejezet, amelyben az IKT környezet változásának a titkos információgyűjtésre gyakorolt stratégiai, jogalkotási, és LI képességeket érintő hatásairól szóló komplex, a fejezetek részkövetkeztetéseit a hipotézisek mentén összefoglaló eredményei kerülnek bemutatásra. A 6. fejezetben kerülnek tételesen felsorolásra az új tudományos eredményként történő elfogadásra javasolt disszertációs kutatási eredmények. A 7. fejezet tartalmazza a kutatás eredményeinek gyakorlati felhasználhatóságára irányuló konkrét ajánlásokat, javaslatokat. Végezetül az értekezés elkészítése, a disszertációs kutatómunka során felhasznált szakirodalom jegyzéke és a publikációk jegyzéke kerül szerepeltetésre, majd a mellékletek jegyzéke és azok csatolása történik.

2. A TÖRVÉNYES KOMMUNIKÁCIÓELLENŐRZÉS (LI) GARANCIÁLIS, HAZAI SZERVEZETRENDSZERI, FOGALMI ÉS MÓDSZERTANI HÁTTERE

Jelen fejezetben az LI garanciális, szervezetrendszeri, fogalmi és módszertani hátterének áttekintésére kerül sor, egyfajta felvezetőként a szükséges alapvető ismeretek tárgyalásaként, a további fejezetekben szereplő kutatási cselekmények előkészítése céljából. A fejezeten belül előkérdésként értelmezésre kerül a „nemzetbiztonsági cél" tartalma, majd vizsgálat tárgyát képezi az LI szabályozásának nemzetközi és hazai keretrendszere, az LI alapvető jogi és adatvédelmi garanciális hátterének áttekintése, az EU digitális piaci és adatvédelmi stratégiai célkitűzései hatásainak elemzése az LI aspektusából. Továbbá az LI hazai szervezetrendszerének és általános normatív háttérének ismertetése, információelméleti háttere és annak átültetése a normatív környezetbe, egyes főbb módszerei, eljárásai, a szükséges kriptográfiai alapismeretek és kihívásainak áttekintése. Valamint elvégzésre kerül az egyes alfejezetek kutatási cselekményei alapján megállapítható részkövetkeztetések levonása.

2.1. A „nemzetbiztonsági célzat" értelmezése

Az értekezés tárgyköre a „nemzetbiztonsági célú" LI-re konkretizálódik, így szükséges egyfajta előkérdésként annak biztonsági stratégiai, szakági jogi, etimológiai[69] és uniós jogi értelmezése (interpretálása), és elhatárolása, legalábbis árnyalása a „bűnüldözési célú" LI-től. A nemzetbiztonság célzat álláspontom alapján a nemzetbiztonsági érdek mentén konkretizálható, azaz lenne konkretizálható, hiszen a „nemzetbiztonsági érdek" értelmezése is tudományos jellegű vitákat gerjeszt az azt vizsgáló kutatók körében. A „nemzetbiztonság érdek"-ből absztrahálható „nemzetbiztonsági célzat" fogalmának levezetése érdekében első lépésként meg kívánom vizsgálni a hazai biztonság és védelmi tárgyú átfogó stratégiák fogalomrendszerét és annak evolúcióját[70], a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (a továbbiakban: Nbtv.) szerinti fogalomrendszerét, a témakört etimológiailag feldolgozó szakirodalmat, valamint az uniós jog tekintetében megjelenő interpretációs formákat. E fejezet

[69] Etimológia: A szavak eredetével foglalkozó nyelvészeti tudományág. Forrás: BAKOS Ferenc (2009): *Idegen szavak és kifejezések szótára*. Budapest: Akadémiai Kiadó Zrt.

[70] Lásd: TÓTH Tamás (2022): Magyarország nemzeti biztonsági stratégiai evolúciója, annak aktualitásai és főbb nemzetbiztonsági vetületei. *Szakmai Szemle*, 20(2), 58-73. Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_2_szam.pdf#page=58 (Letöltés ideje: 2024. február 16.)

következtetéseként értelmezett, meghatározott „nemzetbiztonsági célú” fogalomhasználat fog érvényesülni az értekezés során, így annak részletesebb elemzésére, alátámasztására kerül sor.

Magyar átfogó biztonsági stratégiai fogalomrendszer (Stratégia):

Az 1990-es évektől a közép-kelet-európai térségben egyfajta biztonság-, gazdaság- és társadalompolitikai irányváltás volt megfigyelhető, amely a kétpólusú világrend megszűnésével, a volt szovjet európai befolyási övezet „demokratizálódásával” új geopolitikai helyzetet teremtett. Ez az államok átfogó stratégiai céljaiban kifejezte az európai politikai értékeken alapuló demokrácia, a jogállamiság, az euroatlanti integráció, a piacgazdasági modell kialakításának szándékát, a nemzeti szuverenitás-kiteljesítés mellett.[71] A biztonsági (NATO), gazdasági, politikai (EU), társadalmi, és technológiai környezeti változások folyamatosan hatottak Magyarország átfogó biztonsági stratégiai környezetére, azon belül is a nemzetbiztonsági cél, érdek tartalmára dinamikus módon.[72] A 2004-es biztonsági stratégiában[73] a korábbihoz képest hangsúlyosabb a nemzetbiztonsági szolgálatok szerepe a kormányzati döntés-előkészítés, az ország szuverenitásának, alkotmányos rendjének védelme, és nemzetbiztonsági érdekeinek érvényesítése terén, valamint nyomatékosításra kerül az ágazaton kívüli együttműködés jelentősége is. A 2012-ben elfogadott Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat szerkezetében, tartalmában már érvényesül az Amerikai Egyesült Államok (a továbbiakban: USA[74]) stratégiaalkotási szemlélete.[75] A 2012-es stratégia 2. pontja tovább mélyíti a biztonság átfogó értelmezésének vetületét, 31. pontjában a Magyarországot érintő biztonsági fenyegetések és kihívások kapcsán új tényezőként megjelent a kiberbiztonság és annak garantálása érdekében a nemzetbiztonsági ágazat szerepe is, mely fokozódó hangsúlyosságát a 2013. március 23-án elfogadott Magyarország Nemzeti Kiberbiztonsági (ágazati) Stratégiája[76] is jelez. A 2012-es stratégia tovább mélyíti a nemzetbiztonsági szolgálatok együttműködésének igényét a honvédelmi, rendvédelmi, igazságügyi és polgári védelmi szervekkel.

---

[71] TÁLAS Péter (2013): A nemzeti katonai stratégia és a magyar stratégiai kultúra. *Hadtudomány*, 23(3-4), 22-23. Online: https://www.mhtt.eu/hadtudomany/2013/3_4/Hadtudomany_2013_3-4_3.pdf (Letöltés ideje: 2024. február 16.)

[72] Lásd: DOBÁK Imre – TÓTH Tamás (2023): A külső környezet, és tendenciák nyomon követésének szükségessége a stratégiaalkotás tükrében. In DOBÁK Imre – RESPERGER István (szerk.): *Stratégiák, stratégiai gondolkodás, nemzetbiztonság*. Budapest: Ludovika Egyetemi Kiadó. 33-50.

[73] 2144/2002. (V. 6.) Korm. határozat Magyar Köztársaság nemzeti biztonsági stratégiájáról

[74] USA: United States of America – Amerikai Egyesült Államok

[75] KISS Petra (2012): A magyar stratégiai gondolkodás változása a nemzeti biztonsági stratégiák tükrében. *Hadtudomány*, 22(3-4), 60. Online: https://www.mhtt.eu/hadtudomany/2012/3_4/HT_2012_3-4_Kiss_Petra.pdf (Letöltés ideje: 2024. február 16.)

[76] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

Többek között Európát 2015/16-tól fokozottan érintő migrációs válság, az iszlám fundamentalista terrorizmus térnyerése, az új és innovatív technológiák által megjelenő globális hibrid jellegű biztonsági kihívások, a kiberbiztonságot veszélyeztető tevékenységek fokozódása, valamint a világűrben rejlő lehetőségek biztonsági célú kiaknázhatósága átfogó biztonsági stratégiai felülvizsgálatra késztette a kormányt. Ennek okán 2020. április 23-án hatályba lépett a Stratégia[77]. A szakirodalom alapján a Stratégia világképe „*reálpolitikai, és a globális biztonsági helyzet romló tendenciájával, biztonsági környezetünk jellemzőinek fokozatos romlásával számol a 2020-as évtizedben. Ugyanakkor azonosítja azokat a lehetőségeket is, amelyek elősegíthetik érdekeink érvényesítését.*"[78] A Stratégia fő célja az ország jelenlegi biztonsági szintjének megőrzése és erősítése, valamint az ország további fejlődésének biztosítása, továbbá Magyarország stratégiai célkitűzése, hogy 2030-ra kialakítsa azokat a nemzeti ellenálló, elrettentési, védelmi, válságkezelési és koordinációs képességeket, amelyek előfeltételei a nemzet fejlődéséhez szükséges stabilitásnak és biztonságnak. Ennek érdekében a Stratégia kiemeli többek között a nemzetbiztonsági szolgálatok fokozott szerepét, hiszen a Stratégia 126. pontja alapján a „*biztonság elsődleges alapja a szilárd társadalmi, gazdasági és pénzügyi szerkezet, valamint nemzeti szinten a megelőző és védelmi intézkedések fenntartható és rugalmas rendszere, ezen belül pedig a haderő, valamint a rendvédelmi szervek ([…] a nemzetbiztonsági szolgálatok, […]) célirányos fejlesztése.*" A Stratégia a hazai védelmi ipar fejlesztésének támogatását is nemzetbiztonsági érdekként határozza meg, akár csak az innováción alapuló űrszektor nemzetbiztonsági célú hozzáférését. Továbbra is cél a korábbi stratégiákban szintén megjelenő szervezett bűnözés, terrorizmus, illegális migráció megelőzésében és felderítésében való részvétel. Új elemként került beemelésre a hibrid támadások leleplezésében és elhárításában való közreműködés, illetve a stratégia tovább mélyíti a nemzetbiztonsági szolgálatok ágazatokon átívelő együttműködésének igényét nemzeti és nemzetközi szinten egyaránt.[79]

A Stratégia 166. pontja az Alaptörvény, valamint az Nbtv. vonatkozó anyagi jogi rendelkezéseivel összhangban az átfogó feladatok között kiemeli a nemzetbiztonsági

[77] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról és egyben annak 1. számú mellékleteként a „Biztonságos Magyarország egy változékony világban" című átfogó nemzeti biztonsági stratégia.

[78] CSIKI VARGA Tamás – TÁLAS Péter (2020): Magyarország új nemzeti biztonsági stratégiájáról. *Nemzet és Biztonság*, 13(3), 111. Online: https://www.nemzetesbiztonsag.hu/cikkek/4906-cikk_szoveg-16687-1-10-20210426.pdf (Letöltés ideje: 2023. augusztus 08.)

[79] Lásd: TÓTH Tamás (2022): Magyarország Nemzeti Biztonsági Stratégiájának nemzetbiztonsági aspektusú elemzése. *Szakmai Szemle,* 20(3), 69-99. Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_3_szam.pdf (Letöltés ideje: 2024. február 16.)

szolgálatok szerepét. Eszerint „*A nemzetbiztonsági szolgálatok tevékenysége Magyarország szuverenitása, alkotmányos rendje védelmének, biztonságpolitikai céljai elérésének és nemzeti érdekei érvényesítésének meghatározó eleme. A politikai, katonai és gazdasági információk megvédése szükségessé teszik a korszerű és hatékonyan összehangolt hírszerző és elhárító képességek alkalmazását.* A Stratégia 166. pontja továbbá a nemzetbiztonsági szolgálatok alapvető feladatként definiálja, hogy „*különleges műveleti eszközeik és módszereik hatékony felhasználásával derítsék fel és akadályozzák meg a Magyarország nemzeti érdekeit leplezett formában veszélyeztető törekvéseket, illetve azonosítsák a törekvések hátterében álló állami, illetve nem kormányzati szereplőket*." A biztonsági környezet romlása okán szükségesnek tartja a nemzetbiztonsági szolgálatok képességeinek továbbfejlesztését, különös tekintettel a titkos információgyűjtés koncentrált eszközrendszerére. A Stratégia kiemelt kockázatként azonosítja a kormányzati és létfontosságú rendszereket veszélyeztető, érintő kibertámadásokat, incidenseket. Központi célkitűzésként jelenik meg benne az offenzív kiberképesség kialakítása is, melyek törvényi leképeződésére például az Nbtv. 56. § e) pontjának 2020. július 01-jei módosításával került sor. Solti István gondolatai alapján „*Magyarország nemzetbiztonsági szférájának alapvető rendeltetése és faladata, hogy a kellő időben észlelje, jelezze, befolyásolja vagy megelőzze az ország biztonságát veszélyeztető folyamatokat és jelenségeket, illetve részt vegyen az ország szuverenitását és a demokratikus jogrendet támadó magatartások tevőleges felszámolásában."*[80]

A Stratégia mélyebb vizsgálata alapján megállapítható, hogy alapvető – nemzetbiztonsági – érdekként azonosítja továbbá azt, hogy *„A hazai védelmi ipar, azon belül is a kutatás-fejlesztés és az innováció támogatása nemzetbiztonsági érdek, mivel ezek által csökkenthető az import függőség, növelhető az ellátásbiztonság és hazai gyártmányokkal korszerűsíthetőek a védelmi eszközök.*[81] A nemzetbiztonsági szolgálatokkal szemben általános elvárás, hogy az intenzíven változó külső környezethez (technológiai, normatív, társadalmi, biztonsági, politikai stb.) igazodva hatékonyan és harmonizáltan lássák el alapfeladataikat, amely azonban kizárólag a változások egyedi jellemzőinek figyelembevételével, közép- és hosszú távú stratégiai célkitűzések mentén valósítható meg. Korábbi kutatási eredményeim alapján megállapítható, hogy míg a nemzetbiztonsági tevékenységgel érintett személyek, csoportok és szervezetek

[80] SOLTI István (2014): A nemzetbiztonsági stratégia a Nemzeti Biztonsági Stratégia tükrében. *Nemzetbiztonsági Szemle*, 2(3), 59. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/2084/1362 (Letöltés ideje: 2024. február 14.)
[81] Stratégia 105. pontja

eszközparkjában rövid idő alatt jelennek meg a legmodernebb technológiák, infokommunikációs eszközök és -szolgáltatások, addig a nemzetbiztonsági tevékenység normatív és metodikai kidolgozása, a titkos információgyűjtő képességek fejlesztése egy megfelelő prognosztizációs képességgel bíró hosszú távú folyamat eredménye.[82] 2017. július 1-től megalakult a HM Védelmi Technológiai Kutató Központ, mely feladata „*.a haditechnikai irányú kutatás-fejlesztési és technológiai innovációs tevékenységének stratégiai szintű felügyelete, a kutatás-fejlesztési feladatok fő irányainak meghatározása, továbbá a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Programmal összefüggő hadiipari kutatás-fejlesztési feladatok végrehajtása, […] [amely] 2019. év január 1-jétől […] Modernizációs Intézet néven végzi […] feladatait*”.[83] Ezen honvédelmi K+F+I törekvések katonai nemzetbiztonsági célú szervezeti leképeződése a Katonai Nemzetbiztonsági Szolgálat (a továbbiakban: KNBSZ) szervezetében 2018. január 01-től a KNBSZ Innovációs és Kutatóközpontjában (a továbbiakban: KNBSZ IKK) érhető tetten.[84] A stratégiai K+F+I célkitűzési mentén az MI-vel és a kibervédelemmel kapcsolatos polgári nemzetbiztonsági célú fejlesztések elősegítése érdekében 2020. szeptember 30-án megalakult a Mesterséges Intelligencia Nemzeti Laboratórium (a továbbiakban: MiLab), amely partnerszervezetévé vált a Nemzetbiztonsági Szakszolgálat (a továbbiakban: NBSZ) is. Az NBSZ álláspontja szerint „*az M.I. különösen szakértői és kibervédelmi tevékenységeink során, nem csak szolgáltatásaink minőségi javulását eredményezheti, de szükségszerűen alapja lesz egy hatékonyabb, Magyarország (és az Unió) biztonságát új szintre emelő védelmi-ökoszisztémának.”*[85] Az infokommunikációval kapcsolatos nemzetbiztonsági célú K+F+I okán az NBSZ konzorciumi vezetésével 2020-ban megalakult az Infokommunikációs és Információtechnológiai Nemzeti Laboratórium (a továbbiakban: InfoLab), mely *kiemelten fókuszál a jövő hírközlésének gerincét adó 5G (és 6G) technológiák sérülékenységének, valamint a kiberbiztonság egyes kérdésköreinek, valamint a Mesterséges Intelligencián (MI) alapuló megoldások e-közigazgatásba való bevezetésének*

[82] TÓTH Tamás (2020): Az információgyűjtő szervezetek technikai képességeire ható külső közvetett tényezők. *Felderítő Szemle*, 19(2), 44-45. Online: https://www.knbsz.gov.hu/hu/letoltes/fsz/2020-2.pdf#page=43 (Letöltés ideje: 2024. február 14.)

[83] KENEDLI Tamás (2020): A Katonai Nemzetbiztonsági Szolgálat szakmai fejlődésének legfontosabb sajátosságai az elmúlt években. *Nemzetbiztonsági Szemle*, 8(1), 86-87. Online: https://epa.oszk.hu/02500/02538/00032/pdf/EPA02538_nemzetbiztonsagi_szemle_2020_01_074-094.pdf (Letöltés ideje: 2024. február 19.)

[84] JAGADICS Péter – RAJOS Sándor – SIMON László – SZABÓ Károly (2018): *A magyar katonai elhárítás története 1918–2018*. Budapest: Univerzum Könyvek. 197.

[85] *Mesterséges Intelligencia Nemzeti Laboratórium* (MiLab). Online: https://mi.nemzetilabor.hu/hu/partnerek/nemzetbiztonsagi-szakszolgalat (Letöltés ideje: 2023. november 08.)

kutatására."[86] Kovács László kapcsolódó kutatása alapján „*az elmúlt évek során egyre inkább felértékelődött azoknak az infokommunikációs rendszereknek a szerepe, amelyek a társadalom egésze működésének az alapját is jelentik. Ebből következően ezeknek a rendszereknek a védelme és a biztonsága ma már nemzetbiztonsági érdek, és így stratégiai cél is egyben."*[87] A vizsgált szakirodalom beszámol a fenti stratégiai célkitűzés, valamint annak az Nbtv. 9. §-ban megjelenő elvárások mentén létrejövő, a polgári nemzetbiztonsági szolgálatokat tömörítő új tudományos formáció megalakulásáról, azaz a szolgálatokat felügyelő és irányító Miniszterelnöki Kabinetiroda Polgári Nemzetbiztonsági Szolgálatokat Felügyelő Államtitkárság által irányított Tudományos Innovációs Fórum (a továbbiakban: TIF) ernyőszervezet megalakulásáról. A tanulmány bemutatja, hogy a „*Stratégia által megfogalmazott elvárások hogyan képeződnek le a szolgálatoknál, milyen feladatok, megoldások és képességek (tervezés, reziliencia*[88]*, együttműködés, innováció) jelentek meg. […] Az idézett [Nbtv. 9. §] szakasz a K+F tevékenységet célorientáltan közelíti meg, hiszen annak érdekében kell végezni kutatást, fejlesztést, hogy az alaptevékenység végrehajtását segítse. […] A [TIF működési] modellválasztás adott, mert a Triple Helix rendszer*[89] *is a szereplők kooperációját helyezi a középpontba, de a tudomány, kutatás, fejlesztés és innováció oldaláról.*[90]

A stratégiai evolúciós elemzés során látható, hogy a „nemzetbiztonsági érdek", így az abból absztrahálható „nemzetbiztonsági célzat" tartalma dinamikusan, a kor elvárásai mentén

---

[86] *Infokommunikációs És Információtechnológiai Nemzeti Laboratórium* (InfoLab). Online: https://infolab.nemzetilabor.hu/hu/infokommunikacios-es-informaciotechnologiai-nemzeti-laboratorium-infolab (Letöltés ideje: 2023. november 08.)

[87] KOVÁCS László (2020): A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle*, 145(5.) 17. Online: https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/120/121 (Letöltés ideje: 2023. november 08.)

[88] Lásd: KASSAI Károly (2023): Az ellenálló képességre (resilience) vonatkozó NATO, EU általános követelmények fontosabb megjelenítéseinek áttekintése. *Military and Intelligence CyberSecurity Research Paper*, 3(8). Online: file:///D:/_PC16%20-%20t%C3%B6r%C3%B6lni%20TILOS!/FORWARD/Felhaszn%C3%A1l%C3%B3/Let%C3%B6lt%C3%A9sek/MIC%20RP%202023-8%20-%20Kassai%20K%C3%A1roly%20-%20Az%20ellen%C3%A1ll%C3%B3%20k%C3%A9pess%C3%A9gre%20(resilience)%20vonatkoz%C3%B3%20NATO,%20EU%20%C3%A1ltal%C3%A1nos%20k%C3%B6vetelm%C3%A9nyek%20fontosabb%20megjelen%C3%ADt%C3%A9seinek%20%C3%A1ttekint%C3%A9se.pdf (Letöltés ideje: 2024. február 14.)

[89] „*A Triple Helix a közigazgatás, az iparág és az egyetemi szféra együttműködési modellje, amelynek célja a hatékony kapcsolatrendszer építése a szereplők között, evvel támogatva a folyamatos innovációt.*"

[90] SZABÓ Hedvig (2023): A tudomány és a nemzetbiztonsági érdek, mint a polgári nemzetbiztonsági szolgálatok tudományos működésének új modellje, különféle tényezők hatása innovációs tevékenységükre a mesterséges intelligencia korában. *Nemzetbiztonsági Szemle*, 11(2), 47-56. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/download/6823/5491/29642 (Letöltés ideje: 2024. február 14.)

változik, alakul a hagyományos területektől elmozdulva a digitális kihívások (kibervédelem, űrtechnológia), vagy éppen a K+F+I (védelmi ipar, nemzetbiztonsági ipar, KNBSZ IKK, MiLab, InfoLab, TIF) irányába. Ennek nemzetbiztonsági szakági jogi leképezését az Nbtv. elemzésével is indokolt megvizsgálni, mind anyagi jogi, mind alaki tekintetben.

Hazai szakági jogi fogalomrendszer (Nbtv.):

Anyagi jogi szempontból az Nbtv. 74. § a) pontja taxatív felsorolással definiálja Magyarország függetlenségének biztosítása és törvényes rendjének védelme céljából megjelenő nemzetbiztonsági érdek fogalmát, amely érdekkörben eljárva az egyes nemzetbiztonsági szolgálatok Nbtv. 4. – 9. § feladat- és hatáskörei szerinti tevékenysége az absztrahált „nemzetbiztonsági célzat" fogalma, melyet tevékenységi szempontból érdemes vizsgálni. Azonban ez esetben azonosítható egy a stratégiai evolúció során is felmerülő problémakör, mégpedig az egyes nem tiszta, azaz vegyes nemzetbiztonsági/ bűnüldözési célú feladatok tekintetében például az Nbtv. 74. § ae) alpont szerinti terrorcselekmények, az illegális fegyver- és kábítószer-kereskedelem, a nemzetközileg ellenőrzött termékek és technológiák illegális forgalmának felderítése és megakadályozása – így a határokon átnyúló szervezett bűnözés – tekintetében, amelyek a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) különös részében is deklarált társadalomra veszélyes bűncselekmények. A vizsgált szakirodalom közvetlen nemzetbiztonsági kockázatokat azonosít például a tömeges illegális bevándorlás kapcsán, így a bűnügyi helyzet negatív irányú megváltozását, az embercsempész szervezetek megerősödését, a válságövezetekből Európába érkező migránsok között potenciálisan megbúvó visszatérő harcosok terrorkockázatát, és „élményeiknek", tapasztalataiknak radikalizációs célú közvetítését.[91]

A nemzetbiztonsági/ bűnüldözési célzat elhatárolása, árnyalása körében értelmezhető továbbá például a megbízhatósági vizsgálat kérdésköre is, amelyet az Nbtv. 5/B. § alapján az Alkotmányvédelmi Hivatal (a továbbiakban: AH) a Kormány vagy a Kormány tagjának irányítása vagy felügyelete alá tartozó költségvetési szerv belső biztonsági és bűnmegelőzési célú ellenőrzésként hajt végre, a rendőrségről szóló 1994. évi XXXIV. törvény (a továbbiakban: Rtv.) szerinti belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerv hatáskörébe tartozó

[91] GUBICZA József – LAUFER Balázs (2014): Az illegális migráció aktuális trendjei nemzetbiztonsági szemszögből. *Pécsi Határőr Tudományos Közlemények*, 13(10), 293-294. Online: https://epa.oszk.hu/04500/04581/00015/pdf/EPA04581_pecsi_hataror_2014_287-295.pdf (Letöltés ideje: 2023. szeptember 11.); USHER, Sebastian (2014): *Tracking Syria fighters now main task for MI5*. BBC News. Online: https://www.bbc.com/news/uk-27947343 (Letöltés ideje: 2023. szeptember 11.)

szervek, valamint a honvédelmi szervezetek kivételével. Tehát, ha megbízhatósági vizsgálat keretében LI alkalmazására kerül sor, akkor az Nbtv. 5/B. – 5/D. § szerinti főszabályként nemzetbiztonsági célú, a kivétel szabály alapján az Rtv. szerinti érdekkörben pedig bűnüldözési – szűkebb értelemben belső bűnmegelőzési, bűnfelderítési – célú. Illetve felvetődik a főszabály és kivétel szabály nyomán a honvédelmi, azaz katonai (KNBSZ) és a nem katonai, azaz polgári (IH, AH) nemzetbiztonsági célzat is. Ami az Nbtv. anyagi joga szerinti „nemzetbiztonsági célzat" értelmezéséhez és a „bűnüldözési célzat"-tól való elhatárolásához, de legalábbis „árnyalásához" egyfajta támpontot adhat, az a külső engedélyhez kötött titkos információgyűjtő eszközök Nbtv. szerinti engedélyezésének rendje.[92]

Az Nbtv. 56. § (1) - (2) bek. alapján külső engedélyezőnek minősül a bíró és az igazságügyért felelős miniszter (a továbbiakban: igazságügyi miniszter) (a továbbiakban együtt: engedélyező). Az Nbtv. 58. § (1) bek. szerint az AH Nbtv. 5. § b), d), h) - j) pontjai, valamint a KNBSZ 6. § d), i), l) - n) pontjaiban meghatározott elhárítási, defenzív hírszerző funkciójú nemzetbiztonsági feladatainak ellátása során az Nbtv. 56. §-ban felsorolt titkos információgyűjtést – így az LI-vel érintett kommunikáció tartalmának leplezett megismerését és/vagy rögzítését is – a Fővárosi Törvényszék elnöke által kijelölt bíró engedélyezi. Összefoglalóan ilyen Magyarország:

- törvényes rendjének jogellenes eszközökkel történő megváltoztatására vagy megzavarására irányuló leplezett törekvések felderítése, elhárítása;
- gazdasági, tudományos-technikai, pénzügyi, honvédelmi biztonságát veszélyeztető leplezett törekvések felderítése elhárítása;
- a nemzetbiztonságot veszélyeztető jogellenes fegyverkereskedelemről a honvédelmi szervezetek biztonságát veszélyeztető szervezett bűnözésről szóló információgyűjtés;
- a jogellenes kábítószer- és fegyverkereskedelemről szóló információgyűjtés, annak felderítése, elhárítása;
- továbbá az AH és a KNBSZ működési területükön a nyomozás elrendeléséig végzi az Nbtv.-ben felsorolt Btk. szerinti bűncselekmények felderítését és az azokról való információk gyűjtését.

Összességében az Nbtv. tartalmi értelmezése körében megállapítható, hogy az egyes hazai nemzetbiztonsági szolgálatok Nbtv. szerinti fenti feladat- és hatáskörében első olvasatra

[92] A témakör a 2.5. alfejezetben részletes vizsgálat tárgyát képezi, így ott kerül magyarázásra, kifejtésre.

tapasztalható ugyan némi átfedés, de azok el vannak különítve a katonai és polgári nemzetbiztonsági célzat alapján. Az AH és a KNBSZ vonatkozásában már az alapfeladataik tekintetében is megjelenik a bűnüldözési érdekkörben felmerülő nemzetbiztonsági célú tevékenység, amennyiben a Btk. szerinti tényállások, valamint a bírói engedélyezés alapján végzett Nbtv. 56. § szerinti titkos információgyűjtés kontextusából közelítjük meg a kérdést.

Alaki szempontból a „nemzetbiztonsági érdek"-ből absztrahált „nemzetbiztonsági célzat"-on a külvilág számára megjelenő, és azonosítható módon az Nbtv. 1. §-ban taxatíve felsorolt nemzetbiztonsági szolgálatok (Információs Hivatal, AH, KNBSZ, NBSZ, Nemzeti Információs Központ) tevékenységét értem. Tehát nemzetbiztonsági célú az LI tevékenység, ha azt például az NBSZ az Nbtv. 8. § (1) bek. a) pontja szerinti feladat- és hatásköre alapján végzi, az Nbtv. 54. § j) pontja vagy 56. § d) – e) pontjai szerint eszközök, módszerek alkalmazása, végrehajtása során. Azonban tekintettel például az NBSZ „szolgáltatói" szerepkörére a „nemzetbiztonsági célzat" alaki meghatározása sem ilyen egyértelmű, hiszen figyelembe kell venni azt, hogy mely szervezet érdekkörében jár el, hajtja végre a titkos információgyűjtést (nemzetbiztonsági szolgálat vagy rendőrség, ügyészség, vámhatóság). Így az anyagi jog tartalmán túl alaki szempontból is megjelenik a bűnüldözési érdekkörben felmerülő nemzetbiztonsági célú tevékenység. Ezen kérdéskör mélyebb, részletes vizsgálatára az LI aspektusából a későbbek sor kerül.

Etimológiai értelmezés:

Etimológiai szempontból a hazai és nemzetközi szakirodalmat feldolgozó publikáció felhívja a figyelmet a nemzetbiztonsági szféra meghatározásának magyar problémájára, amely az elnevezés etimológiájából ered, nevezetesen a nemzet és a biztonság szavak összekapcsolásából, hiszen az alkalmazható „nemzeti biztonság" és „nemzetbiztonság" formában is, melyek eltérő jelentéstartalommal bírnak.[93] Az angolszász terminológiában *„egyértelműen elkülöníthető különbséget tesznek a „national security" [az állam biztonsági állapota] és az intelligence [nemzetbiztonsági funkció] fogalmak között. Ezzel szemben a magyarországi terminológiában mindkettő fogalmat kifejezik a nemzetbiztonság kifejezéssel,*

[93] DRUSZA Tamás (2021): A nemzetbiztonsági terület funkciói rendkívüli helyzetekben. In GAÁL Gyula – HAUTZINGER Zoltán (szerk.): *Rendészet a rendkívüli helyzetekben*. Pécs: MHTT. 144-145. Online: https://www.pecshor.hu/periodika/XXIII/drusza.pdf (Letöltés ideje: 2024. február 17.); SABJANICS István (2017): A Nemzetbiztonsági jogi koncepciója. In CSINK Lóránt (szerk.): *A nemzetbiztonság kihívásainak hatása a magánszférára*. Budapest: Pázmány Press. 103. Online: https://jak.ppke.hu/uploads/articles/1185528/file/Csink_maganszfera_TAN40.pdf (Letöltés ideje: 2024. február 19.)

ami komoly értelmezési zavarokhoz vezethet.[94] Tehát egyetértve a vizsgált szakirodalommal a biztonság, mint állapot nemzeti biztonságként, míg a funkció nemzetbiztonságként értelmezendő. Eszerint a nemzetbiztonság, mint állami funkciói elsődleges tartalma „*az adott ország lehető legszélesebb körű stratégiai cselekvési lehetőségei biztosításának támogatása titkos információk szisztematikus gyűjtésével és felhasználásával. […] A titkosszolgálatok így egyfajta generalista szerepet töltenek be az állami szervek között, azaz a társadalmi (szűkebb értelemben állami) működés bármely olyan területén tevékenykedhetnek, ahol szükség van a titkos információk révén történő stratégiai érdekérvényesítésre*."[95] A tevékenység, azaz funkció eredménye így pedig az aktuális és előre jelezhető eseményekből, változásokból adódó biztonsági kihívások és lehetőségek azonosítása.[96]

Uniós jogi értelmezés:

Az Európai Unió működéséről szóló szerződés[97] (a továbbiakban: EUMSZ) vizsgálata során megállapítható, hogy az uniós jogalkotó szintén az angolszász terminológiát alkalmazta (az eredeti angol nyelvű és a hivatalos magyar nyelvű fordítás szerint is), hiszen az EUMSZ 73. cikke az V. cím „*A szabadságon, a biztonságon és a jog érvényesülésén alapuló térség*" (a továbbiakban: SZBJT) című fejezet általános rendelkezési között – helyesen annak alanyi hatályával összhangban – a tagállamok bűnüldöző szervei (igazságügyi szervek, rendőrség, vámhatóságok) számára a „nemzeti biztonság", a „national secuirty" kapcsán határozza meg az együttműködés lehetőségét. Azonban a 2007. december 13-án aláírt Lisszaboni Szerződést elfogadó kormányközi konferencia zárónyilatkozatához csatolt 20. nyilatkozat a személyes adatok Unión belüli kezelése és a „nemzetbiztonság" kapcsolatában kimondja, „*hogy minden olyan esetben, amikor a [EUMSZ] 16. cikk alapján elfogadandó, a személyes adatok védelmére vonatkozó rendelkezéseknek a nemzetbiztonságot közvetlenül érintő vonatkozásuk van, a kérdés sajátos jellegére kellő figyelmet kell fordítani. A Konferencia emlékeztet arra, hogy a jelenleg alkalmazandó jogi szabályozás (lásd különösen a 95/46/EK irányelvet) különleges eltérésekről rendelkezik e tekintetben.*" Ez esetben a jogalkotó az eredeti angol nyelvű szövegben „national security" fogalmat használja, míg a magyar hivatalos fordítás a „nemzeti biztonság" helyett, a „nemzetbiztonság" terminológiát alkalmaz, tehát láthatóan nem egységes a fordítás, és a

[94] DRUSZA 2021: 146
[95] DRUSZA 2021: 147
[96] DOKMAN, Tomislav (2019): Defining the term "Intelligence" - insight into existing intelligence knowledge. *Informatologia*, 52(3-4), 199. Online: https://hrcak.srce.hr/file/341342 (Letöltés ideje: 2024. február 19.)
[97] Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata, OJ C 202, 7.6. 2016, 1–388.

tartalmi értelmezés során alkalmazott fogalomrendszer sem. Érdemes megjegyezni a fenti jogforrásban hivatkozott a 95/46/EK irányelvet[98] (amelyet idő közben felváltott és hatályon kívül helyezett a GDPR, mely elektronikus hírközlési tárgyi hatályú „végrehajtási" irányelve, a 2002/58/EK Elektronikus hírközlési adatvédelmi irányelv[99]). Az elektronikus hírközlési adatvédelmi irányelv „A [95/46] irányelv egyes rendelkezéseinek alkalmazása" című 15. cikk (1) bekezdésében az elektronikus hírközlési szolgáltatás keretében végbemenő személyes adatkezelés és annak korlátozhatósága kapcsán már magyarázza a fogalmat, mintegy harmadik „összemosott" értelmezési módot bevezetve, miszerint „*egy demokratikus társadalomban szükséges, megfelelő és arányos intézkedésnek minősül a nemzetbiztonság (vagyis az állam biztonsága), a nemzetvédelem és a közbiztonság védelme érdekében, valamint a bűncselekmények, illetve az elektronikus hírközlési rendszer jogosulatlan használata megelőzésének, kivizsgálásának, felderítésének és üldözésének a biztosítása érdekében*." Tehát a jogforrás a „nemzeti biztonság", „national security" statikus fogalomértelmezésétől eltérő módon az eddig funkcionalista szempontból értelmezett „nemzetbiztonság" fogalmat magyarázza az „állam biztonsága" statikus fogalommal. Azonban ez esetben is a „nemzeti biztonság"-ról rendelkezik a jogforrás, a helytelenül fordított „nemzetbiztonság" helyett, mivel a norma eredeti angol szövege a „national security (i.e. State security)" kifejezést alkalmazza az „állam biztonsága" helyes meghivatkozásával. A fenti rendelkezés egyébként meghivatkozásra került az EUB ítélkezési gyakorlatában is, például a C-140/20 számú Commissioner of An Garda Síochána ügyben hozott ítélet[100] során, mely tekintetében az EUB az ítélet 17. pontjában az ír jognak megfelelően a „safeguarding of the security of the State" fogalmat alkalmazza, melyet a magyar hivatalos fordítás „a nemzetbiztonság védelme" tevékenységként jelenít meg. A fenti ítélet a továbbiakban egyébként következetesen a fenti fogalomkörnek megfeleltetett „national security" fogalmat alkalmazza, míg a magyar nyelvű értelmezés a „nemzetbiztonság"-ot, az „állam biztonsága" fogalomnak feleltet meg helytelenül.

A GDPR hivatalos magyar fordítása már helyesen alkalmazza a „nemzetbiztonság" funkcionális fogalmát, annak például a (16) preambulumbekezdésében, mely alapján a hatálya

[98] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, OJ L 281, 23/11/1995, 0031 – 0050.

[99] Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv), OJ L 201, 31/07/2002, 0037 – 0047. (a továbbiakban: e-hírközlési irányelv)

[100] C-140/20. számú Commissioner of An Garda Síochána ügyben az Európai Unió Bírósága 2022. április 5-én hozott ítélete [ECLI:EU:C:2022:258]

alól kivonja a nemzetbiztonsági célú adatkezelést. A személyes adatok korlátozásának taxatív felsorolását tartalmazó 5. szakasz 23. cikk (1) bek. 1) pontjánál is megfelelően alkalmazza a „nemzetbiztonság" fogalmat a fordító. Azonban a GDPR angol nyelvű szövege a statikus „national security" fogalmat alkalmazza, ámde a magyar tartalmi interpretáció alapján a funkcionális jellegű „nemzetbiztonság" értelmezési kör érvényesül helyesen. A „national security" angol nyelvű fogalom használatát és annak magyar nyelvű interpretálását tovább bonyolítja az EUSZ fogalomhasználata, miszerint az EUSZ 4. preambulumcikk (2) bek. alapján a szerződés az uniós jog hatálya alól kivonja, és kizárólagos tagállami hatáskörbe delegálja a „nemzeti biztonság"-ot, melyet angol nyelven „national security"-ként nevesít a jogalkotó, ámde a tartalmi értelmezés során megállapítható, hogy ez esetben nem a statikus biztonsági megközelítés, hanem a funkcionális szemléletmódnak kellene érvényesülnie, hiszen „*Az Unió tiszteletben tartja […] az alapvető állami funkciókat, köztük az állam területi integritásának biztosítását, a közrend fenntartását és a nemzeti biztonság védelmét. Így különösen a nemzeti biztonság az egyes tagállamok kizárólagos feladata marad*."[101] Tehát az állami funkció expressis verbis megjelenítése okán a helyes tartalmi értelmezés alapján a „nemzetbiztonság" fordítás lenne a megfelelő fordulat. A fentiek alapján tehát megállapítható, hogy az uniós jog hazai értelmezése során a „nemzetbiztonság" fogalom alkalmazása nem egységes, nem konzekvens, összemosódik a „nemzet biztonsága" az „állam biztonsága" fogalmakkal, amely pedig a normaalkalmazás során kihívásként azonosítható.

Az alfejezet következtetéseként, a stratégiai evolúciós elemzés során láthatóvá vált, hogy a „nemzetbiztonsági érdek", így az abból absztrahálható „nemzetbiztonsági célzat" tartalma dinamikusan, a kor elvárásai mentén változik, alakul a hagyományos területektől elmozdulva a digitális kihívások (kibervédelem, űrtechnológia), vagy éppen a K+F+I (védelmi ipar, nemzetbiztonsági ipar, KNBSZ IKK, MiLab, InfoLab, TIF) irányába. Az Nbtv. tartalmi értelmezése körében megállapítható, hogy az AH és a KNBSZ vonatkozásában már az alapfeladataik tekintetében is megjelenik a bűnüldözési érdekkörben felmerülő nemzetbiztonsági célú tevékenység, amennyiben a Btk. szerinti tényállások, valamint a bírói engedélyezés alapján végzett Nbtv. 56. § szerinti titkos információgyűjtés kontextusából közelítjük meg a kérdést. Alaki szempontból a „nemzetbiztonsági érdek"-ből absztrahált „nemzetbiztonsági célzat"-on a külvilág számára megjelenő és azonosítható módon az Nbtv. 1. §-ban taxatíve felsorolt nemzetbiztonsági szolgálatok tevékenységét értem. Ez alapján tehát

[101] EUSZ. 4. preambulumcikk (2) bek.

nemzetbiztonsági célú az LI tevékenység, ha azt például az NBSZ az Nbtv. 8. § (1) bek. a) pontja szerinti feladat- és hatásköre alapján végzi. Azonban tekintettel például az NBSZ „szolgáltatói" szerepkörére a „nemzetbiztonsági célzat" alaki meghatározása nem ilyen egyértelmű, hiszen figyelembe kell venni azt, hogy mely szervezet érdekkörében jár el, hajtja végre a titkos információgyűjtést, nemzetbiztonsági szolgálat vagy rendőrség, ügyészség, adó- és vámhivatal vonatkozásában, így az anyagi jogi értelmezésen túl alaki szempontból is megjelenik a bűnüldözési érdekkörben felmerülő nemzetbiztonsági célú tevékenység. Továbbá megállapítható, hogy az uniós jog hazai értelmezése során a „nemzetbiztonság" fogalom alkalmazása nem egységes, nem konzekvens, összemosódik a „nemzet biztonsága" az „állam biztonsága" fogalmakkal, amely pedig a normaalkalmazás során kihívásként azonosítható. A fentiek alapján a „nemzetbiztonsági célzaton" a disszertációs kutatómunka során az alaki megjelenést és egyben a funkcionális értelmezést értem, azaz az Nbtv. szerinti nemzetbiztonsági szolgálat külvilág számára is megjelenő, érzékelhető cselekményeit. Így „bűnüldözési célzaton" pedig a büntetőeljárásról szóló 2017. évi C. törvény (a továbbiakban: Be.), az ügyészségről szóló 2011. évi CLXIII. törvény (a továbbiakban: Ütv.), az Rtv., és a Nemzeti Adó- és Vámhivatalról szóló 2010. évi CXXII. törvény (a továbbiakban: NAV tv.) hatálya alá tartozó feladatkörben eljáró szervezetek külvilág számára érzékelhető eljárási cselekményeit, a szervezetek funkcionális megjelenési formáját értem. A „nemzetbiztonsági célú" fogalomkör ennyire részletes elemzése azért volt indokolt és szükségszerű, mert az uniós jog megkülönbözteti és élesen elkülöníti az uniós jog hatálya alá nem tartozó nemzetbiztonsági célú és az uniós jog hatálya alá tartozó bűnüldözési célú (igazságügyi, rendőrségi, vámhatósági) tevékenységet, együttműködést.

2.2. Az LI szabályozásának nemzetközi és hazai keretrendszere

Az LI szabályozási keretinek vizsgálata során a tevékenységet alapvetően nemzetközi, uniós és nemzeti szintű jogforrások mentén indokolt vertikálisan elhatárolni.[102] A nemzetközi jogforrásoktól (pl. nemzetközi szerződések[103]) elkülöníthetőek a soft law körében értelmezett nemzetközi szabványok. Abban az esetben, ha az Unió szintjén vizsgáljuk a szabályozást megkülönböztethetőek az Európai Unió alapjait és működését meghatározó elsődleges jogi

[102] THOMPSON, Arron (2018): *Lawful Interception Basics*. Utimaco. 3. Online: https://slideplayer.com/slide/16142658/ (Letöltés ideje: 2024. február 20.)

[103] Az 1987. évi 12. törvényerejű rendelettel kihirdetett, a szerződések jogáról szóló, Bécsben 1969. évi május hó 23. napján kelt szerződés 2. cikk 1. bekezdés *a)* pontjában, továbbá a nemzetközi szerződésekkel kapcsolatos eljárásról szóló 2005. évi L. törvény 2. § *a)* pontjában foglalt fogalommeghatározás szerint.

aktusok, mint például az EUSZ, az EUMSZ, az Európai Unió Alapjogi Chartája[104] (a továbbiakban: Charta) stb., valamint a másodlagos uniós jogforrások, azaz a rendeletek, irányelvek, határozatok – ajánlások, vélemények –, valamint a Lisszaboni Szerződés hatálybalépését megelőző egyezmények[105].[106] Az EUSZ és az EUMSZ, valamint a tárgykört szabályozó másodlagos jogi aktusok hatálya alapján megállapítható, hogy a bűnüldözési, igazságügyi célú tevékenységtől (pl.: bűncselekmények megelőzése, nyomozása, felderítése, védeljárás) eltérően a nemzetbiztonsági célú tevékenység, így a nemzetbiztonsági célú LI a közösségi jog hatályán kívül eső tevékenység. A tagállamok míg a bel- és igazságügyi együttműködést szupranacionális szintre emelték[107], addig az EUSZ 4. cikk (2) bek. alapján a nemzetbiztonsági tevékenység nem tartozik az Alaptörvény E) cikk szerinti közösen gyakorolt hatáskörök közé, tehát az egyértelműen a nemzeti jog hatálya alá tartozik.[108] Tekintettel az LI alapvető jog korlátozó mivoltára szükséges kihangsúlyozni a személyes adatvédelmet biztosító uniós jogi aktusok és politikai törekvések jelentőségét, melyek releváns kérdései a későbbiekben indokolt mértékben kifejtésre kerülnek.

A nemzetközi normaalkotáson túlmutatóan szükséges kitérni a soft law témakörén belül a de facto (tényleges) és de jure (törvényes) szabványokra[109], szabványosításra, amely egyfajta nyilvános iránymutatást, kellően transzparens műszaki követelményrendszert határoz meg az elektronikus hírközlési szolgáltatók számára, például az LI alrendszer műszaki kialakítása tekintetében, vagy akár az elektronikus információ-, kibervédelem témakörében. Az LI végrehajtására jogosult szervezetek a szabványok alapján tudják specifikálni a szolgáltatók számára kötelezettségként támasztandó műszaki követelményrendszert, mely alkalmas a hírközlő hálózaton keletkező törvényi felhatalmazás és külső engedély alapján ellenőrizendő közlemények LI rendszerbe történő becsatornázására (monitoring alrendszer kialakítására), a

[104] Európai Unió Alapjogi Chartája (2012/C 326/02) OJ C 326, 26.10.2012, 391–407.
[105] „[…] az uniós jogi aktusok és a klasszikus kormányközi együttműködés jogi eszközei között helyezkedtek el." OSZTOVITS András (szerk.) (2011): *Az Európai Unió és az Európai Unió Működéséről szóló Szerződések magyarázata*. Budapest: Complex. 1515.
[106] SZABÓ Marcell (2022): Az Európai Unió jogrendszere. In SZABÓ Marcell – GYENEI Laura – LÁNCOS Petra Lea – PÜNKÖSTY András (szerk.): *Az Európai Unió jogának alapjai*. Budapest: Pázmány Press. 97-122.
[107] Lásd: EUMSZ V. Cikk A szabadságon, a biztonságon és a jog érvényesülésén alapuló térség
[108] BUZÁS Péter - PÉTERFALVI Attila - RÉVÉSZ Balázs (szerk.) (2021): *Magyarázat a GDPR-ról*. Budapest: Wolters Kluwer. 13.
[109] „A szabvány elismert szervezet által alkotott vagy jóváhagyott, közmegegyezéssel elfogadott olyan műszaki (technikai) dokumentum, amely tevékenységre vagy azok eredményére vonatkozik, és olyan általános és ismételten alkalmazható szabályokat, útmutatókat vagy jellemzőket tartalmaz, amelyek alkalmazásával a rendező hatás az adott feltételek között a legkedvezőbb." 1995. évi XXVIII. törvény a nemzeti szabványosításról 4. § (1). bek. A hazai szabályozás leképezi a szabvány ISO/IEC DIR 2:2016 3.1.2. szerinti fogalmát. Online: https://www.iec.ch/members_experts/refdocs/iec/isoiecdir-2%7Bed7.0%7Den.pdf (Letöltés ideje: 2024. július 7.)

tartalom megismerésére, a kísérő és metaadatokhoz való hozzáférésre. Az egyes fogalmak, mint például az elektronikus hírközlési szolgálató, monitoring alrendszer, közlemény, kísérő- és metaadat stb. a hatályos uniós és nemzeti normák, további szakirodalom alapján kerül értelmezésre. Az egyes nemzetközi szabványokat a szabványügyi testületek alkotják, melyek közül az elektronikus hírközlés tekintetében kiemelendő a 3GPP[110] és az ETSI[111]. Az LI-vel kapcsolatos szabványok a későbbiekben kerülnek az indokolt mértékben bemutatásra.

Az LI nemzeti szintű normái tekintetében elkülönülnek a jogszabályok (pl. törvény[112], kormányrendelet[113], kormány tagjának rendelete), a közjogi szervezetszabályzó eszközök (pl. nyilvános, nem nyilvános, titkos kormány határozatok, miniszteri és szervezeti utasítások), valamint a szerveztek közötti együttműködési megállapodások. Az Alaptörvénynél eggyel alacsonyabb hierarchia fokon állnak a törvények, melyek közül a nemzetbiztonsági, vagy a bűnüldözési, igazságügyi célú LI általános jogforrásait, és az egyes érintett ágazatok (pl. elektronikus hírközlés, egyes információs társadalommal összefüggő szolgáltatások) LI-vel kapcsolatos speciális ágazati normáit külön törvények szabályozzák. Az LI végrehajtásával kapcsolatos alacsonyabb szintű rendelkezéseket, részletszabályokat rendszerint kormányrendeletek, a miniszteri rendeletek hivatottak rendezni. A tevékenység szakági jogi szabályozásán túl, tekintettel annak alapvető jog korlátozással járó mivoltára szükséges és indokolt megemlíteni az adatvédelemmel kapcsolatos nemzeti normák, kontroll mechanizmusok jelentőségét is. Az LI-vel kapcsolatos hazai jogszabályi környezet az értekezés során a későbbiekben kerül kifejtésre. Adott rendelkezés azért kerülhet törvénybe, mert alapvető jogot vagy kötelezettséget érint (rendre megállapít, korlátoz), vagy az Országgyűlés kizárólagos jogalkotási tárgykörébe tartozik. Minden, ami nem tartozik az előző két meghatározás szerinti keretbe alacsonyabb szintre kerülhet azzal, hogy törvényi felhatalmazás (keretrendelkezés) mellett alapvető jogot vagy kötelezettséget érintő tárgykörben is megvalósulhat a normaalkotás. Ezek szükségképpen nyilvánosan hozzáférhetőek, mindenki számára megismerhető jogforrások lesznek (pl. kormányrendelet, kormánytag rendelete). Ami ennél is alacsonyabb és a megismerhetősége valamilyen oknál fogva korlátozott, alapvető jogot

[110] 3rd Generation Partnership Project – 3. Generációs Együttműködési Projekt
[111] European Telecommunications Standards Institute - Európai Távközlési Szabványügyi Intézet
[112] Lásd: 2003. évi C. törvény az elektronikus hírközlésről 92. §; Ekertv. 3/B §; 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 2. § (3) bek. - a későbbiekben kifejtve
[113] Lásd: 180/2004. (V.26.) Korm. rendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről; 185/2016. (VII.13.) Korm. rendelet a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről - a későbbiekben kifejtve

érintően korlátozó rendelkezést nem tartalmazhat, de hatáskört vagy illetékességet megállapító, vagy együttműködési kötelezettséget megállapító rendelkezést minden további nélkül.

Az egyes közjogi szervezetszabályozó eszközök meghatározzák az LI szervezeti szintű végrehajtásának rendjét, elkülönítik a jogosult szervezeteken belüli hatásköri/illetékességi kérdéseket, például szervezeti és működési szabályzatok, egyéb az LI tevékenységet részeletesen szabályzó belső normatív utasítások keretében. Az együttműködési megállapodások jogszabályon, rendszerint kormányrendeleteken alapuló kötelezettségek, amelyek az LI-re és annak végrehajtására jogosult szerv, valamint az érintett szolgáltató közötti együttműködés rendjét, a tényleges végrehajtással kapcsolatos feladatokat, kötelezettségeket, műszaki követelményeket stb. hivatottak rögzíteni. Rendszerint a közjogi szervezetszabályzó eszközök, együttműködési megállapodások olyan minősítéssel védhető közérdek körébe tartozó adatokat tartalmaznak, amelyek a minősített adat védelméről szóló 2009. évi CLV. törvény (a továbbiakban: Mavtv.) 3. § (1) a) pontja szerinti nemzeti minősített adatok körébe tartoznak, így ezek vizsgálata nem tárgya az értekezésnek.

2.3. Az LI alapvető jogi és adatvédelmi garanciáinak áttekintése a nemzetközi és hazai jogban

Mint az a témaválasztás indoklása során levezetésre került a titkos információgyűjtés, így annak résztevekénységeként az LI végsősoron egyfajta jogszerű alapvető jog korlátozó eszköz, valamely konkuráló érdek, például a biztonság garantálása érdekében, mely alkalmazását, végrehajtását és annak mélységét, azaz az alapvető jog korlátozásának mértékét a nemzetközi normákban lefektetett, és a nemzeti, tagállami jogrendszerekben alaptörvényi, törvényi szinten meghatározott demokratikus alapelvek szabályozzák. Jelen alfejezet ezen normatív garanciarendszert hivatott áttekinteni, és annak a hazai jogforrásokban való megfelelősségét értékelni Alaptörvényi szintig, továbbá a fentiek okán vizsgálat tárgyát fogja képezni a nemzetbiztonsági célú LI személyes adatvédelmi garanciáinak áttekintése az uniós és hazai jogban.

2.3.1. Az LI alapvető jogi garanciáinak áttekintése

Álláspontom alapján a törvényi szinten szabályozott titkos információgyűjtés, így az LI eszközrendszerének alkalmazását az állam által végrehajtott nem abszolút jellegű alapvető

jog[114] jogszerű korlátozásaként indokolt értelmezni. Ezen jogok esetében az állam kötelezettsége negatív tartalmú, azaz a közhatalom részéről főként be nem avatkozást igényel, illetve a jogszerű beavatkozás csak egyedi és korlátozott – szükséges és arányos – módját teszi lehetővé. Tekintettel arra, hogy az emberi és alapvető jogok általánosan érvényesülő alapelvei a nemzetközi jog által szabályozottak, ezért az állami szintű korlátozás, illetve az egyes olyan előkérdések, mint például, hogy milyen módon és milyen mértékig igazolható a korlátozás, illetve mik a korlátozás korlátjai[115], komplex, tudományos szemléletű vizsgálatához indokolt a nemzetközi közjogi kitekintés.[116] Alapjogi kritériumok vizsgálatánál szükséges az azokat és azok korlátozhatóságát deklaráló, Magyarország vonatkozásában is hatályos elsődleges nemzetközi jogforrások, nemzetközi szerződések vonatkozó rendelkezéseinek rövid áttekintése, valamint az Alaptörvény ezekhez való viszonyának megállapítása.

Az alapjogok szükségképpen konfliktusba kerülhetnek, konkurálhatnak egymással, illetve más alkotmányos értékekkel, érdekekkel és célokkal, például a nemzetbiztonsági érdek konkurálhat a nemzetbiztonsági érdeket sértő egyén magánéletének tiszteletben tartásához, magán-, levéltitokhoz és a személyes adatainak védelméhez fűződő alapvető jogaival, amelyeket a jogalkotónak vagy a jogalkalmazóknak kell feloldania. Az emberi és alapvető jogokat tartalmazó nemzetközi egyezmények megfogalmazzák, hogy milyen módon és milyen mértékben lehetséges az alapvető jogok korlátozása.

---

[114] A nemzetközi jog tudománya az elsődleges emberi jogi dokumentumok alapján az emberi és alapvető jogokat a korlátozás lehetősége és feltételei alapján az alábbi fő kategóriákra osztja:

- abszolút korlátozhatatlan és elidegeníthetetlen emberi jogok – például az élethez és emberi méltósághoz való jog;
- időlegesen felfüggeszthető, illetve korlátozható alapvető jogok – például különleges jogrend idején a gyülekezési szabadság;
- állandó jelleggel korlátozható alapvető jogok – olyan polgári és politikai jogok, melyek állandó jelleggel, de meghatározott feltételek mellett törvényi korlátozás alá vehetők.

Lásd: BALOGH Zsolt (2011): Alapjogok korlátozása az új alkotmányban. *Pázmány Law Working Papers,* 2(19), 1-10. Online: https://plwp.eu/docs/wp/2012/2011-19.pdf (Letöltés ideje: 2024. július 7.); BOKORNÉ SZEGŐ Hanna (1995): Az emberi jogokról való időleges eltérés, illetve az emberi jogok állandó jellegű törvényes korlátozása. *Acta Humana*, (18-19), 24-39.

[115] HALMAI Gábor - TÓTH Gábor Attila (2023): Az emberi jogok korlátozása. In HALMAi Gábor - TÓTH Gábor Attila (szerk.): *Emberi jogok*. Budapest: Osiris Kiadó. 108-109. Online: https://www.academia.edu/43016928/Emberi_jogok_Human_Rights_ (Letöltés ideje: 2024. február 20.)

[116] Lényegesek a nemzetközi jogi szempontok, mert ezek kötelezik az államot – erga omnes és jus cogens normák, vagy szerződéses kötelezettségben jelentkező alávetésként – ugyanakkor az alapjogok korlátozására egy sor olyan konkrét eljárási szabály is kihat, amelyet nem érint közvetlenül a nemzetközi jog, pl. jogforrási hierarchia, jogalkotás folyamata, jogszabályok formai kellékei - amelyek az alapjogok korlátozása szempontjából mégis igencsak meghatározók.

Az ENSZ Közgyűlése által 1948. december 10-én elfogadott Emberi Jogok Egyetemes Nyilatkozatának (a továbbiakban: EJENY) 3. cikke kimondja, hogy „*Minden személynek joga van az élethez, a szabadsághoz és a személyi biztonsághoz*.", továbbá a 12. cikk rendelkezik arról, hogy „*Senkinek magánéletébe, családi ügyeibe, lakóhelye megválasztásába vagy levelezésébe nem szabad önkényesen beavatkozni, sem pedig becsületében vagy jó hírnevében megsérteni. Minden személynek joga van az ilyen beavatkozásokkal vagy sértésekkel szemben a törvény védelméhez*." Az Európa Tanács által 1950. november 4-én Rómában elfogadott Emberi Jogok Európai Egyezményének (a továbbiakban: EJEE[117]) 5. cikke rendelkezik a szabadsághoz és biztonsághoz való jogról, a 8. cikk (1) bek. pedig kimondja, hogy „*Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák*." Az EJEE 8. cikk (2) bek. pedig rendelkezik az (1) bek. rendelkezésének korlátozhatóságáról, miszerint „*E jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság […] érdekében, […] avagy mások jogainak és szabadságainak védelme érdekében szükséges.*" A Charta 6. cikke rendelkezik a szabadsághoz és biztonsághoz való jogról, a 7. cikke a magán- és a családi élet tiszteletben tartásáról, a 8. cikke a személyes adatok védelméről, amely (2) bek. kimondja, hogy „*Az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni*." Az EUSZ 6. cikk (1) bek. kimondja, hogy az EU elismeri a Charta rendelkezéseit, valamint azt primer EU-s jogforrássá emeli, a (2) bek. pedig kimondja, hogy az EU csatlakozik az EJEE-hez – amelyre azonban a EUB 2/13. számú véleménye[118] alapján nem került sor. Magyarország törvényben kihirdetett módon csatlakozott mind az EJENY-hez, EJEE-hez és a Chartához, így azok rendelkezéseit kötelezően alkalmazandónak tartja magára nézve. A fentiek alapján a korlátozására irányuló, a jogbiztonság elvéből levezethető általános formai követelmény a törvényi szabályozás szükségessége, így annak transzparens törvényi szintű jogforrásban való érvényesítése, amellyel párhuzamosan egyben tartalmi követelményként arányossági mérce is megjelenik.[119]

[117] Magyarország tekintetében az EJEE az emberi jogok és az alapvető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt Egyezmény és az ahhoz tartozó nyolc kiegészítő jegyzőkönyv kihirdetéséről szóló 1993. évi XXXI. törvény alapján 1991. november 05-től hatályos.

[118] 2/13. sz. EUB vélemény [ECLI:EU:C:2014:2454.]

[119] GÁRDOS-OROSZ Fruzsina (2020): Az alapjogok korlátozása. In JAKAB András – KÖNCZÖL Miklós – MENYHÁRD Attila – SULYOK Gábor (szerk.): *Internetes Jogtudományi Enciklopédia.* Budapest: ORAC Kiadó. 7. Online: https://ijoten.hu/uploads/az-alapjogok-korlatozasa.pdf (Letöltés ideje: 2024. február 14.)

A formai követelmények érvényesítése mellett szükség van az alapvető jogot érintő normák tartalmi vizsgálatára is, amelyek segítségével megítélhető, hogy a korlátozás célja és mértéke alkotmányosnak tekinthető-e vagy sem. A mérce, azaz az általános teszt klauzula *arányossági teszt*[120] elnevezéssel szerepel az emberi jogok szakirodalmában. Ennek keretében vizsgálandó, hogy az alkalmazott korlátozásnak van-e jogszerű célja, majd, hogy az adott kérdésben a korlátozás eszközei arányosak-e a jogszerűen követett céllal, továbbá, hogy fennáll-e olyan nyomós társadalmi indok, amely feltétlenül megköveteli a jogkorlátozást.[121] Az Alaptörvény I. cikk (3) bek. átemelte a magyar alkotmánybírósági teszt legalapvetőbb követelményeit a Charta 52. Cikk (1) bek. generálklauzulájából: „*Az e Chartában elismert jogok és szabadságok gyakorlása csak a törvény által, és e jogok lényeges tartalmának tiszteletben tartásával korlátozható. Az arányosság elvére figyelemmel, korlátozásukra csak akkor és annyiban kerülhet sor, ha és amennyiben az elengedhetetlen és ténylegesen az Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja*."

Az Alaptörvény E) cikk rendelkezik a magyar jogrend és uniós jog viszonyáról, míg az Alaptörvény Q) cikk a magyar jogrend és a nemzetközi jog viszonyáról, továbbá az Alaptörvény I. cikk (1) – (2) bek. rendelkezik az ember sérthetetlen és elidegeníthetetlen alapvető jogainak tiszteletben tartásáról, valamint, hogy „*Magyarország elismeri az ember alapvető egyéni és közösségi jogait*". Míg az I. cikk (3) bek. kimondja, hogy „*Alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható*." Ezen alapelvek betartása nélkülözhetetlen a jogkorlátozás és a más alapvető jog védelme közötti egyensúly fenntartása érdekében, hiszen titkos információgyűjtés egy aszimmetrikus, egyensúly nélküli viszony, mivel az nem ismert az érintett előtt. Ebből következik, hogy az érintett csak korlátozottan képes az érdekei érvényesítésére, „*így a jogvédelmet és a megfelelő egyensúlyt közvetetten, más, az állam által beépített hatékony garanciákkal, megfelelő kontrollmechanizmusok kiépítésével kell biztosítani*."[122]

---

[120] POZSÁR-SZENTMIKLÓSY Zoltán (2014): Az alapjogi teszt újrafogalmazása. *Jogtudományi Közlöny*, 69(1), 23-34. Online: https://real.mtak.hu/108751/1/jk1401_3.pdf (Letöltés ideje: 2024. február 14.)

[121] KISS Barnabás (2010): Az alapjogok korlátozása az Európai Unió nemzeti alkotmányaiban. *Acta Universitatis Szegediensis: acta juridica et politica*, 54(1), 458. Online: https://acta.bibl.u-szeged.hu/7457/1/juridpol_073_455-465.pdf (Letöltés ideje: 2023. november 08.)

[122] HETESY Zsolt (2011): *A titkos felderítés*. Doktori (PhD) értekezés. Pécs: PTE ÁJKDI. 5–6. Online: https://pea.lib.pte.hu/bitstream/handle/pea/15668/hetesy-zsolt-phd-2012.pdf?sequence=1&isAllowed=y Letöltés ideje: 2023. november 08.)

Tehát a részfejezet következtetéseként megállapítható, hogy Magyarország az Alaptörvény alapján tiszteletben tartja az ember sérthetetlen és elidegeníthetetlen alapvető jogait és ezeket titkos információgyűjtés, illetve annak résztevékenységeként nemzetbiztonsági célú LI során csak más – például a nemzetbiztonság – alkotmányos közérdek érvényesülése érdekében, szükséges és arányos módon korlátozhatja. Ennek adnak törvényi szintű keretet a titkos információgyűjtés engedélyezésére, végrehajtására és ellenőrzésére vonatkozó hazai jogszabályok transzparens garanciái és kontrollmechanizmusai. Így különösen az Nbtv. és a Be., valamint az Ütv., az Rtv. és a NAV tv. rendelkezései, például az alapvető jog beavatkozásának mértéke függvényében szükséges előzetes engedélyezési eljárás (külső/ belső; ügyészi/ bírói/ igazságügyi miniszteri), közbenső kontroll (szervezeti), és az utólagos független ellenőrzés (törvényességi felügyelet, adatvédelmi hatóság) tekintetben, melyek a 2.5.2. részfejezetben kerülnek a szükséges mértékben ismertetésre.

2.3.2. A nemzetbiztonsági célú LI személyes adatvédelmi garanciáinak áttekintése

A titkos információgyűjtés általános adatvédelmi garanciális szabályainak vizsgálatát követően indokolt a jogszabályi elemzés elvégzése kifejezetten az elektronikus hírközlés, kommunikáció során megjelenő személyes adatkezeléssel és annak LI jellegű korlátozásával kapcsolatos különös szabályok terén, tekintettel arra, hogy a személyes adatok védelméhez fűződő jog, és az információs önrendelkezési jog is sérülhet a titkos információgyűjtés, így az LI során. Az EU adatvédelmi reformját követően a GDPR (16) preambulumbekezdése, valamint a 2. cikk (2) bek. a) pontja szerint, az EUMSZ 4. preambulumcikk (1) – (2) bek. alapján a rendelet tárgyi hatálya ugyan nem terjed ki nemzetbiztonsági és honvédelmi célú adatkezelésre, a bűnüldözési célú adatkezelést pedig a bűnügyi irányelv[123] hivatott szabályozni, ennek ellenére a GDPR 23. cikk (1) bek. alapján a fenti alapvető jogok olyan általános közérdekű célkitűzések okán, mint például a nemzetbiztonsági, honvédelmi, közbiztonsági és bűnüldözési érdek, szükséges és arányos módon korlátozhatók, amennyiben a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát.

[123] Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 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 (bűnügyi irányelv), OJ L 119, 4.5.2016, 89–131.

Uniós szinten a személyes adatok elektronikus hírközlési ágazatban való kezelése területén a magánélet tiszteletben tartását és a személyes adatok védelmét a 95/46/EK irányelvhez és a GDPR-hoz képest különös módon az e-hírközlési adatvédelmi irányelv hivatott szabályozni[124]. Ezen jogforrás 15. cikk (1) bek. szerint a hírközlési tevékenységgel kapcsolatos alapvető jogokat a GDPR 23. cikk (1) bek. szerint a tagállamok jogszabályi intézkedésekkel korlátozhatják, tekintettel a Charta 52. cikkének (1) és az EUMSZ 16. cikkének (1) bekezdéseire, amennyiben az „*egy demokratikus társadalomban szükséges, megfelelő és arányos intézkedésnek minősül a nemzetbiztonság (vagyis az állam biztonsága), a nemzetvédelem és a közbiztonság védelme érdekében, valamint a bűncselekmények […] megelőzésének, kivizsgálásának, felderítésének és üldözésének a biztosítása érdekében*." A személyes adatok védelmének az e-hírközlési adatvédelmi irányelv 15. cikk (1) bek. szerinti korlátozhatósága tekintetében számos EUB ítélet[125] is született, mely alakítja az uniós jogot, és jogalkalmazást. A Bizottság 2017. január 10-én előterjesztette[126] ezen irányelvnek a magánéletről és az elektronikus hírközlésről szóló rendelettel való felváltására irányuló javaslatát[127] (a továbbiakban: e-hírközlési adatvédelmi rendelet javaslat), mely azonban a mai napig nem került elfogadásra, viszont tartalmi értelmezése és kontextusba helyezése az értekezés tárgyával indokolt. Az e-hírközlési adatvédelmi rendelet javaslat 11. cikke tárgyalja a hatálya alá tartozó tevékenység végzése során történő személyes adatok védelmének korlátozhatóságát, mely körben megjelenik ugyancsak a nemzetbiztonsági és a bűnüldözési közérdek, melyet szintén kimond a (26) preambulumbekezdés, a szükségesség és arányosság követelményeinek való megfelelés, valamint az EUB és az EJEB Chartával és EJENY-nyel való jogértelmezési összhangjának kikötésével. A rendelet javaslat (15) preambulumbekezdése kimondja, hogy az elektronikus hírközlési adatok bizalmasan kezelendők, hiszen a (2) preambulumbekezdés szerint „*Az elektronikus hírközlés tartalma rendkívül bizalmas adatokat*

[124] Fontos megjegyezni, hogy az elektronikus hírközlési adatvédelmi irányelv 2017. január 11-e óta az Európai Bizottság rendeleti szintű jogalkotási javaslatnak előterjesztése alapján felülvizsgálat alatt van, amely tartalmával kapcsolatban az Európai Parlament és Tanács továbbra is eltérő álláspont képvisel, így „az új jogi aktus hatálybalépésének és alkalmazandóvá válásának időpontja nem határozható meg." (BUZÁS - PÉTERFALVI - RÉVÉSZ 2022: 11)

[125] Lásd: C-207/16 számú Ministerio Fiscal ügyben az Európai Unió Bírósága 2018. október 2-án hozott ítélete [ECLI:EU:C:2018:788]; C-623/17 számú Privacy International ügyben az Európai Unió Bírósága által 2020. október 6-án hozott ítélete [ECLI:EU:C:2020:790[; C-511/18, C-512/18 és C-520/18. számú La Quadrature du Net és társai ügyében az Európai Unió Bírásaga által hozott ítélet [ECLI:EU:C:2020:79]

[126] *Tematikus tájékoztató – A személyes adatok védelme*. Európai Unió Bírósága, 2021. 2. Online: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_hu.pdf (Letöltés ideje: 2024. február 14.)

[127] Javaslat az Európai Parlament és a Tanács rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet), COM/2017/010 final - 2017/03 (COD). Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A52017PC0010 (Letöltés ideje: 2024. február 14.)

tárhat fel a kommunikációban részt vevő végfelhasználókról", amelyek a személyes és különleges személyes adatok körébe tartoznak, melyet magyaráz is a javaslat szövege.

Az Alkotmánybíróság 13/2001. (V. 14.) AB határozatában kimondja, hogy a *„nemzetbiztonsági érdekek védelme alkotmányos cél és állami kötelezettség*".[128] Ezen megállapításból levezetve, valamint a vizsgált szakirodalom alapján megállapítható, hogy a nemzetbiztonsági célú titkos információgyűjtés legitim, alkotmányosan elfogadott adatkezelési cél, az ezt szabályozó törvénynek összhangban kell lennie az alapvető jog korlátozásának az Alaptörvényben, és a nemzetközi jogforrásokban meghatározott feltételrendszerrel.[129] Törvényi szinten összhangban az EUSZ, a GDPR és az Alaptörvény vonatkozó rendelkezéseivel a nemzetbiztonsági és bűnüldözési célú adatkezelés általános szabályozását a 2013. augusztus 01-én – részben[130] – hatályba lépett az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) szabályozza. Az Infotv. 2. § (3) bek. alapján a személyes adatok bűnüldözési, nemzetbiztonsági és honvédelmi célú kezelésére az Infotv.-t kell alkalmazni, mely különös szabályairól a nemzetbiztonsági célú adatkezelés vonatkozásában az Nbtv. is rendelkezik. Az Infotv. 3. §-a szerinti értelmező rendelkezésének 10b. pontjában meghatározza a nemzetbiztonsági célú adatkezelés, továbbá a 10a. pontjában a bűnüldözési célú adatkezelés fogalmát. Az Infotv. jogértelmezése alapján tehát a nemzetbiztonsági célú adatkezelést szintén funkcionálisan közelíti meg a nemzetbiztonsági szolgálatok tekintetében az Nbtv. hatálya alá tartozó adatkezelésük vonatkozásban, azonban azt kiegészíti az Rtv. és a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól szóló 295/2010. (XII. 22.) Korm. rendelet (a továbbiakban: TEK Korm. rendelet) által szabályozott Terrorelhárítási Központ (a továbbiakban: TEK) Nbtv. hatálya alá tartozó adatkezelésével is. Azonban ezzel további feszültséget teremt – vagy az adatkezelés körében éppen, hogy oldva azt – az értekezés 2.1. alfejezetben kikötött alaki jellegű „nemzetbiztonsági cél" és a „bűnüldözési cél" értelmezése, elhatárolása során, mely utóbbit a törvény absztrakciós szinten is definiál. Ezen megközelítésből levezethető a „nemzetbiztonság" angolszász fogalomhasználatán túl (statikus, funkcionális) a „nemzetbiztonsági célzat" adatkezelés szempontú meghatározása egyfajta negatív fogalmi definiálással, mégpedig ami nem tartozik

[128] 13/2001. (V. 14.) AB határozat. Online: https://njt.hu/jogszabaly/2001-13-30-75 (Letöltés ideje: 2024. február 14.)

[129] PÉTEFALVI Attila (2013): A nemzetbiztonsági ellenőrzés új szabályairól. *Acta Humana*, 1(1), 52. Online: https://real.mtak.hu/122840/1/AH_2013_1_Peterfalvi_Attila.pdf (Letöltés ideje: 2024. február 14.)

[130] Az Alkotmánybíróság a 19/2013. (VII. 19.) AB határozata a módosításnak a nemzetbiztonsági ellenőrzésre vonatkozó egyes részeinek hatálybalépését felfüggesztette. Lásd: PÉTERFALVI 2013.

az Infotv. 3.§ 10a. pontja szerinti bűnüldözési célú adatkezelés fogalma alá, az nemzetbiztonsági célú adatkezelés a 3.§ 10.b. pont viszonylatában.

2.4. Az EU digitális piaci és adatvédelmi stratégiai célkitűzéseinek tendenciái

Már 2015-től az Európai digitális egységes piaci stratégia[131] alkotása során megjelent az e-hírközlési adatvédelmi irányelv felülvizsgálatának jogalkotói szándéka, amely kicsúcsosodását a 2017-ben előterjesztett e-hírközlési adatvédelmi rendelet javaslat jelenti, melyről a jogalkotás keretében szóló viták a mai napig folynak. A Bizottság 2018-ban kiadta a „Digitális egységes piac: Politikai megállapodás az 5G korszak távközlési piacait alakító szabályokról" című dokumentumát, amelyben megfogalmazta, hogy stratégiai célkitűzései mentén a távközlési piacot (értsd szűken: elektronikus hírközlési piac) érintő javaslataival törekszik, hogy az EU 2025-ig az internetkapcsolat élvonalába kerüljön egy „Gigabites társadalom"[132] létrehozása érdekében. A Bizottság becslése szerint a célok eléréséhez 500 milliárd eurós beruházásra lesz szükség az elkövetkező évtizedben, amely nagy része a mikrogazdaságból származik majd, azonban az akkori hírközlési trendek mellett valószínűsítette, hogy ezen felül további 155 milliárd euró finanszírozási igény várható. A Bizottság állásfoglalása szerint a hírközlési szabályoknak támogatniuk kell a „Gigabites társadalom" létrehozását, azáltal, hogy a rendkívül nagy kapacitású hálózatokba[133] (például 5G) történő befektetést kötelező célkitűzéssé teszik, és az új, nagyon nagy kapacitású hálózatok kiépítésének elősegítésére összpontosítanak, mivel az új szabályok elősegítik a fenntartható hosszú távú versenyt.[134] Az Európai Parlament és a Tanács 2018. június 5-én politikai megállapodásra jutott az EU elektronikus hírközlési szabályainak frissítéséről, amely keretében elfogadták a Bizottság által javasolt új Európai Elektronikus Hírközlési Kódex[135] (a továbbiakban: Hírközlési Kódex) megalkotását, mely célja, hogy fellendítse a rendkívül nagy kapacitású hálózatokba történő beruházásokat az EU-ban, beleértve a kevésbé urbanizált földrajzi területeket is. Aktuálisan is zajlik a nagy sebességű hálózatok EU-szerte történő gyorsabb kiépítéséről szóló szabályozási folyamat, mely kapcsán

[131] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Európai digitális egységes piaci stratégia, COM(2015) 192 final. (Európai adatstratégia). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52020DC0066 (Letöltés ideje: 2024. február 14.)

[132] Értsd: fejlett információs társadalom, melyben általánosan állnak rendelkezésre a nagykapacitású hálózatok, mint például az 5G (Később részletezve.)

[133] Lásd: Hírközlési Kódex 2. cikk 4. pont.

[134] *Digital Single Market: Political agreement on the rules shaping the telecommunication markets in the 5G era.*

[135] Az Európai Parlament és a Tanács (EU) 2018/1972 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáró. OJ L 321, 17.12.2018, 36–214.

Petra de Sutter belga miniszterelnök-helyettes megjegyezte: „*Európában sokkal egyszerűbb lehetne az optikai és az 5G-hálózatok kiépítése, ha kevesebb adminisztrációval járna*."[136] Andrus Ansip, a Bizottság digitális egységes piacért felelős alelnöke kijelentette: "*Ez a megállapodás elengedhetetlen az európaiak növekvő csatlakozási igényeinek kielégítéséhez és Európa versenyképességének fokozásához. Lefektetjük az 5G európai kiépítésének alapjait*." Mariya Gabriel, a digitális gazdaságért és társadalomért felelős biztos így nyilatkozott: "*Az új távközlési szabályok Európa digitális jövőjének alapvető építőkövei.*"[137] A Hírközlési Kódex irányelv tagállami átültetésének határideje 2020. december 21-e volt, melyet az NMHH közleménye szerint Magyarország 2020. júliusáig bezárólag szinte elsőként hajtotta végre az Unióban, elsősorban az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban: Eht.)[138] és kilenc NMHH rendelet módosításával, további 13 új NMHH rendelet kiadásával.[139] A Hírközlési Kódex aktualizálja és egyesíti az uniós elektronikus hírközlési szabályokat egyetlen olyan szabályozási keretben, amelynek célja az összekapcsoltság, azaz a konnektivitás és konvergencia növelése, valamint a felhasználók adatvédelmi környezetének javítása[140] Európa-szerte. Az egyetemes szolgáltatások tekintetében az európai elektronikus hírközlési szabályok célja, hogy a hatékony verseny révén Európa-szerte megfizethetővé és elérhetővé tegyék a szélessávú internet-hozzáférést és a hangkommunikációt – mely hatásai tekintetében az értekezés tárgyát képező alkalmazásszolgáltatások LI-je aspektusából vizsgálandó szakpolitikai törekvés.[141]

Az Európai Tanács 2020. július 9-én következtetéseket fogadott Európa digitális jövőjének alakításáról, amely fő területei a konnektivitás, a digitális értékláncok, az adatgazdaság, a mesterséges intelligencia, valamint az online/digitális platformok, ebben továbbá kifejti, hogy

---

[136] *A gigabites infrastruktúráról szóló jogszabály: a Tanács és a Parlament megállapodott a nagy sebességű hálózatok EU-szerte történő gyorsabb kiépítéséről*. EU Tanácsa. 2024. február 06. Online: https://www.consilium.europa.eu/hu/press/press-releases/2024/02/06/gigabit-infrastructure-act-council-and-parliament-strike-a-deal-for-faster-deployment-of-high-speed-networks-in-the-eu/ (Letöltés ideje: 2024. február 14.)

[137] *Digital Single Market: EU negotiators reach a political agreement to update the EU's telecoms rules*. Európai Bizottság. 2018. Online: https://ec.europa.eu/commission/presscorner/detail/hu/IP_18_4070 (Letöltés ideje: 2024. február 17.)

[138] Például az Eht. 126/A1. § szerinti különleges hírközlési szolgáltatások, azaz a számfüggetlen személyközi hírközlési (NI-ICS) és az M2M szolgáltatásokra irányuló különös törvényi szabályok átültetésével.

[139] *Teljessé vált az Európai elektronikus hírközlési kódex magyarországi átültetése.* NMHH. 2021. Online: https://nmhh.hu/cikk/216959/Teljesse_valt_az_Europai_elektronikus_hirkozlesi_kodex_magyarorszagi_atultetese (Letöltés ideje: 2024. február 18.)

[140] Lásd: KOVÁCS Anita (2019): A végfelhasználók jogai az új Európai Elektronikus Hírközlési Kódexben. *Híradástechnika*, 74(1), 44-48. Online: https://www.hiradastechnika.hu/documents/4743302/0/HT_2019_Infokom2018.pdf (Letöltés ideje: 2024. február 21.)

[141] *EU Elektronikus Hírközlési Kódex. Európai Bizottság*. 2020. Online: https://digital-strategy.ec.europa.eu/hu/policies/eu-electronic-communications-code (Letöltés ideje: 2024. február 18.)

„*a digitális transzformáció kulcsszerepet fog játszani a pandémia elleni küzdelemben és a Covid19 válságot követő helyreállításban”*.[142] A Tanács 2022. december 08-án elfogadta Digitális évtized 2030 szakpolitikai programot, amely célkitűzéseinek megvalósításához 2030-ra 100%-os biztonságos 5G lefedettséget határoz meg az EU területén, tekintettel a program központi célkitűzéseire a biztonságos és fenntartható digitális infrastruktúrák megteremtése, és a magas szintű konnektivitást biztosító gigabites internethozzáférés biztosítása területén. Az újgenerációs hírközlési hálózatok tekintetében az EU már szabvány szintjén fokozta az elektronikus információbiztonság követelményeit, elsősorban a titkosság tekintetében. Az EU digitális stratégiai célkitűzései és az azzal kapcsolatos aktuális és prognosztikus jog- és szakpolitikai törekvések okán ezen ponton szükséges kitekinteni annak LI-re gyakorolt hatásaira, így az uniós stratégiai célkitűzés hátterében álló tényezők mélyebb összefüggéseinek feltárására. Az e-hírközlési adatvédelmi rendelet javaslat tartalmi értelmezése és kontextusba helyezése az értekezés kapcsolódó részeivel azért szükséges, mert azt összevetve a digitalizációs uniós törekvések keretében megalkotott hatályos normákkal prognosztikus jellegű következtetések válnak levonhatóvá az elektronikus hírközlési és az IKT szolgáltatások piacának jövőbeli alakulásáról, a jogalkotói szemléletről. Annak érdekében, hogy az értekezés célkitűzései megvalósíthatóak legyenek jelen alfejezetben szükséges és indokolt megvizsgálni az EU digitális piaci és adatvédelmi stratégiai célkitűzéseinek tendenciáit az LI aspektusából.

2.4.1. Az EU digitális piaci stratégiai célkitűzéseinek vizsgálata

Az EU Versenyképességi Tanácsának a „Digitális egységes piac: az európai ipar digitális átalakítása” témájú 2015. május 28-29-ei ülésén megvitatták az Európai digitális egységes piacra vonatkozó új stratégiát, és következtetéseket fogadtak el az európai ipar digitális átalakításáról.[143] Dana Reizniece-Ozola, a lett gazdasági miniszter hozzászólása alapján „*egy jól teljesítő digitális egységes piac évi több mint 400 milliárd euróval járulhat hozzá az európai gazdasághoz és több százezer új munkahelyet teremth*et”.[144] A közösségi szintű digitalizációnak jelentős gazdasági növekedést serkentő hatásai vannak uniós szinten. Ez azonban csak a polgárok digitalizációval, az információs társadalommal összefüggő termékekkel és

[142] *Façonner l'avenir numérique de l'Europe - Conclusions du Conseil* (9 juin 2020) Bruxelles. 2020. Online: https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/fr/pdf (Letöltés ideje: 2024. február 18.)

[143] *Competitiveness Council 28 and 29 May in Brussels*. Council of the European Union. 2015. Online: https://www.consilium.europa.eu/media/23442/background-note-compet-may_en.pdf (Letöltés ideje: 2024. február 17.)

[144] *Versenyképességi Tanács, 2015.5.28–29*. Brüsszel. Európai Unió Tanácsa. 2015. Online: https://www.consilium.europa.eu/hu/meetings/compet/2015/05/28-29/ (Letöltés ideje: 2024. február 17.)

szolgáltatásokkal – például az alkalmazás-szolgálttásokkal – kapcsolatos bizalma esetén tud érvényesülni, hiszen ekkor fogyasztanak optimális mértékben. A versenyjogi kontextusokat nem tárgyalva a bizalom egyik fő eleme a személyes adatok védelme, azoknak az e-adatvédelmi hírközlési rendelet javaslat (15) preambulumbekezdése szerinti bizalmassága, így az azokat sértő törekvések megelőzése, elhárítása, felderítése. Ennek egyik fő komponense az elektronikus információvédelem útján elérhető elektronikus információbiztonság, a védelmi intézkedéseken belül is az értekezés szempontjából lényeges kriptográfia, rejtjelezés (2.7. alfejezetben részletesen vizsgálva). Az EU Közlekedési, Távközlési és Energiaügyi Tanácsának 2015. június 11–12-ei ülésén a tagállamok távközlésért (hírközlésért) felelős miniszterei a fentiekkel összefüggésben kifejezték a digitalizált gazdaság fontos szerepét az EU versenyképességének fokozásában, mely egyik kritériumaként azonosították a kiberbiztonság javításának és az elektronikus szolgáltatásokba vetett bizalom erősítésének szükségességét, valamint a jobb infrastruktúra és gyorsabb szélessávú hozzáférés biztosításának nélkülözhetetlenségét.[145] A fentiek alapján úgy tűnik, hogy Veblen 1978-ban publikált gondolati[146] mintegy kb. 45-50 év után is megállják a helyüket, miszerint „*A technológia […] egységes gazdasági rendet teremt, amiben mindenki egy fogaskerék, és hozzájárul az egész gazdasági rend fejlődéséhez*."[147]

A fentiek alapján tehát már 2015-ben az EU-s jogalkotás szintjén megfogalmazódott a hatékony technikai adatvédelmi kompetenciákkal bíró szélessávú hírközlő – például mobilinternet – hálózatok fejlesztésének, elterjedésének szükségessége (3.1. – 3.3. alfejezetekben részletesen vizsgálva) az EU egységes digitális piacának megvalósítása érdekében, így fokozva az Unió versenyképességét és a gazdasági növekedést. Ezen fenti uniós jog- és szakpolitikai törekvések mentén jöhetett létre a digitális szolgáltatásokról szóló jogszabálycsomag, amely további fő célja a versenyképesség és gazdasági növekedés biztosításán túl, vagy annak inkább egyik nem elhanyagolható feltételeként a biztonságos digitális tér létrehozása, melyben a digitális

[145] *Közlekedési, Távközlési és Energiaügyi Tanács, 2015.6.11–12*. Európai Unió Tanácsa. 2015. Online: https://www.consilium.europa.eu/hu/meetings/tte/2015/06/11-12/ (Letöltés ideje: 2024. február 17.)

[146] VEBLEN, Thorstein (1978): *The Theory of Business Enterprise*. London: Routledge.

[147] DOBÁK Imre – KENEDLI Tamás (2023): Információszerzési tendenciák és kihívások a kibertérben rejlő lehetőségek és a mesterséges intelligencia viszonylatában. *Military and Intelligence CyberSecurity Research Paper*, 3(2), 2. Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/MIC%20RP%202023-3%20-%20Dob%C3%A1k%20Imre-Kenedli%20Tam%C3%A1s%20-%20Inform%C3%A1ci%C3%B3szerz%C3%A9si%20tendenci%C3%A1k%20%C3%A9s%20kih%C3%ADv%C3%A1sok%20a%20kibert%C3%A9rben%20rejl%C5%91%20lehet%C5%91s%C3%A9gek%20%C3%A9s%20a%20mesters%C3%A9ges%20intelligencia%20viszonylat%C3%A1ban.pdf Letöltés ideje: 2024. február 18.)

szolgáltatások[148] valamennyi felhasználójának alapvető jogai védelemben részesülnek. Az uniós jogszabálycsomagnak két fő komponense van, a 2022. novemberértől hatályos digitális szolgáltatásokról szóló rendelet[149] (a továbbiakban: DSA[150]) és a digitális piacokról szóló rendelet[151] (a továbbiakban: DMA[152]), mely 2024. január 1-jétől közvetlenül alkalmazandó az EU-ban. Sem a DSA, sem a DMA hatálya nem függ a szolgáltatók letelepedési helyétől (letelepedési ország elve), ha a szolgáltatás a hatáselv alapján az Unió területére hat, azaz ott igénybe vehető, így a hatáselv alapján akár az USA-ban, akár például Kínában letelepedett óriásplatformokra egyaránt alkalmazandó. [153]

A digitális transzformáció, az IKT környezet fejlődése számos társadalmi és gazdasági kihívást is magában rejt, mint például az illegális áruk, szolgáltatások és tartalmak online kereskedelme, cseréje, illetve a manipulatív algoritmusok és a félretájékoztatás veszélye. Az információs társadalom és a digitalizálódó gazdaság bővülése okán a jelentősebb online alapvető platformszolgáltatások a DMA 3. cikk (1) – (2) bek. szerint szabályozott kritériumrendszer, küszöbértékek alapján besorolt „kapuőrként" jelennek meg az európai digitális piacokon (például Meta Platforms Inc., Apple Inc., Microsoft LLC), amelyeknek lehetőségük van arra, hogy jelentősebb részt vállaljanak az alapvető platformszolgáltatásokon megjelenő jogellenes és káros tartalmak visszaszorítása érdekében.[154] A DMA a BEREC[155] témakört érintő legújabb jelentésében, a Hírközlési Kódexben – és az Eht.-ben is – megjelenő fogalomrendszerrel harmonikusan az értekezés szempontjából vizsgált titkosított online számfüggetlen

[148] Digitális szolgáltatásoknak minősülnek az online szolgáltatások az egyszerű weboldalaktól az internetes infrastruktúra-szolgáltatásokig és az online, alapvető platformszolgáltatásokig, melyeken kommunikálhatunk – például az alkalmazásszolgáltatásokon – médatartalmakat streamelhetünk, vásárolhatunk, online bankolhatunk stb. (Ezen szolgáltatások rendszertani elhatárolására a 2.6.1. - 2.6.3. részfejezetekben kerül sor.)

[149] Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet) (a továbbiakban: DSA) OJ L 277, 27.10.2022, 1–102.

[150] DSA: Digital Services Act – digitális szolgáltatásokról szóló törvény

[151] Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály) (a továbbiakban: DMA) OJ L 265, 12.10.2022, 1–66.

[152] DMA: Digital Markets Act – digitális piacokról szóló törvény

[153] DR. SZALAI Anita (2023): *Már hatályos a DSA, a digitális szolgáltatásokról szóló rendelet*. SzalaiLegal. Online: https://www.szalailegal.hu/mar-hatalyos-a-dsa-a-digitalis-szolgaltatasokrol-szolo-rendelet/ (Letöltés ideje: 2024. február 17.)

[154] DALY, Andrew (2022): T*he Digital Markets Act proposes messaging interoperability, but this is easier said than done*. Analysys Mason. Online: https://www.analysysmason.com/contentassets/dbe8d6f83e7f4b9489b3783601ee6d45/analysys_mason_dma_messaging_interoperability_apr2022.pdf (Letöltés ideje: 2024. február 17.)

[155] BEREC: Body of European Regulators for Electronic Communications - Európai Elektronikus Hírközlési Szabályozók Testülete

személyközi infokommunikációt lehetővé tevő alkalmazásszolgáltatásokat NI-ICS[156] kategóriaként hivatkozza. A Bizottság minősítő határozatában a küszöbérték elérése okán NI-ICS kategóriában alapvető kapuőrré sorolta a Meta Platforms Inc.-t (a továbbiakban: Meta), mint a DMA 2. cikk 1. pont szerinti alapvető platformszolgáltatást nyújtó vállalkozást, az általa üzemeltett WhatsApp és Facebook Messenger alkalmazásszolgáltatások, alapvető platformszolgáltatások NI-ICS-ek tekintetében.[157] Tehát a DMA (7) preambulumbekezdése alapján szolgáltatásaik keretében biztosítaniuk kell a jogsértő és káros tartalmak, a jogszerűtlen adatkezelés és tisztességtelen verseny elleni intézkedések érvényesülését, elősegítve a határokon átnyúló üzleti tevékenység elősegítésének, és ezáltal a belső piac megfelelő működésének javítását. A Bizottság minősítő határozatában az Apple Distribution International Ltd. (az Apple európai, írországi székhelyű disztribútora) (a továbbiakban: Apple) által üzemeltett iMessage alkalmazás-szolgáltatást is NI-ICS-ként kezeli, azonban az iMessage tekintetében a DMA szerinti kapuőri minősítése ellen fellebbezett, azzal érvelve, hogy a szolgáltatás nem éri el a DMA szerinti küszöbértéket. Ennek okán a Bizottság piaci vizsgálatot indított, azonban ez nem befolyásolja az iMessage Bizottság általi NI-ICS-ként történő értelmezését.[158]

---

[156] NI-ICS: Number-Independent Interpersonal Communication Services – számfüggetlen személyközi kommunikációs szolgáltatás: Lásd: *BEREC report on interoperability of NumberIndependent Interpersonal Communication Services (NI-ICS)*. BEREC, BoR (23) 92. 2023. Online: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-interoperability-of-number-independent-interpersonal-communication-services-ni-ics (Letöltés ideje: 2024. február 17.)

[157] Commission Decision of 5.9.2023 designating Meta as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector, DMA.100020 Meta - online social networking services, DMA.100024 Meta - number-independent interpersonal communications services, DMA.100035 Meta - online advertising services, DMA.100044 Meta - online intermediation services – marketplace. Brussels, 5.9.2023, C(2023) 6105 final. WhatsApp minősítése, összefoglaló jogalap indoklása: 5.4.3. alpont; Messenger minősítése, összefoglaló jogalap indoklása: 5.5.4. alpont. Online: https://ec.europa.eu/competition/digital_markets_act/cases/202346/DMA_100024_206.pdf (Letöltés ideje: 2024. február 19.); C/2023/1092 a Bizottság határozatának összefoglalója (2023. szeptember 5.) az (EU) 2022/1925 rendelet 3. cikke szerinti határozatról (Ügyek DMA.100020 – Meta – online social networking services; DMA.100024 – Meta – Number-independent interpersonal communications services; DMA.100035 – Meta – Online advertising services; DMA.100044 – Meta – Online intermediation services – Marketplace). 5. fejezet (26) bek. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:C_202301092 (Letöltés ideje: 2024. február 19.)

[158] Commission Decision of 5.9.2023 designating Apple as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector, DMA.100020 Meta - online social networking services, DMA.100013 Apple – online intermediation services – app stores, DMA.100025 Apple – operating systems és DMA.100027 Apple – web browser. Brussels, 5.9.2023, C(2023) 6100 final. iMessages minősítése, összefoglaló jogalap indoklása: 5.4.4. alpont. Online: https://ec.europa.eu/competition/digital_markets_act/cases/202344/DMA_100027_197.pdf (Letöltés ideje: 2024. február 19.); A Bizottság határozatának összefoglalója (2023. szeptember 5.) az Apple-nek a digitális ágazat vonatkozásában a versengő és tisztességes piacokról szóló (EU) 2022/1925 európai parlamenti és tanácsi rendelet 3. cikke értelmében történő kapuőrré minősítéséről (DMA.100013 Apple – online intermediation services – app stores, DMA.100025 Apple – operating systems és DMA.100027 Apple – web browsers). 4. fejezet (14) bek. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:C_202300548 (Letöltés ideje: 2024. február 19.)

A részfejezetben vizsgált uniós digitális egységes piaccal, és kiberbiztonsággal, adatvédelemmel kapcsolatos normák, valamint azok hátterének elemzése első olvasatra úgy tűnhet, mintha csak igen korlátozottan kapcsolódna az értekezés vizsgálatának tárgyához, azonban ez nem igaz, mind az elektronikus hírközlés, azon belül is az internetszolgáltatások, mind az információs társadalommal összefüggő alkalmazásszolgáltatások LI-je szempontjából meghatározó lesz a jövőben az uniós jog- és szakpolitikai törekvések okán. Mind a szolgáltatások elterjedése, a digitális piac dinamikus bővülése miatt, mind a fokozódó normatív adatvédelmi szigorítások és az ebből adódó technológiai fejlődés miatt, mely az alkalmazásszolgáltatások kriptográfiai jellemzőinek fejlődése terén jelentős kihívást eredményez a nemzetbiztonsági célú LI számára. A fentiek okán szükséges az elektronikus információvédelmi, -biztonsági törekvések mélyebb áttekintése is a következő részfejezetben.

2.4.2. Az EU digitális adatvédelmi stratégiai célkitűzéseinek vizsgálata

A fentiek szerinti uniós jog- és szakpolitikai törekvések mentén jöhetett létre a biztonságos digitális piac másodlagos uniós jogforrási komponenseként a 2016-tól formálódó, az EU egészének kiberrezilienciáját javító, az egész Unióban egységesen magas szintű kiberbiztonságot biztosító intézkedésekről szóló 2023-tól hatályos irányelv[159] (a továbbiakban: NIS2[160]), amely jogi intézkedéseket tartalmaz az uniós szintű kiberbiztonság általános szintjének növelése érdekében. A NIS2 az egyes kiemelten kritikus ágazatokban (például hírközlési ágazat, digitális infrastruktúra-szolgáltatások ágazata, kihelyezett IKT-szolgáltatások ágazata és az űralapú szolgáltatások ágazata) működő szervezeteknek, társaságoknak előírja, hogy biztosítaniuk kell a szolgáltatásnyújtáshoz és tevékenységük végzéséhez használt elektronikus információs rendszerek, hálózatok magasabb szintű biztonságát, illeszkedve az EU kiberbiztonsági politikájába.[161] A tagállamoknak, így Magyarországnak is 2024. október 17-ig kell implementálniuk a nemzeti jogba az uniós jogforrást, mely szakmai előkészítése az NBSZ főigazgatójának elnöklésével működő Nemzeti

[159] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv). OJ L 333, 27.12.2022, 80–152.

[160] *Irányelv az egész Unióban egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS2 irányelv).* Európai Bizottság. Online: https://digital-strategy.ec.europa.eu/hu/policies/nis2-directive (Letöltés ideje: 2024. február 17.)

[161] KOVÁCS, László (2018): Cyber Security Policy and Strategy In The European Union and NATO. *Land Forces Academy Review,* 23(1), 16-24. Online: https://doi.org/10.2478/raft-2018-0002 (Letöltés ideje: 2024. február 25

Kiberbiztonsági Koordinációs Tanács (a továbbiakban: NKKT) kereteiben zajlik.[162] Az implementálás nagyrészben már megtörtént a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (a továbbiakban: Kibertan. tv.), és az információs és kommunikációs technológiák [IKT] kiberbiztonsági tanúsításáról szóló 10/2023. (V. 15.) SZTFH[163] rendelet keretében, valamint várható az IoT eszközök nemzeti tanúsítási rendszeréről szóló részletszabályok megalkotása is. Továbbá 2024. január 31-én elfogadásra került a Bizottság 2025. február 27-től alkalmazandó Európai Kiberbiztonsági Tanúsítási Rendszerének (a továbbiakban: EUCC[164]) végrehajtási rendelete[165], mely többek között az IKT termékek biztonsági követelményeit lesz hivatott meghatározni uniós szinten, valamint a felhőszolgáltatások tanúsítási eljárásaira vonatkozó részletszabályok (a továbbiakban: EUCS[166]) is várhatók.[167] A fenti uniós és nemzeti normák mind részei a 2018/19-től formálódó EU Kiberbiztonsági Tanúsítási Keretrendszerének,[168] összhangban a digitalizációs stratégiával.

E ponton szükséges kitekinteni a témaválasztás indoklásában is jelzett, a Digitális évtized 2030 szakpolitikai program keretén belül az EU digitális biztonsági ökoszisztémájának részét képező 2022. december 15-én elfogadott „*Digitális jogokról és elvekről szóló európai nyilatkozat*”-ra, amely célja a technológiai biztonság adatvédelmi szempontú zsinórmértékének kinyilatkoztatása, összhangban a digitális fejlődés elősegítésével, továbbá hogy hozzájáruljon az EU gazdaságának és társadalmának dinamikussá, erőforrás-hatékonnyá és méltányossá válásához. Petr Fiala cseh miniszterelnök e kapcsán elmondta, hogy a nyilatkozat aláírásával „*elkötelezzük magunkat az inkluzív, méltányos, biztonságos, fenntartható és emberközpontú digitális átalakulás mellett. Az alapvető uniós értékek megőrzése ugyanolyan fontos az interneten, mint a valós világban. A nyilatkozat ezenfelül referenciaként szolgál majd a*

[162] 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről

[163] SZTFH: Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH)

[164] EUCC: European Cybersecurity Certification - Európai Kiberbiztonsági Tanúsítási (keret)Rendszer

[165] A Bizottság (EU) 2024/482 végrehajtási rendelete (2024. január 31.) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról. OJ L, 2024/482, 2024.07.02.

[166] EUCS: European Cybersecurity Certification Scheme for Cloud Service - Felhőszolgáltatások Európai Kiberbiztonsági Tanúsítási Rendszere

[167] DR. BENCSIK Balázs (2023): *Az SZTFH szerepe a kiberbiztonságban*. SZTFH. 8. Online: https://www.fogalomtar.hte.hu/documents/10180/4737479/C_3_Dr_Bencsik_Balazs_Szabalyozott_Tevekenysegek_Felugyeleti_Hatosag_szerepe_a_kiberbiztonsagban.pdf (Letöltés ideje: 2024. február 17.)

[168] Lásd: TÓTH Tamás (2019): Az Európai Unió tervezett kiberbiztonsági tanúsítási keretrendszerének bemutatása *Szakmai Szemle*, 17(1), 97-115. Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2019_1_szam.pdf (Letöltés ideje: 2024. február 17.); *Az uniós kiberbiztonsági tanúsítási keret*. Európai Bizottság. Online: https://digital-strategy.ec.europa.eu/hu/policies/cybersecurity-certification-framework (Letöltés ideje: 2024. február 17.)

szakpolitikai döntéshozók, a vállalkozások és az egyéb érintett szereplők számára az új technológiák kifejlesztése és bevezetése során."[169] Az előbbi nyilatkozat továbbá kitér a nyitott módon megvalósuló digitális szuverenitásra, a jogállamiság és a demokrácia tiszteletben tartására, a hozzáférhetőségre, az egyenlőségre,, a rezilienciára, az életminőség javítására, a szolgáltatások elérhetőségére, valamint minden ember alapvető jogainak a tiszteletben tartására. Ami azonban kiemelendő a magánélet védelmével kapcsolatos intézkedések, törekvések tekintetében, hogy a nyilatkozat 16. pontja a védett, biztonságos digitális környezettel kapcsolatban kimondja, hogy „*Mindenki számára hozzáférhetővé kell tenni az olyan digitális technológiákat, termékeket és szolgáltatásokat, amelyek kialakításuknál fogva biztonságosak, védettek, és garantálják a magánélet védelmét, aminek eredményeként biztosított a kezelt információk nagymértékben bizalmas jellege, integritása, rendelkezésre állása és hitelessége.*" – ezen elköteleződés teljes mértékben megfelel az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) fogalomhasználata szerint értelmezett elektronikus információs rendszer biztonságának[170], mely részletesen a 2.7. alfejezetben kerül kifejtésre. A nyilatkozat 18. pontja a magánélet védelme és az adatok feletti egyéni rendelkezés kapcsán kimondja, hogy „*Mindenkinek joga van közlései és az elektronikus eszközein található információk bizalmasságához és ahhoz, hogy ne legyen kitéve jogellenes online megfigyelési, jogellenes széles körű nyomonkövetési vagy lehallgatási intézkedéseknek.*"[171] – azaz szakpolitikai célkitűzésként határozza meg a normatív és elektronikus információ-, kibervédelem fokozását.

A részfejezet következtetéseként megállapítható, hogy mind a digitális, IKT szolgáltatások elterjedése, a digitális piac dinamikus bővülése, mind a fokozódó normatív adatvédelmi szigorítások és az ebből adódó technológiai innováció az alkalmazásszolgáltatások kriptográfiai jellemzőinek fejlődése terén jelentős kihívást eredményez a nemzetbiztonsági célú LI számára. A fenti komplex uniós jog- és szakpolitikai törekvések szerinti digitális ökoszisztéma elemeként értelmezett elektronikus információ-, kibervédelem, azon belül is a kriptográfia részletes kifejtése, és összefüggéseinek feltárása az LI-vel, azaz az értekezés vizsgálatának tárgyával a 2.7. alfejezetben kerül általánosan tárgyalásra, majd speciálisan a 3. fejezetben az

[169] *Déclaration sur les droits et principes numériques: les valeurs et les citoyens de l'UE au cœur de la transition numérique*. Conseil de l'UE. 2022. Online: https://www.consilium.europa.eu/fr/press/press-releases/2022/12/15/declaration-on-digital-rights-and-principles-eu-values-and-citizens-at-the-centre-of-digital-transformation/ (Letöltés ideje: 2024. február 19.)
[170] Ibtv. 1. § (1) bek. 15.pont
[171] The European Parliament, the Council and the Commission solemnly proclaim the following joint Declaration on Digital Rights and Principles for the Digital Decade. 15 December 2022. OJ C 23, 23.1.2023, 1–7.

elektronikus hírközlés LI-je kapcsán, a 4. fejezetben az alkalmazásszolgáltatások LI-je kapcsán. Továbbá a fenti elemzésből levezethető következtetés, hogy az uniós jog terrénumán az elektronikus információ-, kibervédelem (NIS2) az általános adatvédelmi szabályozásnak (GDPR) egy speciális jogterületévé vált a személyes adatvédelem szempontjából.

2.5. Az LI hazai szervezetrendszeri és általános normatív, szakirodalmi háttere

Az alfejezetben az értekezés célkitűzéseinek megvalósítása érdekében jelen alfejezetben vizsgálat tárgyát képezi az LI hazai szervezetrendszere, és nemzetbiztonsági, bűnüldözési célú általános szabályozása, valamint szakirodalom szerinti módszerei és eljárásai.

2.5.1. Az LI hazai szervezetrendszere

A titkos információgyűjtés, annak résztevékenységeként az LI szervezet- és eszközrendszerét végrehajtói oldalról elemezve megállapítható, hogy az Alaptörvény jelentette kerethez igazodva a hazai szervezeti kijelölés transzparensen törvényi szinten történik minden esetben, annak részletszabályai kerülnek rögzítésre kormányrendeleti szinten, hiszen „*a nemzetbiztonsági szabályozás alapját mindenképpen nyilvános jogszabályok kell, hogy adják, amely törvényi szintet jelent, de szerencsésebb, ha keret jelleggel mindez megjelenik alkotmányos szinten is*.”[172] Az Nbtv. 4-8. § határozza meg a nemzetbiztonsági célú LI alkalmazására és annak végrehajtására jogosult nemzetbiztonsági szolgálatok körét.[173] Az Ütv., az Rtv. a NAV tv., valamint a TEK Korm. rendelet és a 293/2010. (XII. 22.) Korm. rendelet (a továbbiakban: NVSZ Korm. rendelet) pedig meghatározzák a bűnüldözési célú titkos információgyűjtő eszközök[174] – az értekezés során beleértendő a leplezett eszközök kategóriája is – alkalmazására jogosult igazságügyi, bűnüldöző, bűnfelderítő, belső bűnmegelőző szervek

[172] SABJANICS 2017: 121

[173] Megjegyzendő, hogy az egyes törvényeknek a Magyarország minisztériumainak felsorolásáról szóló 2022. évi II. törvényhez kapcsolódó módosításáról szóló T/48. sz. törvényjavaslat elfogadásával az Nbtv. és az egyéb rendvédelmi tárgyú jogszabályok jelentős módosításokon mentek keresztül. A törvénymódosítás hatására a polgári nemzetbiztonsági szolgálatok saját állományuk tekintetében ismét ellátják a belső biztonsági és bűnmegelőzési célú ellenőrzési feladatokat, továbbá a kifogástalan életvitel ellenőrzését. Az LI végrehajtását és szervezetrendszerét a normamódosítási csomag nem érintette.

[174] A bűnüldözési célú titkos információgyűjtés és leplezett eszköz alkalmazásának új Be. szerinti elhatárolását lásd: JANCSÓ Gábor (2018): Leplezett eszközök alkalmazása: titkos információgyűjtés az új büntetőeljárási törvényben. *Acta Humana*, 6(1), 19-34. Online: https://folyoirat.ludovika.hu/index.php/actahumana/article/download/880/255/4337 (Letöltés ideje: 2024. február 15.); SZENDREI Ferenc (2020): A rendészeti célú titkos információgyűjtés. *Rendőrségi Tanulmányok*, 3(3), 58-80. Online: https://epa.oszk.hu/04000/04093/00012/pdf/EPA04093_rendorsegi_tanulmanyok_2020_3_058-080.pdf (Letöltés ideje: 2024. február 15.)

körét (a továbbiakban együtt: jogosultak), amely tevékenységhez a Be. eljárásjogi részletszabályokat és keretet biztosít. Az alábbi 3. ábra hivatott szemléltetni az LI alkalmazására és annak végrehajtására jogosult hazai nemzetbiztonság és bűnüldöző szervezeteket[175].

3. ábra: Az LI alkalmazására és annak végrehajtására jogosult hazai nemzetbiztonság és bűnüldöző szervek (Szerk.: A szerző)

A 3. ábrán szereplő kilenc szervezet közül az értekezés szempontjából kiemelendő az NBSZ, mivel az Nbtv. 8. § (1) bek. a) pontja alapján a másik nyolc szervezet írásbeli megkeresésére[176] speciális eszközeivel és módszereivel végrehajtja a titkos információgyűjtést, kvázi „szolgáltatást nyújt" számukra.[177] Ezen szerepkört jogilag is erősítve az Nbtv. 53. § (3) bek. 2018. július 1-ei hatállyal[178] kimondja, hogy „*a titkos információgyűjtés folytatására feljogosított nemzetbiztonsági szolgálat a titkos információgyűjtést önállóan vagy más nemzetbiztonsági szolgálat közreműködésével hajtja végre, vagy a végrehajtáshoz a Nemzetbiztonsági Szakszolgálatot veszi igénybe*". Továbbá a Be. 244. § (1) bek. az Nbtv. 53. § (3) bekezdésével összhangban vagylagosan kimondja, hogy „*A leplezett eszközök*

[175] Az EUMSZ V. cím, 67-89. cikke szerinti SZBJT szerinti uniós terminológia alapján beleértendő a büntető igazságügyi, a rendőrségi és vámügyi bűnüldözési célú titkos információgyűjtés is.
[176] Nbtv. 8. § (3) és (4) bek. alapján az NBSZ saját hatáskörben és kezdeményezésre csak egy igen szűk körben jogosult a titkos információgyűjtő eszközök alkalmazására.
[177] DOBÁK Imre (2015): Nemzetbiztonsági szolgálatok – Betekintés a visegrádi országok (V4) nemzetbiztonsági rendszereibe. *Hadtudományi Szemle*, 8(4), 117. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/10159/2015_4_visegr%c3%a1di%20orsz%c3%a1gok.pdf?sequence=2&isAllowed=y (Letöltés ideje: 2024. február 20.)
[178] Be. 19. § (5) bek.

alkalmazására feljogosított szerv […] a leplezett eszköz alkalmazásához a nemzetbiztonsági szolgálatokról szóló törvény által ilyen szolgáltatások végzésére kijelölt nemzetbiztonsági szolgálatot veszi igénybe". Az Ütv. 25/Q. § (1) bek. kimondja, hogy az ügyészség a titkos információgyűjtés végrehajtásához pedig az NBSZ szolgáltatásait is igénybe veheti.

Továbbá, ha a közösségi jog terén az SZBJT keretében megvalósuló másodlagos uniós jogforrások szerinti bűnüldözési célú együttműködések hazai megfeleltetését vizsgáljuk megállapítható, hogy az igazságügyi (bűnüldözési) célú együttműködés tekintetében a büntetőügyekben kibocsátott európai nyomozási határozatról (a továbbiakban: ENYH) szóló irányelv[179] (a továbbiakban: ENYH irányelv) hazai transzformálására az Európai Unió tagállamaival folytatott bűnügyi együttműködésről szóló 2012. évi CLXXX. törvényben került sor. A törvény 65/A. – 65/D. §-ai szabályozzák az LI terén megvalósuló nemzetközi együttműködést, mely kapcsán az ENYH végrehajtására a törvény 65/A. § (2) bek. alapján a vármegyei főügyészségek, illetve a Fővárosi Főügyészség rendelkezik hatáskörrel, amelyek a magyar joghatóság alá tartozó eljárásokon túl az Ütv. 25/Q. § (1) bek. alapján az ENYH végrehajtása keretében is igénybe vehetik az NBSZ szolgáltatásait LI során. A bűnüldözési célú rendőrségi és a vámhatósági uniós együttműködésre és információcserére ad jogi keretet a Tanács 2006/960/IB kerethatározata[180], amely rendelkezései a magyar jogban a bűnüldöző szervek nemzetközi együttműködéséről szóló 2002. évi LIV. törvény keretén belül került transzformálásra elsődlegesen. A törvény 8. § (1) bek. j) pontja lehetővé teszi nemzetközi együttműködés alapján az Rtv. 71. § és a NAV tv. 60. § szerinti külső bírói engedélyhez kötött titkos információgyűjtést, azon belül is az LI területén történő együttműködést, melyet a „lehallgató eszköz" fogalom használatával megerősít a törvény 36. §-a. Az Nbtv., a Be. és az Ütv. korábbiakban már ismertetett rendelkezéseivel, illetve az Rtv. 75/F. § és a NAV tv. 65/E. § szakaszával harmonikusan a törvény 8. § (2) bek. alapján a hazai bűnüldöző szerv a titkos információgyűjtés végrehajtására szintén igénybe veheti az NBSZ-t.

A fentiek alapján tehát a részfejezet következtetéseként megállapítható, hogy a jogalkotó biztosítja mind a magyar joghatóság szerinti, mind a nemzetközi együttműködések keretében megvalósuló eljárások során a bűnüldözési és a nemzetbiztonsági ágazat közötti

[179] Az Európai Parlament és a Tanács 2014/41/EU irányelve (2014. április 3.) a büntetőügyekben kibocsátott európai nyomozási határozatról. (a továbbiakban: ENYH irányelv) OJ L 130, 1.5.2014, 1–36.

[180] A Tanács 2006/960/IB kerethatározata (2006. december 18.) az Európai Unió tagállamainak bűnüldöző hatóságai közötti, információ és bűnüldözési operatív információ cseréjének leegyszerűsítéséről. OJ L 386, 29.12.2006, 89–100.

„átjárhatóságot", az együttműködés normatív keretét a titkos információgyűjtés során, külön nevesítve speciális szolgáltatói szerepköréből adódóan a NBSZ-t, ami a vizsgált szakirodalom és jogszabályok alapján „*olyan rendvédelmi szerv, amely hazánk nemzetbiztonsága, közrendje és közbiztonsága védelme érdekében folytatja tevékenységét*".[181] Itt szükséges megjegyezni a „nemzetbiztonsági célú" és „bűnüldözési célú" fogalomkör problematikáját, hiszen ha az NBSZ nemzetbiztonsági érdekkörben, nemzetbiztonsági szolgálat megkeresése alapján jár el, akkor nemzetbiztonsági tevékenységet valósít meg, amely nem tartozik a közösségi jog hatálya alá, azonban, ha bűnüldöző szerv megkeresésre, bűnüldözési érdekkörben jár el, akkor a szerződések alapján a tevékenység a közösségi jog hatálya alá tartozik, így például a nemzetközi együttműködésre megnyílik a lehetősége. Azonban, mint arra a 2.1. alfejezetben utaltam elkerülhetetlen a megjelenés, azaz a külvilág számára észlelhető alaki elem, miszerint az Nbtv. szerinti polgári nemzetbiztonsági szolgálat jár el. Ezen kérdéskör részletesebb vizsgálatára és a feloldására tett javaslatra a későbbeikben kerül sor.

Az NBSZ feladat- és hatásköre azért is kiemelt az LI szempontjából, mivel az elektronikus hírközléssel kapcsolatos ágazati törvény,[182] valamint annak vonatkozó végrehajtási rendelete[183] az LI téren kizárólagosságot (koncentrált képességfenntartást, eszközalkalmazást) biztosítanak számára a szolgáltatói együttműködési kötelezettség jogszabályi előírásával. Az NBSZ LI-vel kapcsolatos speciális szolgáltatói szerepköre és annak részletszabályai mind az elektronikus hírközlési szolgáltatások, mind az információs társadalommal összefüggő egyes alkalmazásszolgáltatások terén a későbbiekben kerülnek átfogóan elemzésre. A fentiek alapján reflektálva a 2016-os szakirodalomban[184] levont következtetésekre megállapítható, hogy az NBSZ esetében az egy szervezetben koncentrált LI képesség kialakításra került, mely akár nemzetközi együttműködés keretében bűnüldözési célú LI során is igénybe vehető a jogosultak által.

[181] BODA József (2012): A Nemzetbiztonsági Szakszolgálat helye és szerepe a rendvédelemben. *Pécsi Határőr Tudományos Közlemények*, 11(12), 115.Online: https://www.pecshor.hu/periodika/XIII/boda.pdf (Letöltés ideje: 2024. február 20.)
[182] Eht. 92. § (1) – (6) bek.
[183] 180/2004. (V. 26.) Korm. rendelet 3. §, 6. §
[184] KOVÁCS 2016: 92-93

2.5.2. *Az LI hazai nemzetbiztonsági, bűnüldözési célú általános szabályozása*

Tartalmi oldalról vizsgálva a szakirodalom alapján[185] az LI-t magában foglaló bővebb halmazból, az információs rendszerek ellenőrzésének feladatrendszeréből indokolt kiindulni[186], melyen belül az alábbi 3 főcsoport különböztethető meg az egyes résztevékenységek elhatárolása alapján:

1. adatszolgáltatás;
2. kommunikáció hálózati ellenőrzése – valós idejű vagy utólagos; valamint
3. forenzikus tevékenység – a végponti eszköz fizikai hozzáférésével, vagy távolról.

Az Nbtv. és Be. szerinti hazai szabályozás alapján az alábbi LI résztevékenységi körök határolhatók el egymástól:

1. a kommunikáció releváns kísérő-, metaadataihoz történő hozzáférés[187];
2. a hírközlő hálózaton, vagy információs rendszeren folytatott kommunikáció tartalmának tényleges megismerése és rögzítése;[188] valamint
3. az információs rendszeren, infokommunikációs eszközökön kezelt adatok megismerése és rögzítése[189].

Abban az esetben, ha a fenti három tevékenységi kör alapjog korlátozás szempontjából kerül vizsgálatra, akkor az első esetében sérülnek a legkevésbé a titkos információgyűjtéssel érintett személy alapvető jogai. Ez esetben az LI-t alkalmazó, végrehajtó szerv a kommunikáció tartalmát nem ellenőrzi, csak annak kísérő-, metaadatait kívánja megismerni. A második esetben történhet jelentős mértékben az alapjog korlátozás, hiszen ez esetben az LI magának a hírközlő hálózaton folytatott kommunikáció tartalmának megismerésére irányul. A harmadik eset az első két tevékenységi kör integrált és jóval kibővítettebb változata, mely során az ellenőrzés az infokommunikációs eszköz közvetlen elérésével, úgynevezett végponti

[185] DR. DOBÁK Imre – KOVÁCS Zoltán (2014): Új technológiák hatása a hírszerzésre. In DR. DOBÁK Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. 218. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/100414/609.pdf?sequence=1 (Letöltés ideje: 2024. július 7.); KOVÁCS 2015: 138

[186] Az értekezés során az LI vizsgálata szempontjából az adatszolgáltatás és a kommunikáció hálózati ellenőrzése képezi a vizsgálat tárgyát, azon belül is a későbbiekben ismertetésre kerülő központi monitoring alrendszer útján, az elektronikus hírközlő hálózat oldaláról történő ellenőrzés.

[187] Nbtv. 54. § (1) bek. j) pont; Be. 215. § (9) bek.

[188] Nbtv. 56. § (1) bek. d) pont; Be. 232. § (5) bek.

[189] Nbtv. 56. § (1) bek. e) pont; Be. 232. (1) bek.

ellenőrzéssel történik. Ez esetben magán az eszközön, rendszeren (például okostelefon, számítógép) kezelt adatok, és tevékenységek (például tárolt multimédiás tartalmak, dokumentumok, szöveges tartalmak, online szolgáltatások igénybevétele) teljes körű ellenőrzésére van lehetősége a jogosult LI szervnek, függetlenül az eszköz, szolgáltatás kriptográfiai környezettől,[190] így fennáll az alapvető jog fokozottabb korlátozásának látens lehetősége is.

Az Nbtv. és Be. szerinti általános törvényi szabályozás alapján megkülönböztethető a külső engedélyhez kötött és nem kötött titkos információgyűjtés, amely engedélyeztetési folyamatot az LI tekintetében a jogalkotó a kommunikáció tartalmának megismerése/megismerésének lehetősége mentén határolt el, mely esetben az alapjog korlátozás szempontú megközelítés erőteljesen érvényesül. Külső engedélyezőnek minősül az Nbtv. 56. § (1) - (2) bek. alapján a bíró és az igazságügy miniszter, valamint a Be. 214. § (4) bek. alapján büntetőeljárás során az ügyész és a bíró.[191] Az Nbtv. 54. § (1) bek. j) pontja és a Be. 215. § (9) bek. szerint a jogosult külső engedély nélkül, saját kezdeményezésre végezheti az első tevékenységi körrel érintett kommunikáció kísérő-, metaadataihoz való hozzáférést. A második esetben az Nbtv. 56. (1) bek. d) pontja és a Be. 232. § (5) bek. – szerinti „lehallgatás" során – a jogosult külső engedély birtokában elektronikus hírközlési szolgáltatás keretében elektronikus hírközlő hálózat vagy eszköz útján, illetve információs rendszeren folytatott kommunikáció tartalmát titokban megismerheti és rögzítheti. *„Az elektronikus kommunikáció tartalmának megismerése a magánszférát érintő szinte valamennyi jogot korlátozza, úgymint a magánélet, a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához, továbbá a személyes adatok védelméhez kapcsolódó jogot*."[192] Így annak alkalmazása csak a demokratikus kontrollmechanizmusok érvényesülése mellett történhet. A harmadik esetben az Nbtv. 56. § (1) bek. e) pontja és a Be. 232. § (1) bek. a jogosult számára – információs rendszer titkos megfigyelése során – biztosítja

[190] *A Nemzeti Adatvédelmi és Információszabadság Hatóság hivatalból indított vizsgálatának megállapításai a „Pegasus" kémszoftver Magyarországon történő alkalmazásával összefüggésben (NAIH-423-2/2022.)*. NAIH. 2022.01.31. 31-32. Online: https://www.naih.hu/adatvedelmi-jelentesek/file/486-jelentes-a-nemzeti-adatvedelmi-es-informacioszabadsag-hatosag-hivatalbol-inditott-vizsgalatanak-megallapitasai-a-pegasus-kemszoftver-magyarorszagon-torteno-alkalmazasaval-osszefuggesben (Letöltés ideje: 2024. február 20.)

[191] Az Nbtv. szerinti titkos információgyűjtés, a Be. szerinti leplezett eszköz és az egyes ágazati törvények (Ütv., Rtv., NAV tv.) szerinti titkos információgyűjtés engedélyezéséi rendszerének magyarázatát lásd: 32/2021. NVB határozat III. fejezet. Online: https://www.valasztas.hu/hatarozat-megjelenito/-/hatarozat/32-2021-nvb-hatarozat-a-hajnal-miklos-maganszemely-altal-benyujtott-orszagos-nepszavazasi-kezdemenyezes-targyaban (Letöltés ideje: 2024. február 18.)

[192] BABOS Sándor (2020): Az alapvető jogok korlátozása a nemzetbiztonsági tevékenység során II. *Nemzetbiztonsági Szemle*, 8(4), 54. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/5008/4313 (Letöltés ideje: 2024. február 18.)

az információs rendszeren kezelt adatok leplezett megismerését és rögzítését. Az NBSZ közreműködésével végrehajtott LI során a külső engedély beszerzéséért, valamint a belső engedély megadásáért a megrendelő szerv felelős, míg az „*NBSZ az eszközalkalmazás, a szolgáltatás szakszerűségéért felelős.*”[193] A NAIH az NBSZ-nél megtartott adatvédelmi auditja alapján megállapította, hogy „*a végrehajtás törvényességének biztosítása a szakszolgálatnál olyan fontos szempont, amelyet a szervezet akár a megrendelő szervezettel szemben is érvényesít. […] a szakszolgálat olyan előzetes adminisztratívellenőrzési rendszert épített ki, amely előzetesen kiszűri azokat a megrendeléseket, amelyek törvénysértőek lehetnek.*”[194]

A fentiekben áttekintésre került az LI hazai általános szabályozása, amely a tevékenységgel érintett kommunikáció kísérő, metaadatainak hozzáférésétől, a tartalom megismeréséig terjed, akár hálózati oldalon, akár végponti eszközön történik az LI végrehajtása. A végrehajtás szabályozása összefonódik az alapvető jog szükséges és arányos korlátozásának kritériumára épülő transzparens törvényi szintű engedélyezési eljárásrenddel, amely a demokratikus működés biztosítása érdekében megköveteli az igazságügyi kontroll funkciót a végrehajtás felett, így érvényesítve az LI során a hatalmi ágak megosztását. A külső engedélyhez kötött titkos információgyűjtés, így az LI engedélyezése kapcsán indokolt kitekinteni az EJEB 2016. január 12-ei Magyarországot elmarasztaló ítéletére[195] (a továbbiakban: Ítélet). Ez alapján Magyarország megsértette az EJEE 8. cikk (1) bekezdést, tekintettel azon dilemmára, miszerint „*a végrehajtó hatalmon belüli [nemzetbiztonsági célú titkos információgyűjtés igazságügyminiszteri szintű] engedélyezés megfelelő-e a magánszféra védelme szempontjából*.” A 32/2013. (XI.22.) Alkotmánybírósági határozat[196] figyelembe véve az EJEB ítélkezési gyakorlatát kimondja, „*minthogy a titkos információgyűjtés szükségképpen kizárja a hatékony jogorvoslat lehetőségét, […]. Minderre tekintettel az alkalmazást három szakaszból álló ellenőrzésnek kell alávetni: amikor a beavatkozást elrendelik, mialatt a beavatkozást végrehajtják, miután a beavatkozást befejezték. Az ellenőrzést a végrehajtó hatalomtól független testületeknek kell végezni. Elsősorban az állandó, folyamatos és kötelező ellenőrzés*

[193] BODA 2012: 126; Nbtv. 61. § (1)

[194] *NAIH: a Nemzetbiztonsági Szakszolgálat alkotmányos módon működik*. NBSZ. 2017. Online: https://nbsz.gov.hu/tevekenyseg-mukodes/kulso-vizsgalatok-ellenorzesek/naih (Letöltés ideje: 2024. február 20.)

[195] 37138/14. sz. EJEB ítélet, 2016. január 2-án: Szabó és Vissy kontra Magyarország. Online: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]} (Letöltés ideje: 2024. február 20.)

[196] 32/2013. (XI. 22.) AB határozat a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 58. § (3) bekezdésével kapcsolatos alkotmányos követelmény megállapításáról és alkotmányjogi panasz elutasításáról. ABH 2012/23. 1176. Online: http://www.kozlonyok.hu/kozlonyok/Kozlonyok/1/PDF/2013/22.pdf (Letöltés ideje: 2024. február 20.)

a garancia arra, hogy a konkrét ügyekben nem sértik meg az arányosság követelményét".[197] A fenti dilemma feloldása érdekében a Belügyminisztérium részéről ugyan történtek az Nbtv. módosításra irányuló előkészületek, de érdemi jogalkotás nem. A NAIH elnökének alkotmányossági-kritérium szempontú javaslata értelmében „*A külső kontroll függetlensége és a közjogi–hatalommegosztási elvek szempontjából kifogástalan megoldást eredményezne, ha a jelenleg az igazságügyért felelős miniszterhez tartozó külső engedélyezési hatáskör a bírósághoz kerülne*."[198] Azonban, ha kompetencia-kritériumok szempontjából vizsgáljuk a kérdést, megállapítható, hogy az engedélyezés „*bíró felkészültséget, de nem feltétlenül aktuális bírói státuszt jelent.*"[199] A titkos információgyűjtés külső engedélyezésének utólagos kontrollja tekintetében a NAIH az Alaptörvényben rögzített rendeltetéséből, valamint Infotv. szerinti feladat- és hatásköréből adódóan megállapította annak megfelelő érvényesülését, hiszen „*Az utólagos kontroll garanciális szerepének erősítését az Infotv. módosítása tette lehetővé, amely alapján a Hatóság [a NAIH] a titkos információgyűjtésekkel kapcsolatban hivatalból is indíthat vizsgálatot.*"[200] Ezen felül az Nbtv. 15. – 19/A §-ai alapján az Országgyűlés Nemzetbiztonsági Bizottsága ellátja a nemzetbiztonsági szolgálatok – így azok LI – tevékenységének a törvényességi, parlamenti ellenőrzését.[201]

Ezen a ponton érdemes kitekinteni az LI tevékenységet is magában foglaló összesített, külső igazságügyi miniszteri engedélyhez kötött nemzetbiztonsági célú titkos információgyűjtés/ az arra irányuló kérelmek mennyiségi alakulására a 2015. január 01. - 2023. április 25. között az alábbi 4. ábra szerint:

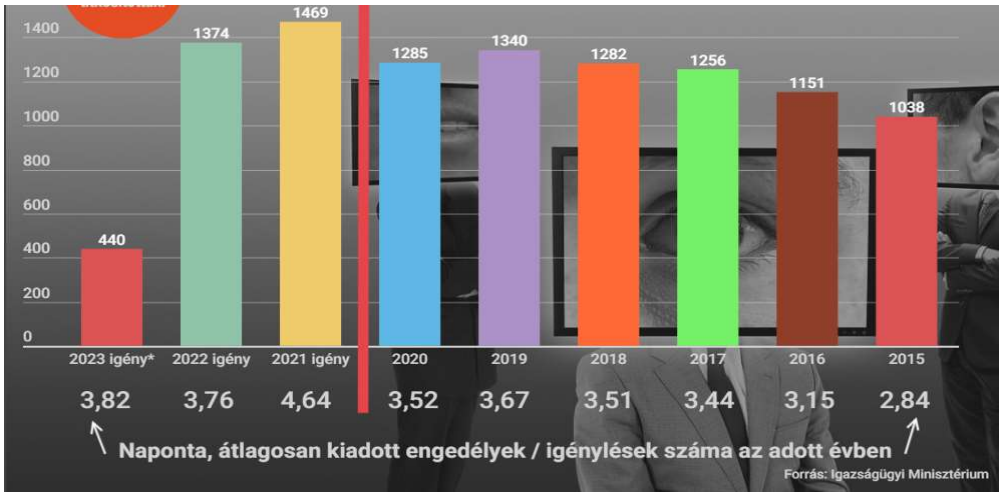
[197] Lásd: SABJANICS István (2017): Az Alkotmánybíróság határozata a bírák nemzetbiztonsági ellenőrzéséről: A jogállamiság gyakorlati értelmezésének két konkuráló oldala. *Jogesetek magyarázata*, 8(4), 19-24.

[198] PÉTERFALVI Attila (2022): *A magánszféra védelme a nemzetbiztonsági célú titkos információgyűjtés során*. Habilitációs tézisek. Budapest: PPKE JÁKDI. 10. Online: https://jak.ppke.hu/storage/tinymce/uploads/old/uploads/articles/2198023/file/Peterfalvi_Attila_habilitacios_tezis.pdf (Letöltés ideje: 2024. február 20.)

[199] DR. BARNÓCZKI László (2019): *Az elszakított testvérek, avagy a titkosszolgálati eszközök hazai szabályozásának lehetséges fejlődési irányai a legújabb kori adatvédelmi jogfejlődés tükrében*. Budapest: ELTE JTI. 24.

[200] PÉTERFALVI 2022: 10

[201] Továbbá a nemzetbiztonsági szolgálatok pénzügyi, gazdasági ellenőrzését az Állami Számvevőszék, illetve a Kormányzati Ellenőrzési Hivatal látja el.



4. ábra: Külső igazságügyi miniszteri engedélyhez kötött nemzetbiztonsági célú titkos információgyűjtés/ az arra irányuló kérelmek mennyiségi alakulása 2015. január 01. - 2023. április 25. között. (Szerk.: A forrás[202])

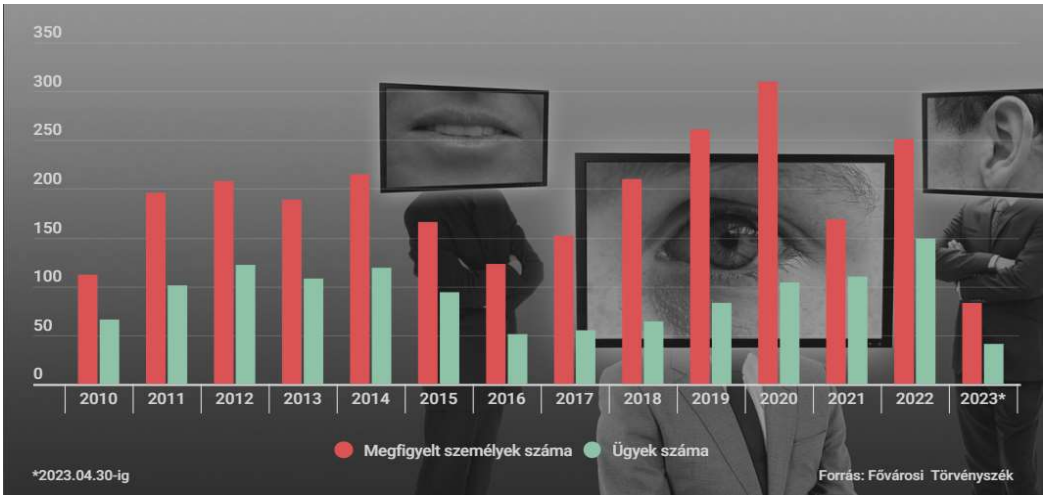
Az Igazságügyi Minisztérium közérdekű adatszolgáltatásán alapuló fenti sajtóközleményben publikált statisztikai adatok alapján megállapítható, hogy a külső igazságügyi miniszteri engedélyhez kötött nemzetbiztonsági célú titkos információgyűjtő eszközök alkalmazására megadott engedélyek (a továbbiakban a részfejezetben: IM TIGY engedély)/ vagy az arra irányuló kérelmek száma 2015 – 2023 között egy rendkívül lapos exponenciálisan növekvő tendenciát mutat, melyben 2020-ban volt egy kisebb visszaesés. A 2016 és 2022 között kiadott nemzetbiztonsági célú IM TIGY engedélyek átlagos emelkedési rátája kiszámolható, amely kerekített értéke +1,7%/év. Ez azt jelenti, hogy 2030-ra kerekítve 1572 nemzetbiztonsági célú IM TIGY engedély kiadása lesz prognosztizálható, amely 198 engedéllyel több, mint 2022-ben. (Levezetés: 5 ábra.)

Év	Becs. engedély/év	Évi becs. növekmény
2022	1374	23,4
2023	1397	23,7
2024	1421	24,2
2025	1445	24,6
2026	1470	25,0
2027	1495	25,4
2028	1520	25,8
2029	1546	26.2
2030	1572	26,7

5. ábra: Nb. célú IM TIGY engedélyek száma 2022-2030. (Szerk.: A szerző)

[202] *Idén tavaszig már 440 titkos megfigyelési igény került Varga Judit elé, de már azt is titkosították, hogy ebből hányat engedélyeztek* HVG.hu. 2023. Online: https://hvg.hu/itthon/20230604_Titkos_megfigyelesek_Varga_Judit_titkositas_nemzetbiztonsag_igazsagugyi_miniszterium_engedely (Leöltési ideje: 2024. február 18.)

A külső bírói engedélyhez kötött nemzetbiztonsági célú titkos információgyűjtésre irányuló kérelmek mennyiségi alakulására is érdemes kitekinteni a 2010. január 01. - 2023. április 30. között az alábbi 6. ábra szerint:



6. ábra: Külső bírói engedélyhez kötött nemzetbiztonsági célú titkos információgyűjtés/ az arra irányuló kérelmek mennyiségi alakulása 2010. január 01. - 2023. április 30. között. (Szerk.: A forrás[203])

A Fővárosi Törvényszék közérdekű adatszolgáltatásán alapuló fenti sajtóközleményben publikált statisztikai adatok alapján megállapítható, hogy a külső bírói engedélyhez kötött nemzetbiztonsági célú titkos információgyűjtő eszközök alkalmazása (a továbbiakban a részfejezetben: bírói TIGY)/ vagy az arra irányuló kérelmek száma 2010 – 2023 között mind az ügyek, mind az érintett (cél)személyek száma tekintetében egy polinomiálisan változó tendenciát mutatott, azonban a 2016-ot követő időszakban egy laposabb exponenciálisan növekvő tendenciát realizál. A 2016 és 2022 között kiadott nemzetbiztonsági célú bírói TIGY engedélyek átlagos emelkedési rátája kiszámolható, amely kerekített értéke +6,1%/év. Ez azt jelenti, hogy 2030-ra kerekítve 239 nemzetbiztonsági célú bírói TIGY engedély kiadása lesz prognosztizálható, amely 90 engedéllyel több, mint 2022-ben. (Levezetés: 7 ábra.)

Év	Becs. ügy/év	Évi becs. növekmény
2022	149	9,1
2023	158	9,6
2024	168	10,2
2025	178	10,8
2026	188	11,5
2027	200	12,2
2028	121	12,9
2029	225	13,7
2030	239	14,6

7. ábra: Nb. célú bírói TIGY ügyek száma 2022-2030. (Szerk.: A szerző)

[203] *Havonta 20 személy titkos megfigyelésére adtak bírói engedélyt idén*. HVG.hu. 2023. Online: https://hvg.hu/itthon/20230613_Havonta_20_szemely_titkos_megfigyelesre_adtak_biroi_engedelyt_iden (Leöltési ideje: 2024. február 18.)

A 4. és 6. ábra adatain alapuló integrált tendenciaelemzés szerint 2020-ban megállapítható egy erőteljes eltérés a két engedélytípus között, miszerint míg az IM TIGY tekintetében visszaesés volt tapasztalható, addig a bírói TIGY tekintetében a legmagasabb számú volt a titkos információgyűjtéssel érintett (cél)személyek száma. Továbbá míg az IM TIGY engedélyek száma 2021-ben volt a legmagasabb, addig a bírói TIGY a (cél)személyek vonatkozásában majdnem 50%-os visszaesést produkált, míg az ügyek számában lineárisan tovább nőt. Azonban mind az IM TIGY, mind a bíró TIGY engedélyek/ügyek összesített mennyiségének tekintetében a 2016-ot követő időszakban megállapítható, hogy azok egy rendkívül lapos exponenciálisan növekvő tendenciát mutatnak. A 2016 és 2022 között kiadott összesített IM és bírói TIGY engedélyek/ügyek mennyiségének lapos exponenciális emelkedési rátája kiszámolható, amely kerekített értéke +3,9%/év. Ez azt jelenti, hogy 2030-ra kerekítve összesen 1811 IM és bírói TIGY engedély kiadása/ ügy elrendelése lesz prognosztizálható, amely 288 engedéllyel több, mint 2022-ben. (Levezetés: 5. és 7. ábra.) Látható, hogy az IM TIGY engedélyek száma 2022-ben 1225-tel volt több, mint a bírói TIGY ügyek száma, mely azt is jelzi, hogy a 2.1. alfejezetben ismertettek alapján a külső engedélyhez kötött nemzetbiztonsági célú tevékenység vonatkozásában a nemzetbiztonsági ügyjelleg a domináns a „bűnüldözési" jelleggel szemben.

A részfejezetben elvégzésre került az LI szervezetrendszerének és általános szabályozásának tartalmi elemzése annak keretében az egyes résztevékenységek azonosítása, a külső engedélyezést szabályozó főbb normák vizsgálata, és a nemzetbiztonsági célú LI kapcsán felmerülő miniszteri szintű engedélyezési dilemma vizsgálata. Továbbá elvégzésre került a miniszteri és bíró engedélyhez kötött nemzetbiztonsági/ vagy bűnüldözési célú titkos információgyűjtésre vonatkozó közérdekű adatszolgáltatás alapú statisztikai adatok trend- és tendenciaelemzése a (2010 -) 2015.Q1. – 2023.Q1. időszakban, mely alapján megállapítható, hogy mind az igazságügyi miniszter által engedélyezett, mind a bírói engedélyen alapuló nemzetbiztonsági célú titkos információgyűjtés mennyiségének tekintetében a 2016-ot követő időszakban azok egy rendkívül lapos exponenciálisan növekvő tendenciát mutatnak. 2030-ra becsülten kerekítve összesen 1811 IM és bírói TIGY engedély kiadása/ ügy elrendelése lesz prognosztizálható, amely 288 engedéllyel több, mint 2022-ben. A fentiek okán szükséges a titkos információgyűjtés keretében érvényesülő egyes LI módszerek és eljárások szakmai, szakirodalmi jellegű vizsgálata is dokumentum-, tartalomfeldolgozás keretében.

2.5.3. *Az LI szakirodalom szerinti módszerei és eljárásai*

Az LI tekintetében a fenti általános törvényi szabályozásnak megfeleltetve az alábbi 4+1 fő módszer, eljárás különböztethető meg a feldolgozott szakirodalom alapján:

- technikai módszerek
  - közbeékelődéses ellenőrzés (MitM[204]),
  - aktív ellenőrzőeszköz (spyware – kémprogram),
  - passzív mély csomagvizsgálat (DPI),
- szolgáltatói együttműködés.[205]

+ „hamis zászlós" művelet

Tekintettel arra, hogy a fenti technikai módszereket és a szolgáltatói együttműködést szakirodalmi szempontból számos szerző feldolgozta[206] mélységében nem kerülnek kifejtésre jelen alfejezetben, csak néhány releváns aktualitás, a közérthetőséget elősegítő összefüggés kerül bemutatásra. A szolgáltatói együttműködés LI szempontú vizsgálata (normatív, szakirodalmi) az értekezés későbbi fejezeteiben központi téma, így az részletesebben a későbbiek során kerül kifejtésre. A „hamis zászlós" művelet, mint új, innovatív módszer a jelen doktori értekezésben bevezetett résztevékenység, amely részletesen kifejtésre és bizonyításra került az alfejezetben.

Mély csomagátvizsgálás (DPI):

A szakirodalom alapján a DPI három fő altípusa különböztethető meg: a kibervédelem[207], a hírközlési szolgáltatások blokkolása[208], valamint az értekezés szempontjából releváns és

---

[204] MitM: Man-in-the-Middle attack – közbeékelődéses „támadás", ellenőrzés. Lásd: THANKAPPAN, Manesh - RIFA-POUS, Helena - GARRIGUES, Carles (2022): Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review. *Expert Systems with Applications*, (210). Online: https://doi.org/10.1016/j.eswa.2022.118401 (Letöltés ideje: 2024. február 15.)

[205] KOVÁCS 2015: 159.

[206] Lásd: BERTA Sándor (2006): *Online házkutatásokat indítanának Németországban*. SG.hu Online: http://sg.hu/cikkek/49079/online_hazkutatasokat_inditananak_nemetorszagban (Letöltés ideje: 2024. február 15.); DAJKÓ Pál (2011): *Lebukott az állami kémprogram*. ITCoffe.hu. Online: http://itcafe.hu/hir/chaos_computer_club_nemetorszag_bundestrojaner.html (Letöltés ideje: 2024. február 15.); KOVÁCS Zoltán (2021): *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai*. Budapest: Ludovika Egyetemi Kiadó. 12-142.; KOVÁCS 2015: 158-171.

[207] Lásd: BIBALBENIFA, J.V. - KRISHNANN, Saravanan – LONG, Hoang Viet, - KUMAR, Raghvendra – Taniar, David (2021): *Performance Analysis of Machine Learning and Pattern Matching Techniques for Deep Packet Inspection in Firewalls*. Online: https://doi.org/10.21203/rs.3.rs-260788/v1 (Letöltés ideje: 2024. február 15.)

[208] Lásd: *Preliminary findings on traffic management practices in Europe show that blocking of VoIP and P2P traffic is common, other practices vary widely*. BEREC. 2012. 8-9.; 22. Online: https://www.berec.europa.eu/sites/default/files/files/document_register/2012/7/BoR12_30_tm-snapshot.pdf (Letöltés ideje: 2024. február 15.)

egyben az ENSZ Nemzetközi Távközlési Egyesülete (a továbbiakban: ITU[209]) által is szabványosított[210] elektronikus hírközlő hálózaton kezelt adatfolyam passzív (törvényes) ellenőrzése[211], monitoringja, azaz a hírközlési LI résztevékenység. A hírközlési LI esetén „*a csomagok vizsgálata alapján dönthető el, hogy az az ellenőrzést végző számára érdekes-e (például adott célszemélyhez tartozik-e az e-mail), vagy sem. Itt a szűrés azonban nem a kiválasztott csomagok blokkolását szolgálja, hanem azoknak az ellenőrzést végző szolgálathoz (is) történő eljuttatását*."[212] A harmadik DPI altípus szerinti LI a hivatkozott szakirodalom és szabvány alapján megvalósulhat az elektronikus hírközlő hálózat központi(core)rendszerén, az elektronikus hírközlési szolgáltató és az LI-re jogosult szervezet együttműködése keretében kialakított központi monitoring alrendszer útján. A módszer a szakirodalom alapján lehetővé teszi a hírközlési hálózaton megjelenő, azon kezelt kommunikációs forgalom kicsatolását, így annak feldolgozását a jogosult LI szervezet által, a titkos információgyűjtés garanciális szabályainak, az alapelvek[213] betartása mellett.[214] A közleményellenőrzési módszer lényege, hogy a kommunikáció tartalmához és kísérő-/metaadataihoz a személyes adat, a közlemény technikai kriptográfiai védelmétől mentes, rejtjelezetlen formában férjen hozzá a jogosult szerv[215], azonban ha ez nem biztosított, szükséges rejtjelfejtés alkalmazása a feldolgozást megelőzően. A kérdéskörből adódó kihívások szintén központi témája az értekezésnek, így annak technológiai és normatív vizsgálatára a későbbiekben kerül sor. Az értekezés szempontjából a központi hálózati monitoring DPI módszer bír relevanciával, mely egyidejűleg

[209] ITU: International Telecommunication Union - Nemzetközi Távközlési Egyesület

[210] Y.2770: Requirements for deep packet inspection in next generation networks. Online: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2770-201211-I!!PDF-E&type=items (Letöltés ideje: 2024. február 15.)

[211] *Next-Generation Deep Packet Inspection*. Leipzig: Rohde &Schwarz GmbH. 2023. Online: https://www.ipoque.com/media/brochures/Solution_guide_en_DPI_3608-7309-62_v0200_144dpi.pdf (Letöltés ideje: 2024. február 15.)

[212] KOVÁCS 2015: 166

[213] Arányosság és szükségesség, célhozkötöttség, készletező adatgyűjtés/ adatkezelés tilalma. Lásd: 32/2013. (XI. 22.) AB határozat a Rendőrségről szóló 1994. évi XXXIV. törvény 7/E. § (3) bekezdésével összefüggésben benyújtott alkotmányjogi panaszról. ABH 2013/924. Online: https://public.mkab.hu/dev/dontesek.nsf/0/16E8FCEE21074786C1257ADA00524AC5?OpenDocument (Letöltés ideje: 2024. február 15.); PÉTERFALVI 2013.

[214] Ennek ismert egyedi, mobil módja is, mikor a „közbeékelődés" nem az elektronikus hírközlő hálózat oldalán kerül bevezetésre a kommunikáló felek között, hanem egyedi jelleggel, kvázi mobil bázisállomást imitálva („IMSI cather", azaz elfogó), de ez már MitM jellegű ellenőrzés a hivatkozott szakirodalom alapján. IMSI: International Mobile Subscriber Identity - nemzetközi mobil-előfizetői azonosító: A SIM-kártya egyedi azonosítója, az előfizető azonosítására és a hálózaton való hitelesítésére szolgál. Az IMSI elfogó használatára a feldolgozott szakirodalom alapján elsőként 1993-ban a német Rohde & Schwarz cég részéről került sor. Lásd: FEDERRATH, Hannes (1999): Protection in Mobile Communications. In MÜLLER, Günter – RANNENBERG, Kai (szerk.): *Multilateral Security in Communications*. Harlow, Essex: Addison-Wesley-Longman, 349-364. Online: https://epub.uni-regensburg.de/7382/1/Fede3_99Buch3Mobil.pdf (Letöltés ideje: 2024. február 15.)

[215] HORTEN, Monica (2012): *The ITU's DPI standard - that's something to be afraid of!*. IPTegrity. Online: https://www.iptegrity.com/index.php/telecoms-package/net-neutrality/827-the-itus-dpi-standard-thats-something-to-be-afraid-of (Letöltés ideje: 2024. február 15.)

nagy mennyiségű azonosító, közlemény ellenőrzését teszi lehetővé,[216] a monitoring alrendszer kialakítási és üzemeltetési költségeit akár az elektronikus hírközlési szolgáltatóra hárítva.

Aktív ellenőrzőeszköz (spyware – kémprogram):

Az aktív ellenőrzés során a célszemély IKT eszközére egy az LI szervezet által felügyelt speciális szoftver kerül konspiráltan telepítésre, mely sok hasonlóságot mutat a kártékony szoftverekkel, de ebben az esetben ez nemzetbiztonsági vagy bűnüldözési érdeket szolgál. Kovács Zoltán szerint „*Talán azt az analógiát lehetne erre alkalmazni, mint amikor egy lőfegyverről beszélünk, amely más értelmet nyer egy bűnöző és mást egy rendőr kezében*."[217] Az eljárás az Nbtv. 56. § (1) bek. e) pontja és a Be. 232. (1) bek. szerinti LI résztevékenységnek feleltethető meg. A jogszabályok gyakorlati alkalmazása során 2021/22-ben napvilágot látott a „Pegasus-esetben" elhíresült kémszoftver működési elve, mellyel kapcsolatos hazai vizsgálatról, és alkalmazásának jogszerűségéről a NAIH publikálta is vizsgálatának nyilvános megállapításait.[218] Ezen eszközök képesek az online kommunikáció, és a már begépelt még rejtjelezetlen tartalom elfogására, a kísérő- és metaadatok kinyerésére, a háttértárban található adatok megszerzésére. Ezt követően az adatokat megküldik az LI-re jogosult aktív ellenőrző eszköz alkalmazójának.[219] A módszer alkalmazásának hátránya tekintettel arra, hogy szoftverről van szó, így annak alkalmazása véges, jóval szűkebb, mint a központi monitoringé.

Szolgáltatói együttműködés:

Ezen jogilag szabályozott tevékenységikörben eljárva az LI-re jogosult szervezet nem technikai LI útján, hanem a szolgáltató által kezelt, az LI-vel értintett célszemély kommunikációját tartalmazó adatokat, valamint annak kísérő- és metaadatait a LI-re jogosult szervezet jogszabályalapú megkeresése, adatkérése esetén adja át. Ezen eljárás az értekezés során vizsgálandó egyik központi témakör, kiemelten a hazai szabályozására és a nemzetközi együttműködés lehetőségeire.

---

[216] KOVÁCS Zoltán (2016): Biztonság vs. törvényes ellenőrzés az internet alapú kommunikációban - ellentétes vagy egymással megférő követelmények? I. *Hadmérnök*, 11(4), 137. Online: http://hadmernok.hu/164_11_kovacs.pdf (Letöltés ideje: 2024. február 20.)

[217] Kovács 2021: 130

[218] *A Nemzeti Adatvédelmi és Információszabadság Hatóság hivatalból indított vizsgálatának megállapításai a „Pegasus" kémszoftver Magyarországon történő alkalmazásával összefüggésben (NAIH-423-2/2022.)*. NAIH. 2022.01.31.

[219] MARQUIS-BOIRE, Morgan – MARCZAK, Bill – GUARNIERI, Claudio – SCOTT-RAILTON, John (2013): *For their eyes only - The Commercialization of Digital Spying*. Citizen Lab and University of Toronto. Online: https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf (Letöltés ideje: 2024. február 15.); GOLOVANOV, Sergey (2013): *Spyware. HackingTeam*. SecureList. Online: http://securelist.com/analysis/publications/37064/spyware-hackingteam (Letöltés ideje: 2024. február 15.)

„Hamis zászlós" művelet:

A technológiai adatvédelmi eljárások, elsősorban a kriptográfia fejlődése korlátozza az LI alkalmazásának hatékonyságát, mely hatására a nyilvánosságra hozott információ alapján az FBI és az Europol sajtóközleményei szerint 2019 óta az FBI[220] az Europollal, és az ausztrál Szövetségi Rendőrséggel szoros együttműködésben a „Trójai Pajzs" nemzetközi bűnüldözési akció[221] keretében kifejlesztette és rejtetten üzemeltette, „elterjesztette" a tevékenységével érintett célszemélyek körében a „lehallgathatatlannak" titulált ANOM csevegőalkalmazást, azaz alkalmazásszolgáltatást. Az ANOM igénybevételével zajló bűnös online kommunikáció tartalmához LI kertében a bűnüldöző szervek rejtjelezetlen formában hozzáfértek, így kijátszva a piaci alkalmazásszolgáltatások kriptográfiai kihívásait. Az ANOM több mint 12.000 titkosított IKT eszközt szolgált ki, több mint 300 bűnszervezet vonatkozásában, amelyek több mint 100 országban működtek/-nek világszerte. Az új platform célja az volt, hogy megcélozza a globális szervezett bűnözést, a kábítószer-kereskedelemmel és pénzmosással foglalkozó szervezeteket, függetlenül működési területüktől. Az FBI és a nemzetközi koalíció további 16 országa, köztük Magyarország, az Europol támogatásával és DEA[222]-val együttműködve a megszerzett 27 millió üzenetből származó információkat 18 hónapon keresztül dolgozta fel.[223] *Nem volt azonban egyszerű feladat egy ilyen rendszer működtetése. Egy, az akcióban részt vett ügyész szerint egy komplett, a bűnözők szemében is hiteles vállalkozást kellett létrehozniuk, ügyfélszolgálattal, technikai támogatással, sőt a hacker támadások ellen is védekezniük kellett.*"[224] A „Trójai Pajzs" akció során látókörbe került LI módszer álláspontom alapján forradalmi, hiszen az FBI nemzetközi multilaterális bűnüldözési célú együttműködés keretében piaci termékként a kiemelt transznacionális szervezett bűnözői körökben elterjesztette a „feltörhetetlenül titkosítottnak" titulált ANOM alkalmazásszolgáltatást, amelyen folyó kommunikáció rejtjelezetlen tartalmához konspirált technikai LI módszerrel hozzáfért. Az így szerezett információk feldolgozását követően a bűnüldözési koalíció globális méretű csapást

[220] FBI: Federal Bureau of Investigation - Szövetségi Nyomozóiroda.
[221] Operation Trojan Shield – Trójai Pajzs Művelet
[222] DEA: Drug Enforcement Administration – Kábítószerellenes Hivatal
[223] *FBI Targets Encrypted Platforms Used by Criminal Groups - Global partners announce results of innovative Operation Trojan Shield.* FBI. 2021.*; 800 criminals arrested in biggest ever law enforcement operation against encrypted communication.* Europol. 2021. Online: https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication (Letöltés ideje: 2024. február 15.); Lásd: *Telefonos csapdával csípett nyakon az FBI több száz bűnözőt*. NBSZ NKI. 2021. Online: https://nki.gov.hu/it-biztonsag/hirek/anom-az-fbi-telefonos-csapdaja-ami-nagyot-szolt/ (Letöltés ideje: 2024. február 15.); *FBI-EUROPOL-KR NNI – ANOM adatok alapján számolták fel a hálózatot*. Police.hu. Online: https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/fbi-europol-kr-nni-anom-adatok-alapjan-szamoltak (Letöltés ideje: 2024. február 15.)
[224] *Telefonos csapdával csípett nyakon az FBI több száz bűnözőt*. NBSZ NKI. 2021.

mért a transznacionális szervezett bűnözésre. [225] Álláspontom alapján, részkövetkeztetésként megállapítható, hogy indokolt a „hamis zászlós" eljárás új, innovatív LI módszerként történő tudományos rendszertani besorolása, annak tudományos kutatómunkában történő vizsgálata.

2.6. Az LI információelméleti háttere és annak átültetése a normatív környezetbe

Az alfejezet érdemi tárgyalását megelőzően a közérthetőség érdekében szükséges az információ fogalmi áttekintése. Maga az információ tartalomból (primer) és kísérő-, metaadatból (szekunder) áll. Tartalomnak minősíthető minden, ami a kommunikáció eredménye, azaz közlemény, vagy az adatok egyéb strukturált formája, például egy tárolt dokumentum.[226] Az LI szempontjából – a jogszabályok tárgyi hatályának megértése érdekében – szükséges a kommunikációs tartalom[227] fogalmát kiterjesztetten értelmezni már a chatfelületre, levelezőkliensbe begépelt-bediktált szövegre, bemásolt linkre, beemelt adatra (például kép, egyéb multimédiás üzenet) is. Az elektronikus információs tartalmak, adatok kezelésével kapcsolatosan, illetve a tartalomra vonatkozóan egyedi azonosító adatok keletkeznek, melyek lehetnek leíró és adminisztratív jellegűek. Ezen leíró-, metaadatok köre jóval bővebb, mint az elektronikus hírközlési szolgáltatáshoz kapcsolódó kommunikációs kísérőadatok köre[228], hiszen minden elektronikus információs rendszer végzett adat-, tartalomkezelési művelet, vagy annak alkalmazásával nyújtott szolgáltatás tekintetében létrejönnek. Az ISO[229] 15489-1:2016 (Információ és dokumentáció — Iratkezelés) szabvány alapján a metaadat olyan adat, amely a nyilvántartott iratok kontextusát, tartalmát, szerkezetét és kezelését írja le, strukturált vagy félig strukturált információ, amely lehetővé teszi rekordok létrehozását, kezelését és használatát egy időben, tartományokon belül és tartományok között.[230] Az adat *„hozzáadott, ismerettöbblet-érték (információérték) nélküli tényező, jelenség, amely akkor válik információvá, vagyis ismerettöbbletté, amikor az érték nélküli állapotában változás áll be, aminek leggyakoribb*

[225] A humán és a technikai titkos információgyűjtő képességek integrált alkalmazásával kapcsolatban lásd: DOBÁK – TÓTH 2022

[226] SYI (2018): Az adatkor hajnalán. *Jel-kép*, 7(1), 24. Online: https://communicatio.hu/jelkep/2018/1/JelKep_2018_1_Syi.pdf (Letöltés ideje: 2024. február 20.)

[227] A kommunikációs tartalom aktuálisan ember-ember, esetleg ember-gép között értelmezhető információgyűjtő szempontból, azonban a technológiai fejlődés által kialakuló autonóm, intelligens rendszerek, robotok, a mesterséges intelligencia térnyerése várhatóan magával fogja hozni az M2M kommunikáció nemzetbiztonsági, bűnüldözési célú ellenőrzésének exponenciálisan fokozódó igényét is, például az újgenerációs infokommunikációs hálózatok, az okos városok, okos járművek fokozódó kialakulása, elterjedése során.

[228] Ekertv. 13/B. § (2) bek.-ben taxatíve felsorolva.

[229] ISO: International Organization for Standardization – Nemzetközi Szabványügyi Testület

[230] *ISO 15489-1:2016 Information and documentation — Records management*. International Organization for Standardization. 3.12. Online: https://www.iso.org/obp/ui/#iso:std:iso:15489:-1:ed-2:v1:en (Letöltés ideje: 2024. február 19.)

viszonyítási alapja önmaga, vagyis az alap vagy kiindulási adat."[231] Az LI szempontjából releváns mind a kommunikációs tartalom – és a kezelt adat –, mind a kísérő- és metaadatok ellenőrzése is, hiszen a fentiek alapján az információ felosztható a tartalomra és a tartalom egyedi azonosítására, vagy annak kezelésére vonatkozó adatokra. Ezen adatkörök jellemzése és egymástól való elhatárolás a tudományos szakirodalom feldolgozásán túl a hazai szabályozás alapján kerül elvégzésre, tekintettel arra, hogy a kommunikáció tartalma, valamint a kísérő- és metaadat fogalomköre eltér a jogforrásokban az elektronikus hírközlési, és az alkalmazásszolgáltatás vonatkozásában.

Annak érdekében, hogy az értekezés célkitűzései megvalósíthatóak legyenek jelen alfejezetben szükséges az elektronikus hírközlési- és az alkalmazásszolgáltatás fogalmi és normatív elhatárolása, a videómegosztóplatform- és lekérhető médiaszolgáltatások elhatárolása az alkalmazásszolgáltatástól, az alkalmazásszolgáltatás fogalmának, rendszertani besorolása alakulásának vizsgálata az EU digitális stratégiai célkitűzései aspektusából, a kommunikáció és a kommunikációs tartalom fogalmának értelmezése a kapcsolódó jogszabályok alapján, illetve a kísérő- és metaadat fogalmának elhatárolása a kapcsolódó jogforrások és kutatási eredmények alapján.

2.6.1. Az elektronikus hírközlési szolgáltatás tartalmi és normatív elhatárolása az alkalmazásszolgáltatástól

A terminológiák (kommunikáció, tartalom, kísérő- és metaadat) rendszertani besorolása és tartalmi értelmezése érdekében szükséges egymástól elhatárolni az elektronikus hírközlési szolgáltatás és az alkalmazásszolgáltatás keretében végbemenő kommunikációt. Itt is érdemes a tágabb fogalomtól a szűkebb felé haladni a definiálás során. Az elektronikus hírközlési szolgáltatás[232] tárgyú tevékenységeket az Eht. szabályozza. Lényegében az értekezés szempontjából ezen körbe tartozó legjelentősebb tevékenység a köznapi értelembe vett internetszolgáltatás (mobil, helyhez kötött) és telefonszolgáltatás (mobil, helyhez kötött), ezen kívül a hírközlési szolgáltató által nyújtott e-mail szolgáltatás (például Magyar Telekom Nyrt. – @t-online.hu). Az Eht. szabályozza tevékenységek végzésével kapcsolatos hatósági

[231] BÁCS Zoltán György (2023): Gondolatok az információ szerepéről – más, egyéni szemszögből. *Nemzetbiztonsági Szemle*, 11(3), 85. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/6862/5705 (Letöltés ideje: 2024. február 19.)

[232] Eht. 188. § 16. pontja szerinti internet-hozzáférési szolgáltatás, a személyközi hírközlési szolgáltatás, valamint a jeleknek elektronikus hírközlő hálózatokon történő átviteléből álló szolgáltatás.

engedélyezési, felügyeleti eljárásokat, valamint a hírközlési LI ágazati törvényi rendelkezéseit. A hírközlés tekintetében infrastruktúra szempontjából beszélhetünk földalatti, földfelszíni, vízi, légi és világűr infrastruktúráról, helyhez kötött és mobil építményről, az átviteli út fajtája szerint pedig lehet vezetékes és vezeték nélküli egyaránt.[233]

Az Eht. szabályozási tárgyán kívül helyezkednek el – legalább is aktuális jogalkalmazói szempontból, mely a 2.6.3. alfejezetben kifejtésre kerül – a napjainkra egyre népszerűbbé váló, az Ekertv. hatálya alá tartozó egyes e-kereskedelemmel és egyéb információs társadalommal összefüggő tevékenységek[234]. Ezek közül kiemelendő az értekezés elsődleges vizsgálati tárgyát képező titkosított online kommunikációt biztosító alkalmazásszolgáltatók[235] tevékenysége. Az Ekertv. rendelkezik továbbá az ezen tevékenységek végzésével kapcsolatos hatósági engedélyezési, felügyeleti szabályokról, és az LI alkalmazásszolgáltatásokat érintő speciális ágazatai törvényi szintű szabályozásáról. Szakirodalmi szempontból az alkalmazásszolgáltatások PC/SaaS[236] felhőalapú számítástechnikai szolgáltatások[237] körébe tartozó CpaaS[238] RTC[239] üzenetküldő szolgáltatások, melyek rendszertanilag az értekezés szempontjából tovább bonthatóak köznapi értelemben vett „chat-" és „e-mailszolgálttásokra". Ezek lehetővé teszik a felhasználók számára, hogy a szöveges üzeneteken túl, multimédiás tartalmakat is megosszanak egymással, mint például hangüzenetek, képek, videók, élő videó streamek, és a jövőben feltételezhetően akár holografikus élő streamek. Az alkalmazásszolgáltatások nagyon népszerűek – melyek felhasználói trendjei, tendenciái a 4. fejezetben vizsgálat tárgyát képezik –, számos alkalmazás tartozik ebbe a kategóriába, mint például a WhatsApp, a Facebook Messenger (a továbbiakban: Messenger), a Telegram, az

[233] Lásd: 20/2020. (XII. 18.) NMHH rendelet az elektronikus hírközlési építmények elhelyezéséről és az elektronikus hírközlési építményekkel kapcsolatos hatósági eljárásokról.; 7/2015. (XI. 13.) NMHH rendelet a nemzeti frekvenciafelosztásról, valamint a frekvenciasávok felhasználási szabályairól 2. § (1) bek. 14. pont

[234] Ekertv. 2. § a) pontja szerinti elektronikus kereskedelmi szolgáltatás (pl.: online piactér); a 2. § j. pont szerinti bejelentés-köteles szolgáltatás (pl.: felhőalapú számítástechnikai szolgáltatás); a 2. § l) pont szerinti közvetítő szolgáltatás (pl.: keresőszolgáltatás, alkalmazásszolgáltatás, videómegosztóplatform-szolg. stb.).

[235] Ekertv. 2. § m) alkalmazásszolgáltató: *„az a természetes, illetve jogi személy vagy jogi személyiséggel nem rendelkező más szervezet, aki, vagy amely elektronikus hírközlő hálózat felhasználásával valamilyen szoftverhez vagy hardverhez való hozzáférést, szoftveres alkalmazást, valamint kapcsolódó szolgáltatásokat biztosít specifikus szoftveren vagy webes felületen több felhasználó számára, időben korlátozott vagy korlátlan módon, havi- vagy használat alapú ellenszolgáltatás fejében vagy ingyenes formában."*

[236] PC/SaaS: Public Cloud/Software as a Service – nyilvános felhő alapú szoftverszolgáltatás. Lásd: OLÁH István – MAGYAR Sándor (2023): Biztonsági kérdések egy publikus felhőben. *Military and Intelligence CyberSecurity Research Paper*, 3(1). Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/MIC%20RP%202023-1%20Ol%C3%A1h%20Istv%C3%A1n%20-%20Magyar%20S%C3%A1ndor%20Biztons%C3%A1gi%20k%C3%A9rd%C3%A9sek%20egy%20publikus%20felh%C5%91ben.pdf (Letöltés ideje: 2023. december 19.)

[237] Ekertv. 2. § jc. pont

[238] CpaaS: Communications Platform as a Service – kommunikációs platformszolgáltatás

[239] RTC: Rich Text Communication – „gazdag" szövegkommunikáció

iMessage, a Signal, a Viber, amelyek egyre több funkcionalitást kínálnak a felhasználók számára. Ezen általánosan ingyenes, titkosított online kommunikációt biztosító alkalmazások az SMS[240] és a hagyományos hanghívások alternatívájának bizonyulnak.[241] Az alkalmazásszolgáltatás jellemzően személyközi felhasználás során igénybe veszi az elektronikus hírközlési infrastruktúrát és a mobilinternetszolgáltatást.

2.6.2. *Videómegosztóplatform- és lekérhető médiaszolgáltatások elhatárolása az alkalmazásszolgáltatástól*

A médiaszolgáltatás esetén a szolgáltatás tárgya a műsorszám, a szolgáltatás nyújtására pedig elektronikus hírközlő hálózat útján kerülhet sor. A médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény (a továbbiakban: Mttv.) 203. § 35. - 36. pontjai alapján két fő csoportjaként elhatárolható egymástól a lineáris és a lekérhető médiaszolgáltatás.[242] Az Mttv., valamint a sajtószabadságról és a médiatartalmak alapvető szabályairól szóló 2010. évi CIV. törvény (a továbbiakban: Smtv.) értelmező rendelkezései szerint a lekérhető médiaszolgáltatás „*olyan médiaszolgáltatás, amelyben a szolgáltató által összeállított műsorkínálat alapján a felhasználó egyéni kérés alapján, az általa kiválasztott időpontban tekintheti, illetve hallgathatja meg a műsorszámokat*."[243] A lekérhető médiaszolgáltatások kapcsán megjegyzendő, hogy az Ekertv. 2020. június 12-től kiterjed még egy további, az információs társadalom által életre hívott szolgáltatási formára, azaz a videómegosztóplatform-szolgáltatásra[244] is, mint az interneten keresztül terjedő multimédiás tartalmak megosztását magában foglaló tevékenység, mely terjedése szorosan összefügg a kommunikációs hálózatok interoperabilitásával és globalizálódásával, valamint a fogyasztói kereslet bővülésével.[245] Az Ekertv. 2. § l) pontjának lf) alpontja a videómegosztóplatform-szolgáltatót szintén közvetítő szolgáltatóként nevesíti, akár csak az alkalmazásszolgáltatót. E

[240] SMS: Short Message Service - rövidüzenet-szolgáltatás

[241] DIXON, S. (2022): *Most popular global mobile messaging apps 2022*. Statista. Online: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (Letöltés ideje: 2024. január 20.)

[242] Lineáris médiaszolgáltatás esetén a médiaszolgáltató műsorrend alapján teszi lehetővé az általa nyújtott műsorszámok egyidejű megtekintését, vagyis időben is rendszerezett műsorszámokról van szó. Lekérhető médiaszolgáltatás esetén egyéni kérés alapján tekinthető, illetve hallgatható meg a kiválasztott műsorszám, így ilyenkor egyszerűen a médiaszolgáltató által összeállított műsorkínálatból van lehetőség választani.

[243] Mttv. 203. § 35. pont; Smtv. 1. § 4. pont

[244] Ekertv. 2. § p) - q) pontjai - egyirányú kommunikáció pl. Netfilx, HBO Go/ többirányú kommunikációt lehetővé tevő szolgáltatás pl. YouTube, Facebook hírfolyam, Twitter hírfolyam,stb.

[245] Lásd: KOLTAY András - MAYER Annamária - NYAKAS Levente - POGÁCSÁS Anett (2014): *A médiaszolgáltatás és a sajtótermék fogalma az új magyar médiaszabályozásban*. Budapest: NMHH Médiatudományi Intézet. 21-27. Online: https://nmhh.hu/dokumentum/162242/tajekoztato02.pdf (Letöltés ideje: 2024. február 16.)

tevékenységet és annak végzőjét az Mttv. 203. § 71a - 71b. pontja definiálja. E szerint a videómegosztóplatform-szolgáltatás *„[…] tájékoztatás, szórakoztatás vagy oktatás céljából elektronikus hírközlő hálózaton keresztül olyan műsorszámokat, illetve felhasználók által létrehozott videókat juttasson el a nyilvánossághoz, amelyekért a videómegosztóplatform-szolgáltató nem tartozik szerkesztői felelősséggel […]*". Ilyen például a YouTube, a Videa, a Facebook hírfolyam, a Facebook és Instagram Reels, a TikTok stb. A törvénymódosítás általános indokolása szerint[246] azért volt szükség az új szolgáltatói kategória definiálására – és így az Ekertv. hatályának kiterjesztésére –, mivel arra a vonatkozó uniós AVMS irányelv[247] szerint jogharmonizációs kötelezettsége volt a tagállamoknak. A módosítás indokolása szerint „*az uniós szabályozás alapján a videómegosztóplatform-szolgáltatók a hagyományos médiaszolgáltatóktól eltérően […] nem tartoznak szerkesztői felelősséggel az elérhetővé tett tartalom vonatkozásában.*"[248] Továbbá a jogszabálymódosítás keretében, szintén az AVMS irányelvhez igazítva elhatárolásra került a videómegosztóplatform-szolgáltatás az újgenerációs lekérhető médiaszolgáltatástól is.[249] Ilyen például a Netflix, HBO Max, Disney. Azért is lényeges ezen szolgáltatási körök elhatárolása az alkalmazásszolgáltatásoktól, mivel legtöbbjük ugyanúgy elérhető mobil rádiótelefon (a továbbiakban: mobil- vagy okostelefon) applikáción keresztül, azonban személyközi kommunikáció, azaz csevegésre nem alkalmasak, amely alól azonban mégiscsak kivételt képez az egyes megosztott tartalmakhoz fűzhető kommentelés, mely egy lényeges jogalkalmazói probléma az egyes szolgáltatások besorolásánál. Hasonló jellegű probléma, ha a videómegosztóplatform-szolgáltatáshoz, ugyan elkülönítve, de csevegőszolgáltatást, azaz alkalmazásszolgáltatást illesztenek, mint például a Facebook és a Messenger esetében.[250]

---

[246] Végső előterjesztői indokolás a médiaszolgáltatással kapcsolatos egyes törvények módosításáról szóló 2019. évi LXIII. törvényhez. Indokolások tára, Magyar Közlöny Melléklete, 2019. július 9. 110–120.

[247] Az Európai Parlament és a Tanács (EU) 2018/1808 irányelve (2018. november 14.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról szóló 2010/13/EU irányelvnek (Audiovizuális médiaszolgáltatásokról szóló irányelv) a változó piaci körülményekre tekintettel való módosításáról. (a továbbiakban: AVMS) HL L 303, 2018. november 28. 69–92.

[248] Végső előterjesztői indokolás a médiaszolgáltatással kapcsolatos egyes törvények módosításáról szóló 2019. évi LXIII. törvényhez. Indokolások tára, Magyar Közlöny Melléklete, 2019. július 9. 111.

[249] Mttv. 203. § 35. pontja

[250] Lásd: KIRÁLY Péter Bálint (2021): A videómegosztóplatform-szolgáltatók szabályozásának kihívásai. *In Medias Res*, 10(2), 312-330. Online: https://inmediasresfolyoirat.hu/imr/article/view/236/237 (Letöltés ideje: 2024. február 16.); DR. PAPP János Tamás (2021): *A közösségi média platformok szabályozása a demokratikus nyilvánosság védelmében.* Doktori (PhD) értekezése. Budapest: PPKE JÁDI. Online: https://real-phd.mtak.hu/1167/1/Papp_Janos_Tamas_dolgozatv.pdf (Letöltés ideje: 2024. február 16.)

Az elektronikus hírközlési szolgáltatásnak, a videómegosztóplatform-szolgáltatásnak, valamint a lekérhető médiaszolgáltatásnak a – titkosított online kommunikációt biztosító – alkalmazásszolgáltatástól való elhatárolását követően szükséges az EU digitális stratégiai célkitűzései kapcsán megjelenő jogszabályoknak (például DMA, Hírközlési Kódex) az alkalmazásszolgáltatás fogalmára, rendszertani besorolására gyakorolt hatásait megvizsgálni, továbbá kimutatni, hogy a digitális ökoszisztéma hogyan befolyásolja az elektronikus hírközlési, és online infokommunikációs jogszabályok hatályának alakulását.

2.6.3. Az alkalmazásszolgáltatás fogalmának, rendszertani besorolásának alakulása az EU digitális stratégiai célkitűzései aspektusából

A 2.4.1. részfejezetben ismertetettek szerint a DMA 1. cikk (3) bek. a hatálya alá vonja a számfüggetlen személyközi hírközlési szolgáltatásokat[251] (NI-ICS), mint a 2018-as Hírközlési Kódex II. cikk 7. pontjában meghatározott elektronikus hírközlési szolgáltatást. Így következhetett be, hogy a Bizottság a küszöbérték elérése okán NI-ICS kategóriában kapuőrré minősítette a Metát a WhatsApp és Messenger alkalmazásszolgáltatások, platformok tekintetében. Továbbá a DMA 2. cikk 2. pontja bevezeti innovatív módon az alapvető platformszolgáltatás fogalmát, amelybe a rendelet szerinti taxatív felsorolás alapján például beletartozik az online közvetítő szolgáltatás (például Netflix, HBO Max), a videómegosztóplatform-szolgáltatás (például YouTube, Facebook hírfolyam), valamint a 2. cikk 2. pont e) alpont alapján az NI-ICS szolgáltatás típus is, mely egyben a Bizottság jogalkalmazása alapján az Ekertv. szerinti alkalmazásszolgáltatás (WhatsApp és Messenger) is.

A Hírközlési Kódex (11) preambulumbekezdése elkezdte közelíteni egymáshoz az elektronikus hírközlési szolgáltatás és az EU információs társadalommal összefüggő szolgáltatásokról szóló 2015-ös irányelvének[252] szekularizált fogalomhasználatát, mivel kimondja, hogy az elektronikus hírközlési szolgáltatások – a különös szabályok kivételével – az információs társadalommal összefüggő szolgáltatásokra vonatkozó fogalommeghatározás hatálya alá is

[251] Hírközlési Kódex a 2. cikk 4. pont: „*elektronikus hírközlési szolgáltatás”* keretében értelmezett II. cikk 7. pont *„számfüggetlen személyközi hírközlési szolgáltatás”: olyan személyközi kommunikációs szolgáltatás, amely nem nyilvánosan kiosztott számozási erőforrások révén, nevezetesen nem nemzeti, illetve nemzetközi számozási tervben szereplő hívószám vagy hívószámok segítségével biztosít kapcsolódást, és amely nem tesz lehetővé kommunikációt nemzeti, illetve nemzetközi számozási tervben szereplő hívószámmal vagy hívószámokkal”*

[252] Az Európai Parlament és a Tanács (EU) 2015/1535 irányelve (2015. szeptember 9.) a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról. HL L 241., 2015.9.17. 1-15. 1.

tartoznak. Ugyanakkor az olyan elektronikus hírközlési szolgáltatásokat, mint a hangalapú- és üzenetküldő szolgáltatásokat, az elektronikus levéltovábbítási szolgáltatásokat általánosan is a Hírközlési Kódex hatálya alá rendeli. Álláspontom alapján ennek történeti, jogpolitikai megértéséhez a 2017-ben előterjesztett e-hírközlési adatvédelmi rendelet javaslatot és annak indokolását is érdemes mélyebben megvizsgálni.

A jogalkotó az e-hírközlési adatvédelmi rendelet javaslat háttere és indokai alapján 2017-ben megállapította, hogy a hatályos irányelv 2009-es legutóbbi felülvizsgálata óta fontos technológiai és gazdasági fejlődés zajlott a piacon, amely okán az nem tartott lépést a technológiai fejlődéssel, következésképpen az már akkor sem nyújtott kellő adatvédelmet az új szolgáltatások használatával lebonyolított kommunikáció során. A javaslat 3.4. alfejezete szerinti hatásvizsgálat alapján a jogalkotó által előnyben részesített szakpolitikai alternatíva hatékonyság, eredményesség és koherencia szempontjából „*Megerősíti az elektronikus hírközlés titkosságának védelmét azáltal, hogy kiterjeszti a jogi eszköz hatályát a funkciójukat tekintve egyenértékű új elektronikus hírközlési szolgáltatásokra*." Tehát az uniós jogalkotói szándék alapján az e-hírközlési rendelet javaslat hatályát ki kívánták terjeszteni a hagyományos elektronikus hírközlési szolgáltatások (telefon, SMS, e-mail, mobilinternet stb.) mellett az olyan új hálózatsemleges, internettechnológia alapú személyközi kommunikációs szolgálásokra, mint a hang- (VoIP[253]), szöveg, és adattovábbítást biztosító alkalmazásszolgáltatásokra, melyek funkcionálisan egyenértékűek a hagyományos elektronikus hírközlési szolgáltatásokkal. A 2017-es hatásvizsgálat együttesen OTT[254]-ként hivatkozik ezen szolgáltatásokra, azonban a fentiek az Ekertv. hatályos fogalomrendszere alapján online kommunikációt biztosító alkalmazásszolgáltatások, egyben a DMA, a Hírközlési Kódex és annak implementálását követően az Eht. szerinti NI-ICS-ek. Az OTT napjainkra egy sokkal szélesebb szolgáltatási kört, platformot fed le, melynek az értekezés szempontjából releváns, már a DMA terminológiájának figyelembevételével definiált főbb részhalmazai az alábbiak szerint csoportosíthatók a közvetítő szolgáltatások keretén belül:

- újgenerációs lekérhető médiaszolgáltatások (például Netflix, Disney, HBO Max);
- videómegosztóplatform-szolgáltatások (például Youtube, Facebook hírfolyam);
- online közösségi hálózati szolgáltatások (például Facebook, Instagram);
- alkalmazásszolgáltatások (például WhatsApp, Messenger, iMessage, Signal).

[253] Voice over IP – internetprotokoll feletti hangátvitel
[254] OTT: Over the Top – Egy olyan alkalmazás vagy tartalomszolgáltatás, amely lehetővé teszi egy termék elérését az interneten keresztül kikerülve a hagyományos terjesztést.

Az e-hírközlési adatvédelmi rendelet javaslat (11) preambulumbekezdése tovább részletezi a kérdéskört, miszerint annak érdekében, hogy a funkcionálisan egyenértékű szolgáltatásokat igénybe vevő végfelhasználóknak is hatékony és egyenlő védelmet biztosítson, a rendelet javaslat az elektronikus hírközlési szolgáltatásokon a Hírközlési Kódexben definiált fogalmat érti. Ezen meghatározásba a javaslat alapján nemcsak az internet-hozzáférést biztosító szolgáltatások, tartoznának bele, hanem a számfüggő vagy számfüggetlen személyközi kommunikációs szolgáltatások, például a VoIP, üzenetküldési és e-mail-szolgáltatások is. Továbbá a javaslat (11) preambulumbekezdése kimondja, hogy „*a hírközlés titkosságának védelme a más szolgáltatásokat kiegészítő, személyközi kommunikációt lehetővé tevő szolgáltatások esetében is elengedhetetlen, vagyis az ilyen, kommunikációs funkcióval rendelkező szolgáltatások is e rendelet hatálya alá tartoznak*."

Tehát a részfejezet következtetéseként megállapítható, hogy az e-hírközlési adatvédelmi rendelet javaslat hatálybalépése esetén az internettechnológiára épülő alkalmazásszolgáltatásokat adatvédelmi szempontból ugyanúgy a hatálya alatt kezelte volna, mint a hagyományos elektronikus hírközlési szolgáltatásokat. Ez egy úttörő, az információs társadalommal összefüggő szolgáltatások és az elektronikus hírközlési szolgáltatások szekularizált adatvédelmi szabályozásának felszámolására tett, a szolgáltatások funkcionalitását figyelembe vevő törekvésként jelent meg 2017-ben. Ezen jogpolitikai szemlélet végül a DMA és a Hírközlési Kódex kapcsán 2023-ra lényegében a hatályos és alkalmazandó uniós jog tételévé vált, így EU-s és tagállami szintű jogalkotói, jogalkalmazói kötelezettségeket testesítve meg. Aktuális példa, hogy a Bizottság a DMA alkalmazása során az alkalmazásszolgáltatások/ NI-ICS körében először a WhatsApp-ot és a Messenger-t alapvető platformszolgáltatássá minősítette. Azonban az információs társadalommal összefüggő infokommunikációs és az elektronikus hírközlési szolgáltatások integrált szabályozásának mind uniós, mind tagállami szinten további teendői vannak. Hiszen például az értekezés tárgyával kapcsolatos hazai jogforrások – az LI tekintetében is – szekularizáltan szabályozzák a tevékenységeket, annak ellenére, hogy a 2020. december 21-től hatályos Eht. módosítás már implementálta az NI-ICS-re vonatkozó különös szabályokat. A disszertáció során az egységes, következetes fogalomhasználat érdekeben a témaválasztás indoklása kikötése szerint is a személyközi titkosított online kommunikációt biztosító IKT szolgáltatók alkalmazásszolgáltatóként kerülnek megnevezésre.

A fentiek alapján látható, hogy az EU digitalizációs törekvései mentén – az információs társadalommal összefüggő szolgáltatások uniós szabályozásának talaján – a DMA és a DSA bázisán kialakult a digitális ágazat, amellyel párhuzamosan a közösségi jog szintjén létrejött egy új jogterület, a platformszabályozás, a platformjog. Ez egyben azt jelenti, hogy „*a korábbi gyakorlat alapján bevettnek tekinthető horizontális szabályozási területek (fogyasztóvédelem, adatvédelem) mellett a digitális transzformáció olyan új horizontális területeket alakított és alakít ki, amelyek ágazatfüggetlenül relevánsak, ide sorolhatók például az adatáramlás, a születőben lévő adatgazdaság (Data Act, Data Governance Act), a mesterséges intelligencia (AIA, AI Liability Directive), valamint a kiberbiztonság (NIS, NIS2, ECI, CER, EIDAS, Cyber Resilience Act,)*."[255] A digitális ágazat beékelődött és jelentős hatást gyakorol mind az elektronikus hírközlési, mind a elektronikus információ-, kiberbiztonsági ágazatra és szabályozásra, mely jogterületek éles elhatárolása még az Unió szintjén is egy alakulóban lévő folyamat, nem hogy a tagállami jog szintjén, mely például az Eht. és az Ekertv. NI-ICS-sel/alkalmazásszolgáltatással kapcsolatos tárgyi hatálya kapcsán, így az LI szabályozása szempontjából is kardinális kérdés. Hiszen például a DMA – és már a Hírközlési Kódex is – a digitális (információs társadalommal összefüggő szolgáltatások) ágazati szabályozásból az NI-ICS tekintetében átnyúl az elektronikus hírközlési ágazati szabályozásba, mely hazai jogforrási szinten az Eht.-ben került adaptálásra, átültetésre, úgyhogy egyébként az Ekertv. hatálya pedig továbbra is kiterjed az alkalmazásszolgáltatóra. Az Eht. és az Ekertv. hatálya ilyen jellegű összeütközésének azonosítása álláspontom alapján új tudományos eredmény is egyben.

Kimutatásra került az alkalmazásszolgáltatásnak az NI-ICS-sel való összefüggése, az Ekertv. és az Eht., DMA, Hírközlési Kódex alapján, illetve az alkalmazásszolgáltatás és az NI-ICS funkcionális azonossága okán fellépő Ekertv. és Eht. tárgyi hatályának összeütközése. Ezen következtetést az Európai Bizottság kapcsolódó joggyakorlata alapján kívánom bizonyítani, miszerint a Bizottság a DMA 3. cikk alapján a 2023. szeptember 05-ei határozatának 5.4.3. és 5.5.4. alpontjai[256] szerinti a Meta Platforms Inc-t, mint a DMA 2 cikk 1. pontja szerinti alapvető

[255] DR. FIRNIKSZ Judit (2023): *Pillanatkép a digitális piacok szabályozásáról - A DMA a vállalati compliance tükrében.* Doktori (PhD) értekezés. Budapest: PPKE JÁDI 68-69. Online: https://jak.ppke.hu/storage/tinymce/uploads/Firniksz_Judit_dolgozatv.pdf?u=1c3e6s (Letöltés ideje: 2024. február 18.)

[256] Commission Decision of 5.9.2023 designating Meta as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector, DMA.100020 Meta - online social networking services, DMA.100024 Meta - number-independent interpersonal communications services, DMA.100035 Meta - online advertising services, DMA.100044 Meta - online intermediation services – marketplace. Brussels, 5.9.2023, C(2023) 6105 final. WhatsApp minősítése, összefoglaló jogalap indoklása: 5.4.3. alpont; Messenger minősítése, összefoglaló jogalap indoklása: 5.5.4. alpont. az (EU) 2022/1925 rendelet 3. cikke szerinti határozatról. 5. fejezet (26) bek.

platformszolgáltatást nyújtó vállalkozást a WhatsApp és Messenger alkalmazások tekintetében kapuőrré minősítette NI-ICS kategóriában. Hiszen ezen szolgáltatások:

- a 2023. február 17-től alkalmazandó DMA 2. cikk 2. pont szerinti alapvető platformszolgáltatás keretében értelmezett 2. cikk. 2. pont e) alpont szerinti számfüggetlen személyközi hírközlési szolgáltatások, azaz NI-ICS[257]-ek;
- a 2020. december 31-től alkalmazandó Európai Elektronikus Hírközlési Kódex 2. cikk 4. pont szerinti elektronikus hírközlési szolgáltatás keretében értelmezett II. cikk 7. pont szerinti számfüggetlen személyközi hírközlési szolgáltatások, azaz NI-ICS-ek;
- a Hírközlési Kódex vonatkozó rendelkezéseit a hazai elektronikus hírközlési ágazati jogba 2020. december 21-től hatályosan átültető Eht. 188. § 16. pontja szerinti elektronikus hírközlési szolgáltatás keretében értelmezett 188. § 123. pontja szerinti számfüggetlen személyközi hírközlési szolgáltatások, azaz az uniós, közösségi joggal (DMA, Hírközlési Kódex) harmonikusan értelmezve (nyelvi, tartalmi), valamint az NMHH fogalomértelmezésével[258] és a BEREC érvelésével[259] is összhangban lévő NI-ICS-ek;
- azonban a WhatsApp és Messenger az Ekertv. 2. § 1. pontja, valamint a 3/B. § szerinti hazai értelmezés alapján egyben titkosított kommunikációt biztosító alkalmazásszolgáltatások is.

Továbbá a Bizottság minősítő határozatában az Apple Distribution International Ltd.[260] által üzemeltett iMessage alkalmazásszolgáltatást is NI-ICS-ként értelmezi, azonban az Apple iMessage tekintetében való DMA szerinti kapuőri minősítése ellen fellebbezett, de ez nem befolyásolja az iMessage NI-ICS-ként való Bizottság általi értelmezését.[261]

---

[257] NI-ICS: Number-Independent Interpersonal Communication Services – számfüggetlen személyközi kommunikációs szolgáltatás: Lásd: *BEREC report on interoperability of NumberIndependent Interpersonal Communication Services (NI-ICS)*. BEREC, BoR (23) 92. 2023.

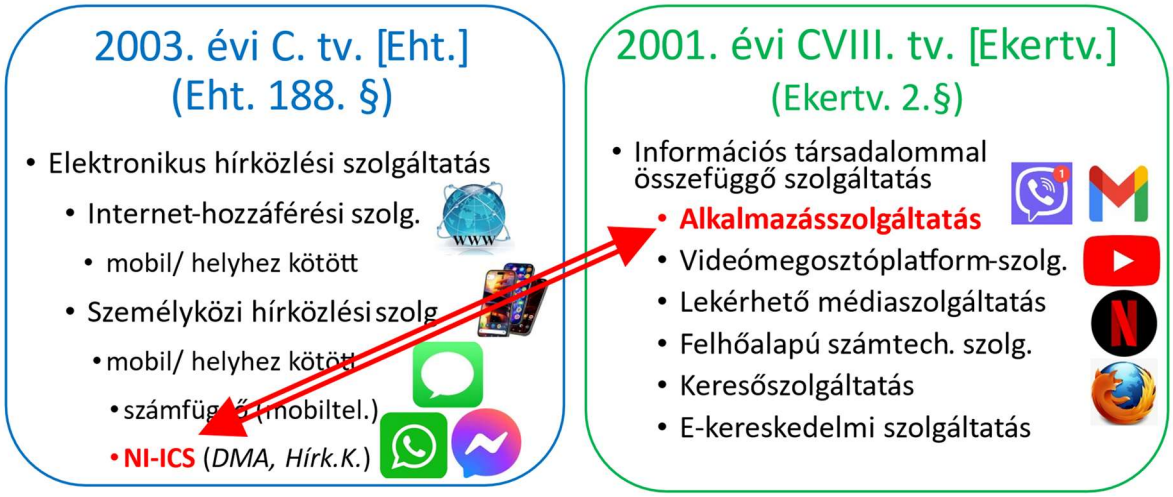
[258] Lásd: NMHH. Online: https://nmhh.hu/media-es-hirkozlesi-biztos/kisokos/elem/176/Alapfogalmak (Letöltés ideje: 2024. február 20.)

[259] *BEREC report on interoperability of NumberIndependent Interpersonal Communication Services (NI-ICS)*. BEREC, BoR (23) 92. 2023.

[260] Az Apple európai, írországi székhelyű disztribútora

[261] Commission Decision of 5.9.2023 designating Apple as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector, DMA.100020 Meta - online social networking services, DMA.100013 Apple – online intermediation services – app stores, DMA.100025 Apple – operating systems és DMA.100027 Apple – web browser. Brussels, 5.9.2023, C(2023) 6100 final. iMessages minősítése, összefoglaló jogalap indoklása: 5.4.4. alpont.; A Bizottság határozatának összefoglalója (2023. szeptember 5.) az Apple-nek a digitális ágazat vonatkozásában a versengő és tisztességes piacokról szóló (EU) 2022/1925 európai parlamenti és tanácsi rendelet 3. cikke értelmében történő kapuőrré minősítéséről (DMA.100013 Apple – online intermediation services – app stores, DMA.100025 Apple – operating systems és DMA.100027 Apple – web browsers). 4. fejezet (14) bek.

Az értekezés szempontjából az Eht. és az Ekertv. szerinti releváns főbb szolgáltatástípusok elhatárolását a 8. ábra hivatott szemléltetni, egyben ábrázolva az Eht. által szabályozott NI-ICS és az Ekertv. által szabályozott alkalmazásszolgáltatás funkcionális azonossága okán fellépő Eht. és Ekertv. tárgyi hatályának összeütközését.



8. ábra: Az Eht. és az Ekertv. szerinti főbb releváns szolgáltatástípusok elhatárolása (Szerk.: A szerző)

2.6.4. Kommunikáció, kommunikációs tartalom fogalma, kísérő- és metaadat elhatárolása

A kommunikációs ismeretek átfogóbb vizsgálatától eltekintve, hiszen ezt már számos szerző, megtette, megállapítható, hogy a kommunikáció információelméleti-kibernetikai értelemben magában foglalja a komplex információcserét, akár az embertől függetlenített értelemben is. A kommunikáció technikai értelemben véve az ember alkotta technológiai rendszereken, mint például elektronikus hírközlőhálózaton, postaküldeményben történő információátadást foglalja magában.[262] Az értekezésben – mint, ahogy az a témaválasztás indoklása során is kikötésre került – a technikai értelemben vett, személyközi jellegű kommunikáció vizsgálata bír relevanciával, tekintettel arra, hogy a hatályos szabályozás alapján ellenőrzés, LI alá a konkrétan meghatározott természetes személyek elektronikus hírközlő hálózaton (csatornán[263])

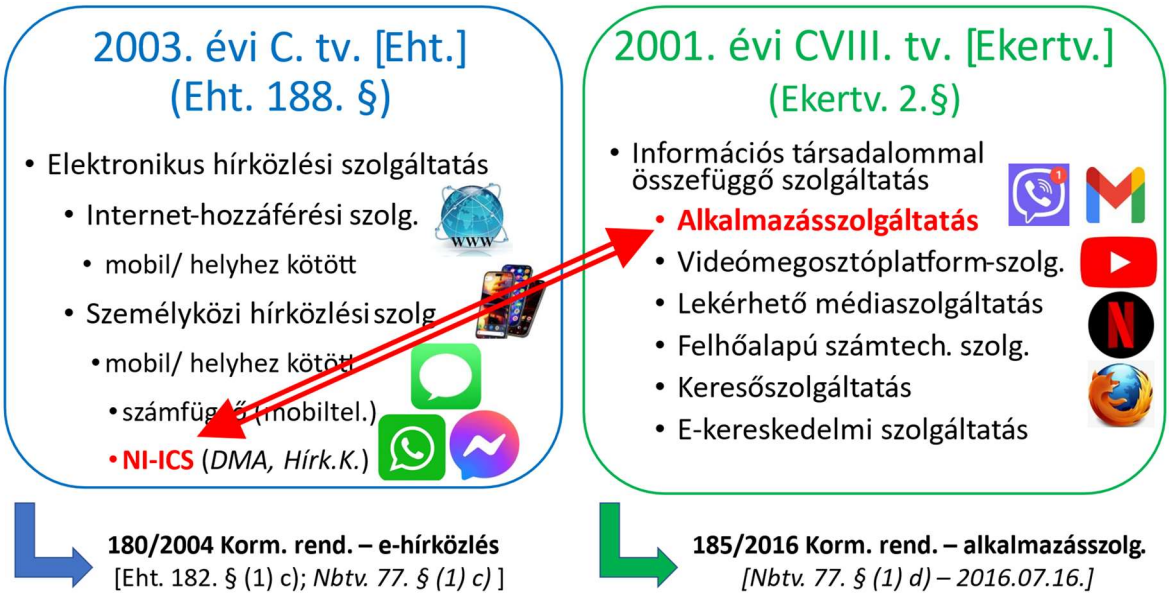
[262] BUDA Béla (1988): *A közvetlen emberi kommunikáció szabályszerűségei.* Budapest: Tömegkommunikációs Kutatóközpont. 16-17. Online: http://www.budabela.hu/dokumentumok/onallokotetek/kozvetlenemberi-kommunikaciotext.pdf (Letöltés ideje: 2024. február 20.)

[263] Az egyéb csatornák elemzése, mint például a postai küldemények nem képezik az értekezés tárgyát. Az elektronikus hírközlési csatornán továbbított közlemény eredeti formája lehet hang, szöveg, vagy adat, jel azonban ezek elhatárolása egymástól nem indokolt az értekezés szempontjából.

folytatott kommunikációja vonható.[264] Az LI tekintetében további jogalkalmazási nehézség, hogy mind a kommunikáció és tartalmának fogalma, mind a kísérő- és metaadat fogalma eltér az Eht. és az Ekertv. szerint. A fogalmak meghatározására a titkos információgyűjtés során a szolgáltatók számárára előírt együttműködés és annak rendjét szabályozó rendeletek hivatottak. Az uniós jogban az elektronikus hírközlési szolgáltatás tekintetében definíciót nyújt az e-hírközlési adatvédelmi irányelv, és az e-hírközlési adatvédelmi rendelet javaslat is iránymutató.

Az Eht. hatálya alá tartozó tevékenységekhez kapcsolódóan az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről szóló 180/2004. (V.26.) Korm. rendelet 2. § a) pontja szerint a kommunikáció az Eht. 159/A. § (6) bekezdésében meghatározott fogalom. Az e-hírközlési adatvédelmi irányelv a kommunikációt, mint „közlés" definiálja a 2. cikk d) pontjában. A kommunikáció tartalmáról a 180/2004. (V.26.) Korm. rendelet 2. § b) pontja rendelkezik. Az e-hírközlési adatvédelmi irányelv a kommunikáció tartalmának általános definiálása helyett a 2. cikk e), h) pontjai alapján speciálisan a „hívás" és az „elektronikus levél" fogalmát határozza meg. Az e-hírközlési adatvédelmi rendelet javaslat 4. cikk (3) bek. a) pontja a korábbi szabályozási szemléletet felváltva – a javaslat (11) preambulumbekezdése alapján összhangban a Hírközlési Kódex fogalomhasználatával – szükségszerűen már általánosan definiálja az elektronikus hírközlési adatok fogalmát, melyek „*az elektronikus hírközlés tartalma és elektronikus hírközlési metaadatok*". Az e-hírközlési adatvédelmi rendelet javaslat tervezetének 4. cikk (3) bek. b) pontja meghatározza az elektronikus hírközlés tartalmát, valamint a 2. cikk (3) bek. e) pont aktualizálja az elektronikus levél fogalmát. Az Ekertv. hatálya alá tartozó tevékenységhez kapcsolódóan a kommunikáció fogalmát a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről szóló 185/2016. (VII.13.) Korm. rendelet 1. § b) pontja állapítja meg. A kommunikáció tartalmáról a 185/2016. (VII.13.) Korm. rendelet 1. § c) pontja rendelkezik. A Eht. és az Ekertv. szerinti egyes, az értekezés szempontjából lényeges főbb szolgáltatástípusokat, valamint a fenti törvényekből, és az Nbtv.-ből az LI végrehajtásával kapcsolatosan levezethető kormányrendeletek összefüggéseit az alábbi 9. ábra hivatott szemléltetni:

[264] Tapasztalva például az MI alapú autonóm rendszerek fejlődését, alanyi oldal tekintetében szükséges a szakmai és jogászi, jogtudományi gondolkodás fókuszát a robotika által vezérelt M2M kommunikáció LI-jére helyezni, azonban ez nem képezi az értekezés tárgyát.



9. ábra: Az Eht. és az Ekertv. szerinti főbb releváns szolgáltatástípusok elhatárolása, valamint a szolgáltatók és az LI-re jogosult szervezetek együttműködésének rendjéről szóló kormányrendeletek (Szerk.: A szerző)

A hatályos szabályozás alapján az elektronikus hírközlés során végbemenő kommunikáció véges, behatárolható számú felek közötti információcsere, közlés vagy arra irányuló kísérlet az Eht. hatálya alá tartozó szolgáltatások igénybevétele során, illetve azon műsorterjesztés, amely egyedi előfizetőhöz, felhasználóhoz köthető. E vonatkozásában a tartalom pedig minden a kommunikáció során továbbított információ, jel, amely alól kivételt képez a kísérő adat. Tehát mobiltelefon kommunikáció, azaz az Eht. 188. § 16. pontja szerinti elektronikus hírközlési szolgáltatás keretében értelmezett 188. § 122. pontja szerinti számfüggő személyközi hírközlési szolgáltatás (NB-ICS[265]) során a hang (például a Magyar Telekom Nyrt. mobil hálózatán folytatott hívás) és szöveges SMS alapú közlés. Megállapítható, hogy míg az Eht. a „tartalmat" beszéd vagy nem beszéd jellegű jelként azonosítja, addig az e-hírközlési adatvédelmi rendelet javaslat már innovatív szemléletben azt küldött/ fogadott tartalomként közelíti meg, példálózó jelleggel azonosítva a szöveg, beszéd, videó, kép és hang típusokat, melyeket tartalmazó elektronikus üzenetként definiálja az „elektronikus levelet".

Alkalmazásszolgáltatás esetén a kommunikáció egyedi felhasználók, vagy azok csoportja számára nyújtott, valamilyen szoftver (például Messenger, Viber alkalmazás), webes felület által biztosított információcserét lehetővé tevő szolgáltatás igénybevétele során végbemenő

[265] NB-ICS: number-based interpersonal communications service - számfüggő személyközi hírközlési szolgáltatás. Lásd: Hírközlési Kódex 2. cikk 6. pont

közlés, mely elektronikus hírközlő hálózat (például mobilinternet) igénybevétele útján valósul meg. E vonatkozásában a kommunikáció tartalma alapjába véve ugyanaz, mint az elektronikus hírközlési szolgáltatás során, azonban a technológia adta lehetőségek alapján ezt kibővítetten kell értelmezni a multimédiás adattal. Kiemelést érdemel, hogy a kommunikáció tartalmának titkosítása, megváltoztatása vagy tömörítése esetén taralomnak csak a közlés eredeti formájára visszaállított adat[266] minősül. Ennek az LI eredményes végrehajtása szempontjából van kiemelt jelentősége, hiszen például a kriptográfiai eljárásokkal rejtjelezett tartalomhoz technikailag hiába fér hozzá a jogosult szervezet, az nem értelmezhető, dolgozható fel a titkos információgyűjtés során, csak egyedi rejtjelfejtő eljárást követően. Mindkét fenti esetben lényeges tartalmi elem, hogy a szolgáltatások keretében továbbított, vagy továbbításra előkészített adat az azt átvevő, azonosítható előfizetőhöz vagy felhasználóhoz valamilyen eljárás mentén kapcsolható legyen, azaz egyedi felhasználóhoz legyen köthető, mely az LI szempontjából lényeges.

Az elektronikus hírközlési szolgáltatások és az alkalmazásszolgáltatások elhatárolása során megkülönböztethető a kísérőadat és metaadat fogalomköre. Az Eht. hatálya alá tartozó tevékenységekhez kapcsolódóan a 180/20004. (V.26.) Korm. rendelet 2. § e) pontja rendelkezik a kísérőadat fogamáról, melyet az e-hírközlési adatvédelmi irányelv 2. cikk nem definiál, annak b) pontja forgalmi adatról rendelkezik, amely „*egy közlésnek az elektronikus hírközlő hálózaton keresztül történő továbbítása vagy erre vonatkozó számlázás céljából kezelt minden adat*”. Az Eht. 157. – 159/A. §-aiben, külön részfejezetben a forgalmi és számlázási adatokról pedig részletesen rendelkezik. Mind az Eht, mind az e-hírközlési adatvédelmi irányelv külön rendelkezik a helymeghatározási adatok köréről és szabályairól, melyek jelentőséggel bírhatnak a titkos információgyűjtés eredményessége szempontjából. Az elektronikus hírközlési szolgáltatás során értelmezett kommunikációval összefüggő kísérőadat taxatíve meghatározott elemeit sem az Eht., sem az e-hírközlési irányelv nem definiálja, arra az anyagi jogszabályokból és a technológia aktuális állapotából lehet következtetni. A 180/2004. (V.26.) Korm. rendelet 5. § (1) bekezdéséből levezetve kísérő adatnak minősül az Eht. 156. § (16) - (17) bek., a 157. § (10) bek. és a 159/A. § (1) - (2) bek. szerinti adat,[267] különösen a szolgáltató által kezelt, az LI-

[266] Például amit a csevegőfelületre a felhasználó begépelt küldés előtt, vagy amit a fogadást és desifrírozást követően a címzett elolvas és értelmezhető számára.

[267] E rendelkezés nem a kommunikáció tartalmához való hozzáférést szabályozza, hanem a közleményhez és annak tartalmához kapcsolódó, a fenti rendelkezések szerinti adatok szolgáltatását, tehát a kísérőadatokat.

vel érintett felhasználó, előfizető által elektronikus hírközlési szolgáltatás igénybevételével összefüggésbe hozható hívásforgalmi, helymeghatározási, előfizetői, és számlázási adatok.

Az Ekertv. szerinti titkosított online kommunikációt biztosító alkalmazásszolgáltatás tekintetében, a 185/2016. (VII.13.) Korm. rendelet 1. § d) pontja szerint a metaadat az Ekertv. 13/B. § (2) bekezdésében meghatározott adat, tehát az LI-vel érintett szolgáltatás típusa, a felhasználónak vagy az előfizetőnek a szolgáltatás igénybevételéhez szükséges azonosító adatai, az igénybevétel dátumát, kezdő és záró időpontja, valamint a regisztrációhoz és az igénybevételhez használt IP-cím és portszám, továbbá a felhasználó azonosító adatai. Tehát metaadat a titkosított alkalmazásszolgáltatás igénybevételével végbemenő kommunikáció vonatkozásában elsősorban a felhasználóra utaló azonosítóadat, a kommunikáció időpontja, valamint a kommunikáció során felhasznált végponti eszköz (például mobiltelefon, számítógép) elektronikus hírközlő hálózat igénybevétele során kibocsájtott egyedi azonosító adata, IP-címe és portszáma. Az IP-címek elsődleges jelentősége az alkalmazásszolgáltatások LI-je vonatozásában – akár statikus, akár dinamikus az IP – a helymeghatározás tekintetében értékelődik fel. Az e-hírközlési adatvédelmi rendelet javaslat tervezetének 4. cikk (3) bek. b) pontja alapján az elektronikus hírközlési szolgáltatás során kezelt adat vonatkozásában a jogalkotó szakítani próbált a kísérőadat meghatározással, egységesítési törekvésként az Ekertv. fogalomrendszerével is harmonikusan már elektronikus hírközlési metaadatot definiál, melybe integrálja a forgalmi és helymeghatározási adat fogalmát is, a kor elvárásainak megfelelő egységes jogalkalmazást elősegítve.

2.7. Kriptográfiai kitekintés és annak főbb kihívásai

Az alfejezeteben általános felhasználói szemléletben betekintés történik a kriptográfia alapismereteibe, az egyes algoritmusok, eljárások csoportjaiba kitérve már a poszt-kvantumkriptográfia jellemzőire, ismertetésre kerülnek a kriptográfiára ható főbb kihívások, hiszen csak így érthető meg kellően, hogy többek között mi vezet az alkalmazásszolgáltatások kriptográfiai környezetének folyamatos fejlődéséhez, mely végsősoron az LI hatékonysága és technológia-igénye szempontjából bír relevanciával. Ezt követően a jogosulatlan támadások és a jogosult LI aspektusából megvilágításra kerül a C2SE és az E2EE lényegi különbsége.[268]

[268] A résztémakörrel kapcsolatos korábbi kutatási eredményeimet lásd: TÓTH, Tamás (2023): Actualities of certain security aspects of cryptography with regard to information societies. *National Security Review*, 9(1), 107-118. Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2023_1_NSR.pdf (Letöltés ideje: 2024. február 23.)

2.7.1. *A kriptográfiáról általában, rendszertan és áttekintése*

A kriptográfia a kriptopológia, azaz a titkos kommunikáció tudományának egyik ága a kriptoanalízis[269] mellett, *„az adatok, üzenetek rejtjelzésével (kódolás, sifrírozás) és megfejtésével (rejtjelfejtés, dekódolás, desifirozás) foglalkozó tudományág, a matematikai tudományok egyik részterülete.*"[270] A kriptográfia lényegében azon algoritmikus módszereket, valamint azok használatának pontos leírását tartalmazó protokollokat vizsgálja, amelyek hozzájárulnak az Ibtv. fogalomhasználata szerint értelmezett elektronikus információs rendszer biztonságához, azaz a kommunikációs vagy a tárolt adatok bizalmasságának[271] (köznapi értelemben vett titkosságának) és sértetlenségének[272], azon belül is hitelességének, letagadhatatlanságának biztosításához.[273] Az Ibtv. szerinti „bizalmasság" összhangban áll az e-hírközlési adatvédelmi rendelet javaslat (15) preambulumbekezdésének fogalomhasználatával. Az uniós jogpolitikai törekvés a rendelet javaslat (1) preambulumbekezdésében a bizalmassággal, a titkosság elvével kapcsolatban kimondja továbbá, hogy azt „*az aktuális és jövőbeli kommunikációs eszközökre, többek között a hívásokra, az internet-hozzáférésre, az azonnali üzenetküldő alkalmazásokra, az e-mailekre, az internetes telefonálásra és a közösségi médián keresztül küldött személyes üzenetekre egyaránt alkalmazni kell."* – tehát ezen rendelkezésből is levezethető az online infokommunikációs szolgáltatások, így az alkalmazásszolgáltatások elektronikus hírközlés körében történő értelmezésének szándéka. Az információ-, adatvédelem[274] körében értelmezett kriptográfiai algoritmusok, protokollok, egyéb eljárások és módszerek annak csak az egyik pillérét, azaz az elektronikus logikai védelmi[275] komponenseit jelentik, amelyek mellett legalább annyira lényeges az adminisztratív,

---

[269] Lásd: VAJDA István (1998): *Kriptográfia bevezető*. Budapest: BME VIK. 87. Online: http://www.hit.bme.hu/~buttyan/courses/BMEVIHI4363/theory.pdf (Letöltés ideje: 2024. február 20.)

[270] MUHA Lajos – KRASZNAY Csaba (2018): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem. 85. Online: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/12932 (Letöltés ideje: 2024. február 15.)

[271] Ibtv. 1. § (1) bek. 8. pont *„bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;"*

[272] Ibtv. 1. § (1) bek. 39. pont

[273] Ha a „*Digitális jogokról és elvekről szóló európai nyilatkozat*" 16. pontját vizsgáljuk a 2.4.2. alfejezet szerint, akkor kijelenthető, hogy az Ibtv.-ben lefektetett fogalomhasználat 11 év múltán is aktuális és szakszerű mind a hazai, mind az uniós jogalkotás szintjén, mely szövegezésébe nem kisebb szaktekintélyek vettek részt, mint Dr. Muha Lajos ny. ezredes, Dr. Krasznay Csaba, és Dr. Bodó Attila Pál.

[274] *„A védelem – a magyar nyelvben – tevékenység, illetve tevékenységek sorozata, amely arra irányul, hogy megteremtse, fejlessze, vagy szinten tartsa azt az állapot, amit biztonságnak nevezünk. Tehát a védelem tevékenység, amíg a biztonság egy állapot.*" MUHA Lajos (2007): *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme*. Doktori (PhD) értekezés. Budapest: ZMNE. 11. Online: http://real-phd.mtak.hu/74/1/1228916.pdf (Letöltés ideje: 2024. február 12.)

[275] Ibtv. 1. § (1) bek. 34. pont

fizikai és személyi védelmi intézkedések, biztonsági feltételek biztosítása, azonban az utóbbi két tárgykör nem képezik az értekezés tárgyát, az adminisztratív védelem az adtavédelmi normák tekintetében elemzésre kerül.

A kriptográfiai titkosítás, azaz a rejtjelezés olyan eljárás, amely lehetővé teszi, hogy egy sértetlen, hiteles rejtjelezett üzenet vagy egyéb adat biztonságosan kerüljön továbbításra, tárolásra anélkül, hogy jogosulatlan harmadik fél számára értelmezhetővé válna.[276] Elektronikus hírközlő hálózatban, infokommunikációs szoftverekben (például alkalmazásszolgáltatásban) a titkosítás folyamata során a küldő nyílt üzenete a rejtjelezés, vagyis adott protokollnak megfelelő matematikai műveletek, algoritmusok alkalmazása során egy titkos/nyilvános kulccsal ellátott rejtjelezett üzenetté „kódolódik", melyet csak a megfelelő titkos megoldó kulcs birtokában tud visszafejteni a címzett, így számára nyíltan értelmezhetővé téve az üzenetet, egyéb adatot. A rejtjelezés (titkosítás) és az üzenet tartalmának nyílt visszafejtése (megoldás) történhet a kommunikáló felek végponti infokommunikációs eszközein, ekkor végpont-végpont titkosításról (E2EE) beszélünk. Továbbá megkülönböztethető még a kliens-szerver titkosítás (C2SE), mikor a két fél közé beékelődik egy szerver, mely feladata, hogy a küldő által elküldött titkosított üzenetet megfejtse, majd azt a címzett fél számára újra rejtjelezett formában továbbítsa, mely üzenetet a címzett fél tud visszafejteni. Az értekezés a kriptográfia komponensei közül az elsőt, azaz a titkosítást, azon belül is az algoritmus alapú titkosítást hivatott részletesebben vizsgálni, amely fontos szerepet játszik a biztonságos online kommunikációban is. A titkosítás megnehezíti a külső, legtöbbször jogosulatlan fél számára az adatok megismerését, és értelmezését, így a felhasználók adatai biztonságban maradhatnak, megfelelve az egyre szigorodó adatvédelmi előírásoknak, azonban egyben kihívást is jelentve az LI számára. A kriptográfiai algoritmusokat és protokollokat használ a fentiek megvalósítása érdekében. [277] A rejtjelező algoritmusok két fő típusra

[276] „*Egy üzenet titkossága azt jelenti, hogy csak a kívánt partner számára rekonstruálható annak nyílt tartalma. Egy dekódolt üzenet hitelessége azt jelenti, hogy a kódolt üzenet módosítatlanul, eredeti állapotában érkezett meg a dekódolóhoz, s a tartalmából kiderül, hogy a partner küldte. Szemléletes példával illusztrálva: ha a postás felbontja a levelet, akkor annak tartalma már nem titok, de ha a levél tartalmát nem módosítja, s úgy kézbesíti, az üzenet még hiteles marad*." BUTTYÁN Levente – VAJDA István (2005): *Kriptográfia és alkalmazásai*. Budapest: Typotex. 17-18.

[277] *„Az algoritmusok olyan függvények, amelyek a titkosítás és a visszafejtés során kerülnek felhasználásra. A protokollok lépések sorozatát foglalják egybe, amelyek segítségével két vagy több partner megvalósítja a kitűzött feladatokat. A két építőelem kölcsönösen kiegészíti egymást. A protokollok magukba építik az algoritmusokat, az algoritmusok pedig támaszkodnak a protokollok által kialakított kapcsolódási pontokra*." Takács Péter (2009): *Kriptográfiai protokollok formális vizsgálata a CSN logikai rendszer bővítésével*. Doktori (PhD) értekezés. Debrecen: DE ITDI. 6. Online: https://dea.lib.unideb.hu/server/api/core/bitstreams/7eca2ade-7dfa-4d4f-9360-c12c8f592019/content (Letöltés ideje: 2024. február 20.)

oszthatóak, mégpedig a szimmetrikus és az aszimmetrikus kulcsú titkosítás vonatkozásában, illetve van számos további eljárás, módszer melyek az 1. számú mellékletben[278] kerülnek általánosan ismertetésre. Az 1. számú melléklet tartalmi és fogalomhasználati ismerete ajánlott az értekezés későbbi fejezeteiben használt kriptográfiai fogalmak megértéséhez. Jelen részfejezetben a digitalizáció, a technológiai fejlődés hatására kialakult poszt-kvantumkriptográfia általános jellemzői kerülnek innovatív szemléletben bemutatásra.

Poszt-kvantumkriptográfia:

A nem is olyan távoli jövőbe tekintve már küszöbön áll a rendkívül nagy számítási igénnyel bíró, ámde rendkívül magas kriptográfiai védelmet biztosító poszt-kvantumkriptográfia. A hagyományos kriptográfiai módszerek, mint például az RSA[279] a matematikai problémák nehézségén alapulnak, míg a kvantumtitkosítás a kvantummechanika jelenségeire, mint például az összefonódásra és a mérésre támaszkodik. A poszt-kvantumtitkosításnál a két kommunikáló fél összefonódással előállít egy csak általuk ismert kulcspárt. A rejtjelezés során a kulcs egyik felét a küldő fél alkalmazza, míg a kulcs másik felét a fogadó fél használja a visszafejtéshez. Ha valaki megpróbálja elfogni vagy lemásolni a hálózaton továbbított rejtjelezett adatot, a kvantummechanikai jelenségek miatt az összefonódott kulcs megváltozik, és a kommunikáció zavarossá válik, feltárva a jogosultak számára a támadást.[280] Magyarországon az Ibtv. 1. § (1) bek. 49. pontjának 2022. július 01-jétől hatályba lépett módosítása következtében definiálja, értelmezi is a poszt-kvantumtitkosítás[281] fogalmát. A NIS2 törekvéseivel összhangban az Ibtv. 1. § (1) bek. 50. pontja alapján a kormányzati célú hírközlőhálózatok igénybevételére kötelezettek, a hitelintézetekről és a pénzügyi vállalkozásokról szóló törvény szerinti bankok, valamint a lakosság ellátása szempontjából kiemelten fontos közműszolgáltatók, közszolgáltatók körében[282] az SZTFH elnökének vonatkozó rendelete alapján – amely még nem

[278] 1. számú melléklet: *Főbb kriptográfiai protokollok, algoritmusok, eljárások általános ismertetése*

[279] RSA: az algoritmus feltalálói Ron Rivest, Adi Shamir és Leonard Adleman nevének kezdőbetűiből származik.

[280] CHEN, L.– JORDAN, S. – LIU, Y.– MOODY, D. – PERALTA, R. – PERLNER, R.- DANIEL, S. (2016): Report on Post-Quantum Cryptography. NIST.IR 8105. 1-2. Online: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (Letöltés ideje: 2024. február 16.)

[281] poszt-kvantumtitkosítás: a matematikailag valószínűsíthetően igazolható, kvantumszámítógép által megvalósított támadás ellen a hagyományos kriptográfiai alkalmazáson felüli poszt-kvantum alkalmazást, illetve megoldást nyújtó titkosítás, amely során a két végpont közötti kommunikáció felhasználásával, az adatátvitellel megosztott kulcsot hoz létre a két végfelhasználó között, anélkül, hogy a kulcsot jogosulatlan harmadik fél megismerné

[282] Ezen szolgáltatók egy része a kritikus információs infrastruktúrák körébe tartozó entitás, melyek fokozottabb védelme még inkább indokolt és egyben jogszabályi kötelezettség is például az Ibtv. alapján. Lásd: BODÓ Attila Pál – BOGNÁR Balázs (2019): *Kritikus információs infrastruktúrák védelme*. Budapest: NKE. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/13801/Kritikus%20informacios%20infrastrukturak%20vedelme_Eves%20tovabbkepzes_felelos%20vezeto.pdf?sequence=3&isAllowed=y (Letöltés ideje: 2024. február 16.); KASSAI Károly (2023): A honvédelmi célú elektronikus információs

került kiadásra – kijelölt szervezetek számára kötelező lesz a poszt-kvantumtitkosítás. [283] A poszt-kvantumkriptográfia jelenleg fejlesztés és szabványosítás alatt álló technológia, és csak korlátozottan alkalmazható a gyakorlatban. Az NIST[284] szabványosítással kapcsolatos 2016-ban indított pályázata keretében,[285] 2022-ben bemutatta az első négy olyan poszt-kvantumkriptográfiai szabványjelölt algoritmust (Dilithium, Falcon, Kyber, SPHINCS+), amelyek ellenállóak lehetnek a kvantumszámítógépekkel szemben is.

2.7.2. A kriptográfiára ható főbb kihívások

Egyfajta előkérdés tisztázása érdekében a kriptográfiára ható főbb kihívások vizsgálatát megelőzően, a rejtjelezett közlések tekintetében az üzenetek értelmezhető tartalmához való jogosult hozzáférés alapján szükséges elhatárolni egymástól az adatkezelésre jogosultak feladók/ címzettek körét, valamint a harmadik felek körét, azon belül is a kvázi jogosult felek és a jogosulatlan felek halmazát. Jogosulatlan félként a támadók azonosíthatók, amelyek tevékenysége például anyagi haszonszerzés, károkozás, ellenérdekelt információgyűjtés és hírszerzés, valamint terrorizmus során jelentkezhet. Kvázi jogosult félként azonosíthatóak az LI végzésére jogosult szervezetek, valamint az adatkezelést, -feldolgozást végző szervezetek, például az alkalmazásszolgáltató. Az előkérdés tisztázását követően hipotetikusan megállapítható, hogy a jogosultalan támadó alapfeltételezés szerint részletesen ismeri a kriptográfiai algoritmust, a rejtjelezett üzenet megfejtéshez szükséges titkos kulcs kivételével. Ez alapján a rejtjelező algoritmus által nyújtott védettség nem haladhatja meg a titkos kulcs védettségének szintjét, vagyis a titkos kulcs az a kiemelten védett információ, amely gyorsan és megfelelő időközönként cserélhető, míg a rejtjelező rendszer többi elemét hosszabb ideig nem szükséges nagyobb ráfordítás mellett megváltoztatni. Tehát a kriptográfiai algoritmusok vonatkozásában nem azoknak a titkossága a mérvadó, hanem az általuk generált kulcsok

---

rendszerek fejlesztéséhez szükséges, továbblépést megalapozó vizsgálat – egy zöld könyv kialakításának támogatása. *Military and Intelligence CyberSecurity Research Paper*, 2(5). Online: https://hhk.uninke.hu/document/hhk-uni-nke-hu/MICRP%202022_5%20Kassai%20K%C3%A1roly%20-%20A%20honv%C3%A9delmi%20c%C3%A9l%C3%BA%20elektronikus%20inform%C3%A1ci%C3%B3s%20rendszerek%20fejleszt%C3%A9s%C3%A9hez%20sz%C3%BCks%C3%A9ges,%20tov%C3%A1bbl%C3%A9p%C3%A9st%20megalapoz%C3%B3%20vizsg%C3%A1lat%20%E2%80%93%20Egy%20z%C3%B6ld%20k%C3%B6nyv%20kialak%C3%ADt%C3%A1s%C3%A1nak%20t%C3%A1mogat%C3%A1sa.pdf (Letöltés ideje: 2024. február 16.);

[283] DR. GYÖMBÉR Béla (2022): *Poszt-kvantumtitkosítást vezetnek be Magyarországon*. Jogalap, Online: https://jogalappal.hu/poszt-kvantumtitkositast-vezetnek-be-magyarorszagon/ (Letöltés ideje: 2024. február 16.)

[284] NIST: National Institute of Standards and Technology (USA) – Nemzeti Szabványügyi és Technológiai Intézet

[285] *Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms*. NIST. 2022. Online: https://csrc.nist.gov/News/2016/Public-Key-Post-Quantum-Cryptographic-Algorithms (Letöltés ideje: 2024. február 16.)

védelme. Egy támadás során a megfejtéshez szükséges kulcsok megismerése és alkalmazása a támadók célja, így hozzáférve a rejtjelezett kommunikáció visszafejtett, eredeti, számukra is értelmezhető tartalmához. Az értekezésben a támadók által alkalmazható módszerek közül a nyilvános elektronikus hírközlő hálózaton (csatornán) végbemenő rejtjelezett kommunikáció vonatkozásában csak az algoritmikus típusú támadási módszerek kerülnek áttekintésre.

Passzív támadási módszerként nevesíti a szakirodalom az úgynevezett „lehallgatást", azaz a passzív DPI jellegű támadást a kommunikáló felek közé történő szerver, vagy hálózati oldali „közbeékelődéssel", a hálózaton átfolyó kommunikáció monitorozását, analizálását, amely során a támadó a nyilvános csatornán áramló adatfolyam birtokába jut. Passzív támadás során nem kerül sor a protokoll működésébe való beavatkozásra, csak a csatornában folyó üzenetek megismerése történik, azok módosítása nem. A védett információ rejtjelezése ez esetben a nyílt hálózaton továbbított kommunikáció eredeti tartalmához való jogosulatlan hozzáférés megakadályozását biztosítja. A rejtjelezés célja alapvetően a passzív támadások megakadályozása.[286] Aktív támadás esetén a támadó alapvető célja a közlemény vagy részeinek észrevétlen módosítása, kicserélése vagy törlése. A támadó ténylegesen beavatkozik a protokollba. Ismert aktív támadási forma még a hamis identitáskeltés, azaz a jogosult fél megszemélyesítése, fiktív jogosultság kreálása, amely során a jogosult fél identitásának látszatát keltve történik a védett információk megszerzése. A támadó malware-ek, spyware-ek, azaz rosszindulatú kémprogramok, trójai programok, férgek alkalmazásával igyekszik hozzáférni a számára is értelmezhető védett információkhoz.[287] Az aktív támadások kriptográfiai algoritmikus módszerekkel nem megakadályozhatók, azonban protokollok alkalmazásával észlelhetővé, azonosíthatóvá tehetők. További klasszikus támadási forma az aktív MitM, amely során a támadó képes az áldozat és a kommunikációs partner közötti adatátvitelt ellenőrizni, megváltoztatni és manipulálni, akár azt a látszatott keltve, mintha az áldozat közvetlenül kommunikálna a partnerrel.[288] Érdemes megvizsgálni az EU jogpolitikai törekvéseinek egyes szemelvényeit is a kriptográfiát, azon belül is a bizalmasságot érintő kihívások tekintetében. Mint az már a fentiekben is hivatkozásra került az e-hírközlési

[286] KAUR, Roop Kamal – KAUR, Kamaljit (2015): A New Technique for Detection and Prevention of Passive Attacks in Web Usage Mining. I. *Journal of the Western Mystery Tradition*, 15(6), 55. Online: https://www.mecs-press.org/ijwmt/ijwmt-v5-n6/IJWMT-V5-N6-7.pdf (Letöltés ideje: 2023. december 20.)

[287] KAHATE 2013: 15-16

[288] KAUFMAN, C. - PERLMAN, R. - SPECINER, M. (2017): *Network Security: Private Communication in a Public World.* Delhi: Pearson India Education Services Pvt. 9. Online: https://dokumen.pub/network-security-private-communication-in-a-public-world-2nd-ed-14th-printing-9780130460196-9789332578210-9789332586000-0076092018469-0130460192.html (Letöltés ideje: 2024. február 20.)

adatvédelmi rendelet javaslat (15) preambulumbekezdése rendelkezik az elektronikus hírközlési adatok bizalmasságáról méghozzá adatvédelmi aspektusból, mely negatív megközelítésből azt jelenti, hogy a kommunikáció akár emberi, akár automatizált gépi adatkezelés eredményű megzavarása, a jogosult felek hozzájárulása nélkül tilos. Azonban kontextusba is helyezi azt annak kihívásaival, amely átfogó értelmezése érdekében a javaslat bevezeti és magyarázza a technológiai fejlődésből adódó hatásokra is reflektáló „kifürkészés"[289] fogalmát, mely jogosulatlanság esetén támadó jellegű lehallgatásként, törvényes végrehajtás esetén pedig LI tevékenységként azonosítható.

A rejtjelező algoritmusok titkossága, azaz bizalmassága – ebből a szempontból hatékonysága – tekintetében el kell egymástól határolni a gyakorlati és a feltétlen titkosságot. Az algoritmus gyakorlati titkosságot biztosít, ha feltöréséhez irreálisan nagy számítási kapacitási igény szükséges, de meg van rá az elméleti lehetőség, például kimerítő keresés során. Az algoritmus feltétel nélküli titkosságot biztosít, ha a feltörés érdekében megszerezhető információk sem elegendőek a sikeres rejtjelfejtéshez, bármekkora számítási kapacitással is bírjon a támadó. A ma ismert egyetlen feltétel nélküli titkosságot biztosító algoritmus az On Time Pad, ami azonban gazdaságossági és szervezési okokból általánosan nem terjedt el.[290] A vizsgált szakirodalom szerint általános kihívás a kriptográfiai algoritmusok és protokollok folyamatos elavulása a technológiai, IKT fejlődés okán, azonban ez nem jelenti egyben a titkosság gyakorlati sérülését.[291] Ezen gondolatot kiegészítem a személyes adatvédelem folyamatosan szigorodó normatív elvárásaival, mely kifejtésére, bizonyítására a későbbiekben kerül sor.

A jövő egyik legambivalensebb kriptográfiai kihívása a kvantumszámítás, mely lényegében elavulttá, törhetővé tenné például az RSA és az ECC kriptográfia használatát.[292] Azonban

[289] Lásd: E-hírközlési adatvédelmi rendelet javaslat (15) preambulumbekezdés

[290] VAJDA 1998: 91

[291] „*Minden jelenleg alkalmazott negyedik generációs titkosítás tökéletlen […], tehát feltörhető, viszont ez jó esetben időben lehetetlen feladat. Megfelelő algoritmusnak tekintjük például azt, ami a Föld összes számítógépének együttes számítási kapacitásával évezredek-évmilliók alatt törhető fel. Ezek a nagy számok kifejezetten hangzatosak, de valójában – a számítási kapacitás Moore-törvény szerinti növekedése és kódtörési feladatok többezer magos grafikai processzorokra való áthelyezése miatt – már az eredmény, hogyha évtizedekig megfelelő védelmet nyújt az adott algoritmus az adatainknak. Így folyamatosan avulnak el a régebben biztonságosnak tekintett algoritmusok. […] A probléma megoldása mindössze annyi, hogy a korábbi algoritmusokat a kor színvonalának megfelelő jobb algoritmussal helyettesítjük, az adatokat újrakódoljuk."* SZÁDECZKY Tamás (2016): Kriptográfiai protokollok megfelelősége; *Hadmérnök*, 11(4), 179. Online: http://real.mtak.hu/49982/1/164_15_szadeczky.pdf (Letöltés ideje: 2024. február 16.)

[292] DR. SAARINEN, O. (2023): Intro to Side-Channel Security of NIST PQC Standards; NIST PQC Seminar, 04 April 2023. 2-3. Online: https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/pqc-seminars/presentations/2-side-channel-security-saarinen-04042023.pdf (Letöltés ideje: 2024. február 16.)

jelenlegi ismeretinek szerint a kvantumszámítógépekkel szemben továbbra is biztonságos maradhat a szimmetrikus kulcsú titkosítás (nagyobb kulcsméret esetén) és a hash függvény (nagyobb output érték esetén).[293] A vizsgált források alapján a kvantumszámítással nem ellenálló kriptográfiai eljárások a közeljövőben elavulttá fognak válni, azonban 2030-ig nem várható a nagy teljesítményű kvantumszámítógép megjelenése.[294]

2.7.3. Kliens-szerver (C2SE)/ Végpont-végpont (E2EE) kriptográfia

A C2SE egy olyan titkosítási koncepció, amelyet a végponti forrás- vagy célkliens és a szerver, például PC/SaaS felhő közötti kommunikáció biztonságosabbá tételére alkalmaznak. Az OSI-modell[295] szerinti 4. szállítási réteg általános protokolljává a szabványosított SSL/TLS[296] protokoll vált. Főként olyan hírközlő hálózatoknál alkalmazzák, amelyen a felek nem rendelkeznek teljes ellenőrzéssel a hálózat és a végponti kliensek között. C2SE alkalmazásának tipikus példája az internet-hozzáférési szolgáltatás. A technológia használata különösen elterjedt a videókonferencia-alkalmazásokban, mint például a Skype és a Webex esetében[297], azonban mint az a témaválasztás indoklásában is megállapítható, ezen szolgáltatások is elkezdtek átállni az E2EE-re.[298] A C2SE-t alkalmazó platformok esetében a szerver kompromittálásával a támadó számára rejtjelezetlen formában hozzáférhetővé válhatnak az azon kezelt védett adatok, hiszen a kompromittált szerver felhasználásával képes mind passzív, mind aktív támadásokat végrehajtani.[299] A C2SE-vel védett kommunikációs infrastruktúra kitettségének kockázata egyszerű hanyagságból is eredhet. Sajtóinformációk alapján 2019-ben

---

[293] CHEN, L.– JORDAN, S. – LIU, Y.– MOODY, D. – PERALTA, R. – PERLNER, R.- DANIEL, S. (2016): *Report on Post-Quantum Cryptography*. NISTIR 8105. 2. Online: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (Letöltés ideje: 2024. február 16.)

[294] PFEIFFER Szilárd (2023): *Már ma is törhető az RSA titkosítás*?. HSWS. Online: https://www.hwsw.hu/hirek/65635/rsa-titkositas-kvantumszamitogep-feltores-kod-algoritmus.html (Letöltés ideje: 2024. február 16.); FLACHNER Balázs (2023): *Tényleg itt a minden titkosítást feltörő kvantumszámítógép?*. Telex. Online: https://telex.hu/tudomany/2023/02/11/kvantumtechnologia-kvantumszamitogep-rsa-eljaras-titkositas-kriptografia (Letöltés ideje: 2024. február 18.); ZENTAI Dániel (2021): *Kriptográfia a kvantumszámítógépek világában*. Budapest: „Infokommunikáció 2021" Konferencia kiadvány és korreferátum gyűjtemény, *Hírvillám*, 12(3), 201. Online: https://comconf.hu/kiadvany/H%C3%ADrvill%C3%A1m_2021_3.pdf (Letöltés ideje: 2024. február 18.)

[295] OSI: Open Systems Interconnection – nyílt rendszerek összekapcsolása. Lásd: TANENBAUM, Andrew S. – WETHERALL, David J. (2013): *Számítógép-hálózatok*. Budapest: Panem Könyvek. 60-61. Online: http://gbb2.atw.hu/kieg/szte/tanenbaum_szamhalo.pdf (Letöltés ideje: 2024. február 18.)

[296] TLS: Secure Sockets Layer/ Transport Layer Security (TLS 1.3 szabvány: RFC-TLS13-28)

[297] HORMAN aka HORMS, Simon (2005): *SSL and TLS An Overview of A Secure Communications Protocol; Security*. Canbera: Mini-Conf at Linux.Conf.Au, 1. Online: https://projects.horms.net/projects/ssl_and_tls/stuff/ssl_and_tls.pdf (Letöltés ideje: 2024. február 18.)

[298] BÁNYÁSZ et al. 2022: 26

[299] ALWEN, Joël (2020): *End-to-End Encryption vs. Client-to-Server Encryption*. Wickr. Online: https://wickr.com/end-to-end-encryption-vs-client-to-server-encryption/ (Letöltés ideje: 2024. február 18.)

több mint 300 millió WeChat és QQ chat applikáción továbbított privát üzenet szivárgott ki egy rossz konfigurációs szerverbeállítás okán.[300] Többek között az alkalmazásszolgáltatások biztonsága iránti növekvő kereslet, valamint az adatvédelmi előírások szigorítása szükségessé tette az E2EE általános elterjedését. Az optimálisan alkalmazott E2EE technológia fokozott biztonsági paraméterein túl, egyben fenntartható választ kínál a támadásokkal szemben.[301]

A modern E2EE során az adatok rejtjelezése és visszafejtése a kétoldalú kommunikáció végső pontjain, például magában az okostelefonra telepített alkalmazásszolgáltatás szoftverében történik. Célja, hogy védelmet nyújtson a köztes hálózatokon történő adatátvitel során úgy, hogy a közlés tartalma a kiszolgáló szerveren sem kerül kicsatolásra, kezelésre rejtjelezetlen formában. Csak a feladó és a címzett rendelkezik a rejtjelezett adatok megfejtéséhez szükséges titkos kulcsokkal.[302] Az E2EE során az adatok a feladó végponti eszköz elhagyása előtt kerülnek rejtjelezésre a kulccsal, mely csak a címzett titkos privát kulcsával fejthetők meg, amikor az hozzáférhetővé válik a fogadó végponti eszközön. A támadók nem férhetnek hozzá a szerveren kezelt adatokhoz értelmezhető formában, mert nem rendelkeznek az adatok visszafejtéséhez szükséges privát kulcsokkal.[303] Napjainkra az E2EE alkalmazása általánosan elterjedt az online kommunikációban, így az alkalmazásszolgáltatások körében is, mely részletesebb elemzésére az értekezés későbbi alfejezetében kerül sor. Az E2EE hátrányai közé sorolható például a végpontok meghatározásának kitettsége, mivel a visszafejtés csak a definiált végpont számára hozzáférhető privát kulccsal biztosítható, így nélkülözhetetlen azok egyedi és egyértelmű meghatározása. Amennyiben támadók a végpontokat kompromittálják hozzáférhetnek a titkos kulcshoz, így képessé válhatnak a rejtjelezett üzenetek, adatok visszafejtésére. Attól még, hogy a hálózaton rejtjelezett közlések áramlanak, azok kísérő-,

[300] LIAO, Shannon (2019): *Over 300 million Chinese private messages were left exposed online*. The Verge. Online: https://www.theverge.com/2019/3/4/18250474/chinese-messages-millions-wechat-qq-yy-data-breach-police (Letöltés ideje: 2024. február 19.)

[301] Az első globálisan elterjedt, és 1991-ben az interneten is publikált E2EE koncepcióban is alkalmazható kriptográfiai protokollt Philip R. Zimmermann hozta létre Pretty Good Privacy (a továbbiakban: PGP) néven, amely a világ legszélesebb körben elterjedt e-mail protokolljává vált.[301] Azóta számos más és jóval fejlettebb E2EE protokoll jelent meg, többek között a Telegram által alkalmazott MT Proto, a Signal, Facebook Messenger és WhatsApp által is alkalmazott Signal Protocol, valamint a Viber Protocol. *Phil Zimmermann*. The Center for Internet and Society at Stanford Law School. Online: https://cyberlaw.stanford.edu/about/people/phil-zimmermann (Letöltés ideje: 2024. február 19.)

[302] SCHNEIER, Bruce (1996*): Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C*. New Jersey: John Wiley & Sons, 313-314. Online: https://dokumen.pub/applied-cryptography-second-edition-protocols-algorithms-and-source-code-in-c-2nbsped.html (Letöltés ideje: 2024. február 19.)

[303] BLAISE, O. – AWODELE, O. – YEWANDE, O. (2021): An Understanding and Perspectives of End-To-End Encryption; *IRJET International Research Journal of Engineering and Technology*, 8(4), 1086. Online: https://www.researchgate.net/publication/350850077_An_Understanding_and_Perspectives_of_End-To-End_Encryption (Letöltés ideje: 2024. február 19.)

metaadatainak egy része továbbra sem E2EE rejtjelezett, ami szintén hasznos információkkal szolgálhat a támadók számára. Az E2EE kellő biztonságos a kor adat- és információvédelmi elvárásainak megfelelően. Bár az E2EE fokozottan biztonságos kriptográfiai technológia, a kvantumszámítás idővel annak elavulásához vezethet.[304] E2EE esetén a rejtjelezett adatok a kiszolgáló, például az elektronikus hírközlés- vagy az alkalmazásszolgáltató által szerveroldalon a C2SE koncepciótól eltérően, titkosítatlan formában nem kicsatolhatóak, hozzáférhetőek a támadók számára, így megelőzve egy például egy DPI támadás sikereségét.[305]

A részfejezet következtetéseként megállapítható, hogy a fentiek alapján adat- és információvédelmi szempontból az alkalmazásszolgáltatások tekintetében indokolt a mobilinternet hálózat (elektronikus hírközlési szolgáltatás) védelme érdekében használt C2SE és az alkalmazásszolgáltatások által biztosított E2EE koncepció együttes alkalmazása, hiszen így a szerveroldalon kicsatolható forgalom például DPI támadás során az E2EE-nek köszönhetően nem fejthető vissza jogosulatlan fél által, a megfelelő titkos kulcs jogszerűtlen ismerete nélkül. A C2SE koncepció alkalmazása a mobilhálózatban pedig többlet biztonságot jelent, hiszen a szerveroldalon kívül a kommunikáció metaadatai nyíltan nem hozzáférhetőek. Azonban ez a kvázi jogosult harmadik felek tevékenysége, azaz a nemzetbiztonsági és bűnüldözési célú LI során kihívást okozhat, mely technológiai és normatív szempontú elemzése, mind az elektronikus hírközlési – mobilinternet – szolgáltatás, mind az alkalmazásszolgáltatások tekintetében az értekezés során, a meghatározott új kutatási módszertan során átfogóan vizsgálatra, elemzésre kerül a tudományos következtetések levonása, azok bizonyítása érdekében, összhangban az értekezés célkitűzéseivel.

2.8. Részkövetkeztetések

Az értekezés érdemi tartalmi első része, azaz a 2. fejezet fő tárgyköre az LI garanciális, szervezetrendszeri, fogalmi és módszertani hátterének áttekintésére egyfajta felvezetőként, a szükséges alapvető ismeretek tárgyalásaként, a további fejezetekben szereplő kutatási cselekmények előkészítése céljából került sor. A fejezeten belül előkérdésként értelmezésre

[304] LUTKEVICH, Ben – BACON, Madelyn (2021): End-to-End Encryption (E2EE). TechTarget. Online: https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE (Letöltés ideje: 2024. február 20.)

[305] Lásd: TÓTH Tamás (2023): Actualities of certain security aspects of cryptography with regard to information societies. *National Security Review*, 9(1), 107-118. Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2023_1_NSR.pdf#page=107 (Letöltés ideje: 2024. február 16.)

került a „nemzetbiztonsági cél” tartalma, vizsgálat tárgyát képezte az LI szabályozásának nemzetközi és hazai keretrendszere, az LI alapvető jogi és adatvédelmi garanciális hátterének áttekintése, az EU digitális piaci és adatvédelmi stratégiai célkitűzései hatásainak elemzése az LI aspektusából. Továbbá az LI hazai szervezetrendszerének és általános normatív háttérének általános ismertetése, információelméleti háttere és annak átültetése a normatív környezetbe, egyes főbb módszerei, eljárásai, a szükséges kriptográfiai alapismeretek és kihívásainak áttekintése. Az egyes al- és részfejezetekben a meghatározott kutatási módszertan alkalmazása során elvégzett cselekmények alapján az alábbi fő részkövetkeztetések vonhatók le:

2.1. alfejezet: A stratégiai evolúciós elemzés alapján a „nemzetbiztonsági érdek”, így az abból absztrahálható „nemzetbiztonsági célzat” tartalma dinamikusan, a kor elvárásai mentén változik, alakul a hagyományos területektől elmozdulva a digitális kihívások (kibervédelem, űrtechnológia), vagy éppen a K+F+I (védelmi ipar, nemzetbiztonsági ipar, KNBSZ IKK, MiLab, InfoLab, TIF) irányába. Az elvégzett további kutatási cselekmények alapján **a „nemzetbiztonsági célzaton” a disszertációs kutatómunka során az alaki megjelenést és egyben a funkcionális értelmezést értem**, azaz az Nbtv. szerinti nemzetbiztonsági szolgálat külvilág számára is megjelenő, érzékelhető cselekményeit. A „nemzetbiztonsági célú” fogalomkör részletes elemzése azért volt indokolt és szükségszerű, mert az uniós jog megkülönbözteti és élesen elkülöníti **a hatálya alá nem tartozó nemzetbiztonsági célú és az uniós jog hatálya alá tartozó bűnüldözési célú tevékenységet, együttműködést.**

2.2. alfejezet: A tagállamok míg a bel- és igazságügyi együttműködést szupranacionális szintre emelték, addig ez a nemzetbiztonsági tevékenységi körben nem érvényesül, tehát az keményen a nemzeti jog hatálya alá tartozik, azonban annak alapvető jog korlátozó eljárásait – mint például a titkos információgyűjtés eszközrendszerén belül értelmeztet LI-t – megfeleltetve a nemzetközi jog szintjén meghatározott és az **Alaptörvényben, valamint további törvényekben** adaptált emberi és alapvető jog védelmi garanciális szabályoknak. Az LI-vel kapcsolatos műszaki ajánlásokat, elvárásokat **szabványokban határozzák meg egységes és transzparens** nemzetközi szintű műszaki jellegű követelményrendszert támasztva. Állami szinten az LI-t a nemzetközi jog és annak állami jogba is adaptált, átültetett garanciáihoz igazított **törvényi szinten szabályozzák,** az arányosságra, szükségességre, valamint a védendő közérdekekre tekintettel. Az LI-re vonatkozó részletszabályok pedig rendszerint **kormányrendeleti szinten kerülnek deklarálásra**. [H1] Az ennél mélyebb nemzeti szintű szabályozás rendszerint a közjogi szervezetszabályzó eszközök, együttműködési

megállapodások körébe tartozik, amelyek részletszabályainak tartalma rendszerint minősített adat, ami nem képezi az értekezés vizsgálatának tárgyát.

2.3. alfejezet: Megállapítást nyert, hogy Magyarország az Alaptörvény, és az azzal összefüggésben megalkotott törvényi szabályozás alapján tiszteletben tartja az ember sérthetetlen és elidegeníthetetlen alapvető jogait és ezeket nemzetbiztonsági célú LI során csak más, például a nemzetbiztonság alkotmányos közérdekének érvényesülése érdekében, szükséges és arányos módon korlátozhatja. Megállapítást nyert, hogy ugyan a nemzetbiztonsági tevékenység szabályozása nem tartozik az uniós jog hatálya alá, azonban az arra való hivatkozással, mint közérdekű cél korlátozható a személyes adatok védelme, megfelelő garanciális szabályok mellett, például nemzetbiztonsági célú LI során. Ennek speciális adatvédelmi keretei levezethetőek a GDPR és az e-hírközlési adatvédelmi irányelvből, amely leképződése a hazai jogban a nemzetbiztonsági célú adatkezelés szabályozása érdekében megjelenik az Infotv. általános rendelkezésiben, valamint az Nbtv. vonatkozó részletszabályaiban törvényi szinten.

2.4. alfejezet: Megállapításra került, hogy az IKT környezet fejlődéséből adódó Unió digitális egységes piacának stratégiai célkitűzéseivel kapcsolatban vizsgált hatályos jogszabályok (DMA, DSA, GDPR, e-hírközlési adatvédelmi irányelv, Hírközlési Kódex, NIS2) és jogszabálytervezetek (e-hírközlési adatvédelmi rendelet javaslat) alapján aktuálisan és prognosztikusan koherens, következetes jog- és szakpolitikai törekvést követnek a digitális, IKT termékek és szolgáltatások elterjedése érdekében, amely elsősorban gazdaság-, társadalompolitikai célkitűzéseken alapul. A stratégiai célok eléréséhez elengedhetetlen a felhasználói bizalom megléte, erősítése az IKT termékek és szolgáltatások iránt, melyhez nélkülözhetetlen a digitális biztonság megteremtése. Ehhez normatív és technológiai elektronikus információ-, kibervédelmi intézkedésekre van szükség, amelynek az értekezés szempontjából érdemi technológiai eleme a kriptográfia, normatív eleme pedig a személyes adatvédelem. Megállapítható, hogy az uniós jog terrénumán az elektronikus információvédelem (NIS2) az általános adatvédelmi szabályozásnak (GDPR) egy speciális jogterületévé vált a digitalizáció hatására a személyes adatvédelem szempontjából.

Továbbá a 2.1. és 2.4. alfejezet alapján a 2018/2020-ban megfogalmazott és 2030-ig szóló uniós digitális piacra, hírközlésre vonatkozó stratégia célkitűzéseket összevetve a 2020-tól hatályos

hazai Stratégiával[306] komplex szemléletű következtetésként megállapítható egyfajta direkt, vagy indirekt harmónia az EU digitalizációs/ hírközlési stratégiai célkitűzései – melynek szerves részét képezi a normatív és technológiai adatvédelem, -biztonság – és Magyarország biztonsági átfogó stratégiai célkitűzései között. Ami azért is figyelemreméltó, mivel a korábbi 2012-es Stratégia felülvizsgálatára a kormányt a terrorizmus, illegális migráció, technológiai, hibrid, kiberbiztonsági kihívások indukálták. **Tehát következtetésképpen megállapítható, hogy a digitalizációban, az IKT technológiákban rejlő új típusú biztonsági kihívások és lehetőségek mind az Unió szintjén, azaz a közösségi jog terrénumán, mind Magyarország szintjén, azaz a tagállami jog terrénumán átfogó digitalizációs/ biztonsági stratégiai felülvizsgálatot, „újragondolást" eredményeztek, amely az uniós és a magyarországi jogalkotásban is megtestesült** – azonban ez álláspontom alapján nem lehet egy statikus állapot, a felülvizsgálatnak folyamatosnak, dinamikusnak kell lennie, alkalmazkodva például a digitális IKT környezet változásaihoz.

2.5. alfejezet: Tételes jogszabályelemzés keretében áttekintésre került az LI hazai szervezetrendszere, annak központi szolgáltató szervezeteként került azonosításra az NBSZ, amely mind nemzetibiztonsági érdekkörben, mind bűnüldözési érdekkörben eljárva végrehajtja az LI-t az arra jogosult hazai megrendelő szervek megkeresése esetén, mind a magyar joghatóság alá tartozó eljárások, mind felkérés esetén a közösségi jog hatálya alá tartozó nemzetközi bűnüldözési célú együttműködés **keretében a transzparens törvényi garanciák és eljárási, engedélyezési szabályok mellett.** [H1] A 2.1. és a 2.5. alfejezetek összevetésével feltárásra került a „nemzetbiztonsági célú" és „bűnüldözési célú" tevékenység értelmezési problémaköre az uniós jog aspektusából, például az NBSZ LI-vel kapcsolatos speciális hazai szolgáltatói szerepköre kapcsán, hiszen ha nemzetbiztonsági érdekkörben, az Nbtv. szerinti nemzetbiztonsági szolgálat megkeresése alapján jár el, akkor nemzetbiztonsági tevékenységet valósít meg, amely nem tartozik a közösségi jog hatálya alá. Azonban, ha az NBSZ bűnüldöző szerv megkeresésére, bűnüldözési érdekkörben jár el, akkor a szerződések alapján a tevékenység a közösségi jog hatálya alá tartozik, így például a nemzetközi együttműködésre megnyílna a lehetősége, azonban mint arra a 2.1. alfejezetben utaltam elkerülhetetlen a megjelenés, azaz a külvilág számára észlelhető alaki elem, miszerint akár hogyan is nézzük az Nbtv. szerinti polgári nemzetbiztonsági szolgálat jár el. Továbbá reflektálva a

[306] A Stratégia 126. pontja éppen 2030-ig írja elő az innovatív és a biztonsági kihívásokkal, fenyegetésekkel reziliens, technológia fókuszú hazai biztonsági ökoszisztéma kialakítására irányuló átfogó célkitűzést.

szakirodalomban[307] levont következtetésekre **megállapítható, hogy az NBSZ esetében az egy szervezetben koncentrált LI képesség kialakításra került, amely akár nemzetközi együttműködés keretében bűnüldözési célú LI során is igénybe vehető a jogosultak által.** [H1]

Mind normatív, mind szakirodalmi szempontból feldolgozásra kerültek az LI egyes résztevékenységei és azok összefüggése az alapvető jog korlátozás mértékével. A nemzetbiztonsági célú külső engedélyezési eljárása kapcsán kitekintés történt az EUB vonatkozó ítélete és a NAIH ezzel kapcsolatos észrevételei alapján azon dilemmára, miszerint a külső engedélyhez kötött titkos információgyűjtés, így az LI alkalmazásának, végrehajtásának miniszteri szintű engedélyezése kellő garanciális szabályokat nyújt-e? Azaz a külső engedélyezési eljárás megfele-e a hatalmi ágak szétválasztása elvének (alkotmányossági-kritérium), vagy más **módon biztosítja a külső kontroll érvényesülését (kompetencia-kritérium)**, mely álláspontom alapján a hazai gyakorlatot, és szakirodalmat vizsgálva nem kétséges.

Következtetés került levonásra az igazságügyi miniszteri és bíró engedélyhez kötött nemzetbiztonsági célú titkos információgyűjtésre, így az LI-re is vonatkozó közérdekű adatszolgáltatáson alapuló 2016.Q1. – 2023.Q1. közötti időszakot felölelő statisztikai adatok trend- és tendenciaelemzésével, amely szerint megállapítható, hogy azok átlagosan laposabb exponenciálisan növekvő tendenciát mutatnak. Megállapításra került, **hogy a külső engedélyhez kötött nemzetbiztonsági célú tevékenység vonatkozásában a nemzetbiztonsági ügyjelleg a domináns a bűnüldözési jelleggel szemben. Ez a feldogozott szakirodalom alapján összefüggésbe hozható akár az Európát 2015/16-tól érintő iszlám fundamentalista terrorizmussal és az illegális migráció fokozódó tendenciájával is.** A nemzetbiztonsági célú titkos információgyűjtéssel kapcsolatos igényeknél tapasztalható növekvő tendencia gyakorlati alátámasztásául is szolgál a Stratégia 165. pontjában „*a titkos információgyűjtés koncentrált eszközrendszerére"* irányuló nemzetbiztonsági ipari K+F+I-s célkitűzésnek, azaz a gyakorlat alátámasztja a stratégiai célkitűzést.

A hagyományos technikai LI módszerek és a szolgáltatói együttműködés bemutatásán túl **ismertetésre került az FBI által vezetett multilaterális nemzetközi bűnüldözési**

[307] KOVÁCS 2016: 92-93

együttműködésben végrehajtott „Trójai Pajzs" innovatív komplex akció keretében megvalósuló ún. „hamis zászlós" LI művelet. A bűnüldözési koalíciónak az ANOM szoftver, alkalmazásszolgáltatás (NI-ICS) kapcsán elért, a transznacionális szervezett bűnözésre mért csapása okán tudományos vizsgálata és új LI módszer-, rendszertani szintre emelése álláspontom alapján indokolt, így annak LI rendszertani elemként történő besorolása és bizonyítása is elvégzésre került. [H1]

2.6. alfejezet: Részeredményként megállapításra került, hogy **az uniós adatvédelmi jog- és szakpolitikai törekvések már 2017-től a titkosított online kommunikációt lehetővé tevő alkalmazásszolgáltatások és a hagyományos elektronikus személyközi hírközlési szolgáltatások adatvédelmi szabályozását a digitalizáció, az IKT környezet fejlődéséből adódó elvárások mentén integráltan kezelték volna. Ezen jogpolitikai szemlélet végül a DMA és a Hírközlési Kódex kapcsán 2023-ra lényegében a hatályos és alkalmazandó uniós jog tételévé vált, így EU-s és tagállami szintű jogalkotói, jogalkalmazói kötelezettségeket testesítve meg. Aktuális példa, hogy a Bizottság a DMA alkalmazása során az alkalmazásszolgáltatások/NI-ICS körében először a WhatsApp-ot és a Messenger-t alapvető platformszolgáltatássá minősítette. Azonban az információs társadalommal összefüggő infokommunikációs és az elektronikus hírközlési szolgáltatások integrált szabályozásának mind uniós, mind tagállami szinten további teendői vannak.** Hiszen például az értekezés tárgyával kapcsolatos hazai jogforrások – az LI tekintetében is – szekularizáltan szabályozzák a tevékenységeket, annak ellenére, hogy a 2020. december 21-től hatályos Eht. módosítás már implementálta az NI-ICS-re vonatkozó különös szabályokat. Továbbá a titkosított kommunikációt biztosító alkalmazásszolgáltatás Ekertv. szerinti fogalma elhatárolásra került az információs társadalom által (AVMS, Mttv., Smtv.) életre hívott olyan szolgáltatásoktól, mint a videómegosztóplatform-szolgáltatás (például YouTube, Facebook és Instagram hírfolyam), a lekérhető médiaszolgáltatás (például Netflix, HBO Max, Disney), illetve a DMA szerinti online közösségi hálózati szolgáltatás (Facebook, Instagram), melyek többsége applikáció formájában is elérhető mobil végponti IKT eszközön például mobiltelefonon, így tág értelemben kvázi alkalmazásszolgáltatásként is értelmezhetők.

Megállapításra került, hogy az EU digitalizációs törekvései mentén – az információs társadalommal összefüggő szolgáltatások uniós szabályozásának talaján – a DMA és a DSA bázisán kialakult a digitális ágazat, amellyel párhuzamosan a közösségi jog szintjén létrejött egy új jogterület a platformszabályozás, a platformjog. A digitális ágazat beékelődött és jelentős

hatást gyakorol mind az elektronikus hírközlési, mind az elektronikus információ-, kiberbiztonsági ágazatra és szabályozásra, mely jogterületek éles elhatárolása még az Unió szintjén is egy alakulóban lévő folyamat nem, hogy a tagállami jog szintjén, mely például az Eht. és az Ekertv. NI-ICS-sel/alkalmazásszolgáltatással kapcsolatos tárgyi hatálya kapcsán, így az LI szabályozása szempontjából is kardinális kérdés. Hiszen például a DMA – és már a Hírközlési Kódex is – a digitális (információs társadalommal összefüggő szolgáltatások) ágazati szabályozásból az NI-ICS tekintetében átnyúl az elektronikus hírközlési ágazati szabályozásba, amely hazai jogforrási szinten az Eht.-ben került adaptálásra, átültetésre, úgyhogy egyébként az Ekertv. hatálya pedig továbbra is kiterjed az alkalmazásszolgáltatóra. Az Eht. és az Ekertv. hatálya ilyen jellegű összeütközésének azonosítása álláspontom alapján új tudományos eredmény is egyben. **Tehát kutatási eredményként feltárásra és bizonyításra került az Ekertv. szerinti alkalmazásszolgáltatásnak az Eht. szerinti számfüggetlen hírközlési szolgáltatással (NI-ICS-sel) való összefüggése, illetve azok funkcionális azonossága okán előállva az Ekertv. és az Eht. tárgyi hatályának konfliktusa.**

2.7. alfejezet: Áttekintésre kerültek a kvantumszámítás elterjedésének ambivalens veszélyei, továbbá előkérdésként tisztázásra került a rejtjelezett információhoz hozzáférők osztályozása, rendszertani besorolása „jogosultság" szerint, így megállapításra került, hogy a kvázi jogosult felek halmazába sorolható be az LI végzésére jogosult szervezet. **Mind a hazai tagállami jog (Ibtv.), mind az uniós jog (GDPR, e-hírközlési adatvédelmi irányelv és rendelet javaslat, Hírközlési Kódex) fogalomhasználata alapján megállapításra került, hogy a kriptográfia elméleti, szakirodalmi ismeretei beépültek a jogpolitikai törekvésekbe az IKT környezet változásaira reflektáló módon.**

Megállapításra és levezetésre került, hogy adat- és információvédelmi szempontból az alkalmazásszolgáltatások tekintetében indokolt a mobiltelefon és -internet hálózat (elektronikus hírközlési szolgáltatás) védelme érdekében használt C2SE és az alkalmazásszolgáltatások által biztosított szoftver alapú E2EE koncepció együttes alkalmazása, hiszen így a hálózati oldalon kicsatolható forgalom például MiTM támadás során az E2EE-nek köszönhetően nem fejthető vissza jogosulatlan fél által, a megfelelő titkos kulcs jogszerűtlen ismerete nélkül. A C2SE koncepció alkalmazása a mobilhálózatban pedig többletbiztonságot jelent, hiszen a szerveroldalon kívül a kommunikáció metaadatai nyíltan nem hozzáférhetőek. **A fentiek alapján kutatási részeredményként megállapításra, és kriptográfiai, technológiai adatvédelmi oldalról bizonyításra került, hogy a C2SE/E2EE kriptográfia integrált**

alkalmazása a nemzetbiztonsági és bűnüldözési célú LI során kihívást okozhat elsősorban az alkalmazásszolgáltatások tekintetében. [H3]

Továbbá megállapításra került, hogy az EU-s digitalizációra, az elektronikus hírközlési- és az információs társadalommal összefüggő szolgáltatásokkal, azon belül is az alkalmazásszolgáltatásokkal kapcsolatos fokozott normatív és technológiai adatvédelmi törekvésekkel összhangban, a feltárt kriptográfiai kihívások alapján szükségessé váló rejtjelező eljárások indokoltak és szükségesek, mind a GDPR, mind az e-hírközlési adatvédelmi rendelet szerinti adatbiztonság fokozása érdekében. A DMA valamennyi online kapuőr közvetítő szolgáltatóval, így a Metával szemben is, mint alapvető platformszolgáltatásokat nyújtó vállalkozás a WhatsApp és a Messenger tekintetében széles körű, új átláthatósági kötelezettséget támaszt, például az illegális tartalmak új jelölési mechanizmusának tekintetében, amely egyik kritériuma az üzleti felhasználók számára a végső fogyasztók felé vezető fontos átjárók, azaz az adatátviteli utak ellenőrzése, mely technológiai kivitelezhetősége az E2EE esetén megkérdőjelezhetővé válik. [H3]

3. AZ ELEKTRONIUS MOBIL HÍRKÖZLÉSI ELLENŐRZÉST ÉRINTŐ IKT TRENDEK, TENDENCIÁK

A 2. fejezet „általános”, felvezető jellegű részkövetkeztetései alapján megállapításra került, hogy az Európai Unió joghatósága területén egy gazdaság-, társadalompolitikai fejlődési törekvéstől áthatott erőteljes digitalizáció van folyamatban, amely egyik szegmense a polgárok közötti, személyközi infokommunikációs IKT termékek és szolgáltatások nagyarányú, általános elterjedése, mely egyik feltétele az ezekkel szembeni felhasználói bizalom erősítése. Ennek mind normatív (jogszabályok), mind technológiai (elektronikus információ-, kibervédelem) adatvédelmi környezete napról napra dinamikusan fejlődik a megfelelő színvonalú adatbiztonság, így a fogyasztók számára optimális biztonságú IKT termékek és szolgáltatások kereskedelmét és azon keresztül fogyasztását elősegítve. Az IKT piac tekintetében a központi szerep az elektronikus hírközlési szolgáltatások (infrastruktúra és integrált szolgáltatás), és az új innovatív internet-technológiára épülő, titkosított online kommunikációt biztosító alapvető platform-, alkalmazásszolgáltatásokra (szoftver) épül. Ezen szolgáltatásokat az információs társadalom[308] tagjai az okos, smart mobil végponti IKT eszközeiken vehetnek igénybe (mobiltelefon, okosóra, tablet, laptop), melyek biztonsági tulajdonságainak fokozása központi uniós jog- és szakpolitikai törekvés. Az adatbiztonság érdekében még kiemeltebb követelmények érvényesülnek a lakosság ellátása szempontjából kiemelten fontos kritikus infrastruktúra ágazatokban, így például az energetikai, egészségügyi, e-közigazgatási és az infokommunikációs ágazatban egyaránt, már ha csak a poszt-kvantumkriptográfia törvényi szintű előírására is gondolunk.

Tapasztalható a digitalizációban rejlő bűnelkövetési lehetőségeket kiaknázó, mikro szinten a határokon átívelő és egyre kifinomultabban szerveződő bűnözés, makro szinten a nemzetbiztonsági érdekeket is fenyegető, veszélyeztető transznacionalizálódó és hibrid jellegű cselekmények (terrorizmus, proliferáció, szervezett bűnözés, a nemzeti szuverenitás elleni szervezett tevékenység) jelenléte, fokozódása. Sabjanics István a terrorizmus egyes nemzetközi hatásai kapcsán kutatásában vizsgálta a félelem hatását a nemzetközi kapcsolatokra, amelyben egyes veszélyek harmadik államokba való transzplantálásáról van szó például az eltérő

[308] Lásd: NEMESLAKI András (2018): *Információs társadalom*. Budapest: Dialóg Campus Kiadó. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12655/web_PDF_ATMA_Informacios_tarsadalom.pdf;jsessionid=33682253A09701DAF4AF3EDB5EC40EE4?sequence=1 (Letöltés ideje: 2024. február 21.)

kulturális alapok, az empátia, a politikai és katonai szövetségek aspektusából, mely alapján megjelenik a veszélyérzet exportálása/importálása különféle érdekek mentén.[309] A fentiek elleni fellépésen alapuló nemzetbiztonsági, bűnüldözési érdek egyfelől hatékony és innovatív információgyűjtő szervezeteket, így a titkos információgyűjtés komplex eszközrendszerének dinamikus és nagy volumenű K+F+I tevékenységét indukálta hazai biztonsági stratégia szintjen, mely az innovatív fogalomértelmezés szerint egyben nemzetbiztonsági érdek is. Ezen nemzetbiztonsági ipar kialakítására irányuló törekvés leképeződése az állami szervezetek szintjén, az egyes nemzetbiztonsági szolgálatok és kutatóhelyek együttműködésében megtörtént. Tekintettel az infokommunikáció fejlődésére az egyik kiemelt ilyen fejlesztési iránynak álláspontom alapján a nemzetbiztonsági célú LI fókuszában kell összpontosulnia, nyilvános kutatási eredmények tekintetében is.

A fentiek alapján jelen fejezet a 2. fejezet részkutatási eredményeire építve célirányosan az elektronikus hírközlés trendjeit, tendenciáit és jellemzőit kívánja vizsgálni a nemzetbiztonsági célú LI aspektusából, azon belül is elsősorban a számfüggő mobil hírközlési szolgáltatások (mobiltelefon – hang, SMS), valamint a mobilinternet hozzáférési szolgáltatások (mobilinternet) tekintetében. A vizsgálat a szükséges mértékig érinteni fogja az elektronikus hírközlő hálózati oldalról, az intelligens- és okos városok („smart city") koncepció[310] keretében, az EU-s törekvésekkel összhangban kialakuló komplex digitális ökoszisztémával, az IKT fejlődés lehetőségiből adódó új szoftveralapú szolgáltatásokkal megjelenő „lehallgatás" jellegű biztonsági kihívásokat, egyben LI lehetőségeket.[311] A vizsgálat fókusza a személyközi kommunikáció során az 5G, 6G hálózatok, a VR/AR prognosztizálható információgyűjtő, speciális hírközlési LI lehetőségeit öleli fel, nem IoT jellegű aspektusokat.

---

[309] SABJANICS István (2021): *A terrorizmus hatásai és megjelenése a demokratikus jogrendben*. Budapest: Akadémiai Kiadó. 2.3 fejezet.

[310] Lásd: SALLAI Gyula (2018): *Az okos városok - (Smart City)*. Budapest: Dialóg Campus Kiadó. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12649/Web_PDF_Smart_City.pdf (Letöltés ideje: 2024. február 21.)

- *„digitális város a digitális (IKT, infokommunikációs) infrastruktúra kiépítését és az infokommunikációs szolgáltatások elérhetőségét foglalja magában, beleértve a telefonszolgáltatásoktól kezdve akár a szélessávú mobilinternet-szolgáltatást is;*
- *az intelligens város az IKT-háttérre alapozó intézményi (önkormányzati, vállalati, banki stb.) elektronikus szolgáltatások (e-szolgáltatások: e-kormányzat, e-business, e-tanulás, e-egészségügy stb.) széles körét is tartalmazza, amelyek nyújtása – amennyiben internetalapú – a hagyományos internet (IPv4) segítségével megoldható;*
- *az okos város (smart city) az élhetőbb várost célozza meg; adatok gyűjtésére, feldolgozására és hasznosítására is építő, internetalapú okos alkalmazások sokaságát jelenti, amelyek minél integráltabban, stratégiai szemléletben valósulnak meg.*" SALLAI 2018: 16

[311] Azonban e tárgykör elmélyült vizsgálata nem tárgya az értekezésnek, hiszen ez elsősorban IoT irányú kutatást igényel.

Jelen fejezet fő tárgyköre a mobil hírközlési ellenőrzést érintő IKT trendek, tendenciák komplex elemzése a meghatározott kutatási módszertan alapján, a hipotézisek alátámasztása és az új tudományos eredmények eléréséhez szükséges részkutatómunka elvégzése érdekében. A fejezeten belül vizsgálat tárgyát képezi az elektronikus digitális mobil hírközlőhálózatok (a továbbiakban: mobilhálózat) evolúciója, fejlődési trendjei, a mobilhálózatok felhasználói tendenciái, a mobilhálózatok kriptográfiai környezetének evolúciója, trendjei, kitekintve az LI szabványosításra, a hazai hírközlési kommunikációellenőrzés normatív, szervezeti, technológiai evolúciójára. Valamint elvégzésre kerül az egyes alfejezetek kutatási cselekményei alapján megállapítható részkövetkeztetések levonása.

3.1. Az elektronikus digitális mobil hírközlőhálózatok evolúciója, fejlődési trendjei

A mobiltelefonokra telepített alkalmazásszolgáltatás alapú kommunikáció elsődleges csatornája az Eht. 188. § 22. pont fogalomhasználata szerinti elektronikus hírközlő hálózat, azon belül is a vezeték nélküli, azaz a mobilinfrastruktúra, így indokolt megvizsgálni ezen hálózatok evolúcióját, és az értekezés szempontjából lényeges ismérveit, valamint következtetéseket levonni jövőbeli trendjeik, tendenciáik vonatkozásában[312] az LI elméleti aspektusából is. Ismertetésre kerül a mobilhálózatok kriptográfia evolúciója, és az LI szabványosításra is kitekintés történik. A vizsgálat az LI szempontjából lényeges, hiszen várhatóan prognosztikusan következtetések lesznek levonhatóak a hálózatokon megjelenő adatforgalom mennyiségéről és diverzifikáltságáról, a sávszélességről, a késleltetési időről a felhasználói trendek, tendenciák alapján.

3.1.1. A digitális mobil hírközlés és az IP technológia (2G, 3G, 4G)

Az 1990-es évektől az analóg 1G hálózatokban rejlő hiányosságok kiküszöbölésére a digitalizáció jelentette a megoldást, így létrehozva a digitális mobil hírközlő-, azaz 2G technológiát, melyek közül a GSM[313] vált a legelterjedtebbé. A 1,8 GHz frekvenciájú GSM hálózatok a hang alapú közlemények mellett már biztosították SMS-t, illetve később az

[312] Az altémakörökkel kapcsolatos korábbi kutatási eredményeimet lásd: TÓTH Tamás (2020): A mobilhálózatok technológiai fejlődéstörténete: Az analóg hangátviteltől az 5G-hálózatokig. *Nemzetbiztonsági Szemle*, 7(4), 51. Online: https://epa.oszk.hu/02500/02538/00031/pdf/EPA02538_nemzetbiztonsagi_szemle_2019_04_044-060.pdf (Letöltés ideje: 2023. december 19.)

[313] GSM: Global System for Mobile (Communications) – globális mobilkommunikációs rendszer

adatátviteli sebesség növelésével a képi multimédiás tartalmak (MMS[314]) megosztását, valamint lehetővé vált a nemzetköz barangolás (a továbbiakban: romaing[315]) mobilhálózatok között. A mobil bázisállomások általi hálózati lefedettséget biztosító cella[316] alapú 2G rendszer a TDMA[317] és az FDMA[318] technológia kombinációját használta, melynek köszönhető biztosított a dinamikus csatornakiosztás, továbbá egy frekvenciasávban adott egyszerre több felhasználó csatlakozása. Maghálózata a PSTN[319]. 2G-n a mobiltelefon a 3GPP TS 05.08. szabványban[320] leírtak szerinti rádióterjedési viszonyok folyamatos mérésével határozza meg és optimalizálja a cellaválasztását. Megjelent a WAP[321], azaz a mobilinternet szolgáltatás, így a weboldalak csökkentett változatai is elérhetővé váltak. A hálózat kezdetben 14,4 kbit/s sávszélességgel üzemelt, majd a GPRS[322] technológia lehetővé tette a 2,5G megjelenését, mely által már 115 kbit/s-ra nőtt a sávszélesség, míg a 2,75G, azaz az EDGE[323] szabvány megjelenését követően 384 kbit/s adatátviteli sebesség válhatott elérhetővé a hálózaton.[324] A GSM hálózat a 2000-es évekre a felhasználók folyamatosan bővülő sávszélességi, adatátviteli igényeket már csak korlátozottan tudta kiszolgálni.

Megoldást jelentett az Európában 2001-től bevezetett 3G technológia, ami a WCDMA[325] szélessávú kódelosztásos hozzáférési modellre épül, így rétegezett hálózat hozható létre, a mikro- és makrocellák kevert kialakításával a lefedettség és a sávszélesség a sűrűn lakott területeken növelhetővé vált.[326] A 3G hálózat biztosította az általános lakossági mobilinternetes adatforgalom lebonyolítására, a GSM-alapú hang és SMS kommunikáció mellett. A

[314] MMS: Multimedia Messaging Service – multimédiás üzenetküldési szolgáltatás
[315] Eht. 188. § 9. pont
[316] „*A cellás elv lényege, hogy a sík terepen elméletileg kör alakú cellák – amelyek a nyilvános célú hálózathoz csatlakoznak – saját adó-vevő állomással rendelkeznek, és egy olyan frekvenciakészletet használnak, amelynek egyik elemét sem alkalmazzák a szomszédos cellákban. A cellákon áthaladó mobiltelefon-használók automatikusan arra a frekvenciára váltanak, amelyiket az éppen látogatott cella használ*.” HAIG 2018: 38
[317] TDMA: Time Division Multiple Access - időosztásos többszörös hozzáférés
[318] FDMA: Frequency Division Multiple Access - frekvenciaosztásos többszörös hozzáférés
[319] PSTN: Public Switched Telephone Network - nyilvános célú telefonhálózat
[320] 3GPP TS 05.08. - Radio subsystem link control (Rádió alrendszer kapcsolat vezérlése)
[321] WAP: Wireless Application Protocol – a vezeték nélküli adatátviteli protokoll
[322] GPRS: General Packet Radio Service – általános csomagkapcsolt rádiószolgáltatás
[323] EDGE: Enhanced Data rates for GSM Evolution – GSM-rendszer csomagkapcsolt adatátviteli megoldásának továbbfejlesztése.
[324] SAGARKUMAR B. Patel (2018): Comparative Study of 2G, 3G and 4G. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 3(3), 1962-1963. Online: https://www.researchgate.net/publication/327763959_Comparative_Study_of_2G_3G_and_4G (Letöltés ideje: 2023. július 25.)
[325] WCDM: Wideband Code Division Multiple Access – szélessávú, kódosztásos, több hozzáféréses kapcsolat
[326] DWIVEDI, Vidya Kant – SHUKLA, Manoj (2007): *Code Division Multiple Access (CDMA) System in Multipath Environment.* National Conference on Communication Technology. 1-3. Online: www.researchgate.net/publication/200783159_Code_Division_Multiple_Access_CDMA_System_in_Multipath_Environment/link/09984da86bc439f832012f0a/downloadL (Letöltés ideje: 2023. december 19.)

3G/UMTS[327] technológia kezdeti 384–2000 kbit/s (kb. 2–10 Mbit/s) sávszélességről, a 3,5 G, azaz a HDSPA[328] szolgáltatás 14,4 Mbit/s sávszélességre növelte az adatátviteli kapacitást.[329] A technológia hírközlést forradalmasító hatásait a hazai statisztikai adatok is jelzik, „*A mobiltelefonozás 1993-ban indult Magyarországon, először vállalkozók, üzletemberek, és azok használták, akiknek munkájához szükséges volt a gyors híráramlás. A mobil-előfizetések száma igazán 2000 körül ugrott meg, s 2006-ban már 10 millió előfizetés volt az országban.”*[330] A 3G forradalmasította a hírközlés globalizációját a szélessávú mobilinternet elérés bevezetésével, mivel a megjelenő okostelefonokon, fejlett IKT eszközökön elérhetővé váltak a minőségi online tartalmak, az üzleti alkalmazások, valamint a 2.6.1. – 2.6.3. részfejezetekben ismertetett digitális IKT, OTT, alapvető platformszolgáltatások. A szakirodalom alapján „*A videómegosztó platformok használata a gyermekek körében szinte egyetemes (95%), és a legtöbben azt nyilatkozták, hogy a koronavírus-világjárvány idején többet használtak videómegosztó platformokat, mint korábban.*”[331] A fenti internet-technológiára épülő szolgáltatások hozzáférhetőek és akár csekély informatikai tudással is használhatók bárki által a meglévő IKT eszközökön,[332] az újgenerációs lekérhető médiaszolgáltatások kivételével legtöbbször ingyenesen igénybe vehetők. Abban az esetben, ha ezen chat alkalmazásszolgáltatások titkosított online kommunikációt tesznek lehetővé az Ekertv. 2. § m) pont szerinti, a 3/B. § és 13/B. § alapján értelmezhető alkalmazásszolgáltatásoknak minősülnek, tehát a kutatás tárgyát képezik. Korábbi kutatási eredményeim alapján megállapítható, hogy „*A társadalom infokommunikációs szokásai, igényei alapján látható, hogy az adatátviteli sebesség és a sávszélesség folyamatos növelése továbbra is indokolt volt, annak érdekében, hogy minél nagyobb mennyiségű adat legyen továbbítható, minél rövidebb időn belül. Az interneten elérhető, nagy felbontású videókhoz és más, magas sávszélességet igénylő szolgáltatásokhoz (például élő, nagyfelbontású, HD-minőségű videókonferenciák) való hozzáférés igénye alapvetővé vált*.”[333]

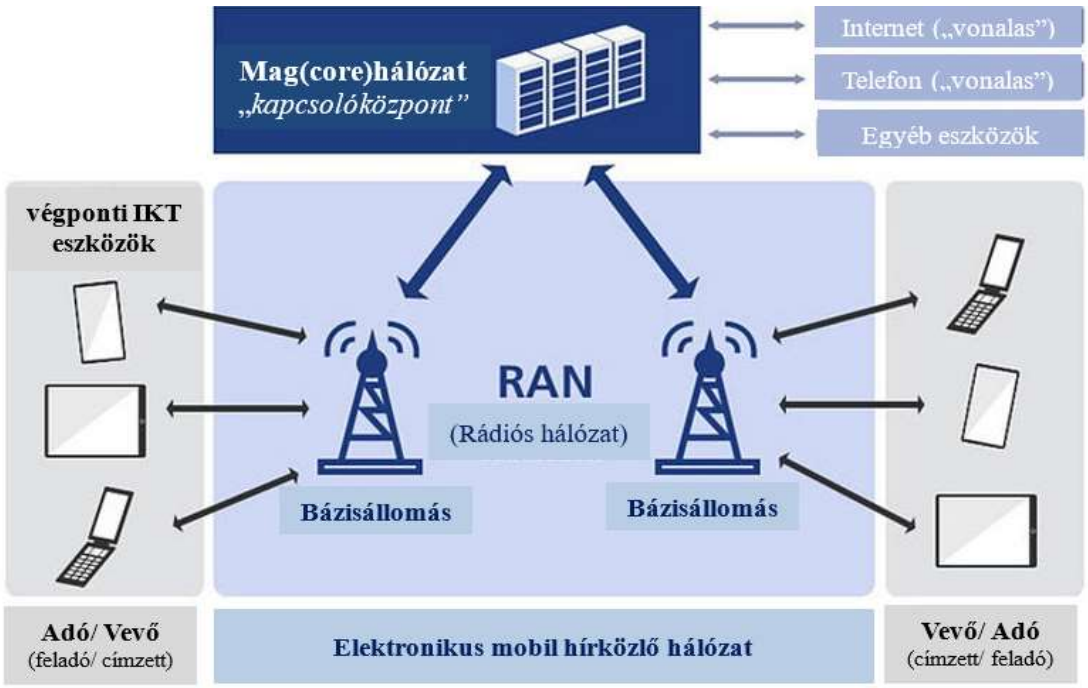
[327] UMTS: Universal Mobile Telecommunications System – univerzális mobil távközlési rendszer
[328] HSDPA: High Speed Downlink Packet Access – nagysebességű csomagletöltési hozzáférés
[329] ANWAR, Toni (2008): Performance Analysis of 3G Communication Network. *ITB Journal of Information and Communication Technology,* 2(2), 154–155. Online: https://doi.org/10.5614/itbj.ict.2008.2.2.4 (Letöltés ideje: 2023. december 19.)
[330] *Gazdasági és társadalmi változások az 1990-es években és a 2000-es évek első felében*. NKP. Online: https://okostankonyv.nkp.uni-eszterhazy.hu/tankonyv/tortenelem_12/lecke_05_035 (Letöltés ideje: 2023. július 27.)
[331] KIRÁLY 2021: 312
[332] KOVÁCS 2015: 136
[333] TÓTH 2020: 51.

Megoldást az internet-technológiára épülő központi(core)rendszerrel rendelkező 4G LTE[334] hálózat biztosítja. A 4G 2005-ben először Dél-Koreában volt elérhető WiMAX néven, Magyarországon 2012. január 1-től üzemel. A 4G VoLTE[335], azaz a hangszolgáltatás 2017. április 27-től érhető el, mely által a hanghívások is a 4G hálózaton bonyolíthatók le, ami gyorsabb hívásfelépülést, HD hangminőséget és folyamatos 4G sebességű mobilinternet-kapcsolatot biztosít. Az első VoLTE szolgáltatás 2012-ben szintén Dél-Koreában indult el.[336] A 4G technológia célja a számítási felhő fejlesztési lehetőségek kiszélesítése is volt a nagyfelbontású multimédiás, illetve 3D-s tartalmak mobilinternet alapú eléréséhez. Az LTE egy szélessávú, IP-alapú (internet protokoll) csomagkapcsolt, nagy sebességű mobiltávközlési technológia,[337] adatátviteli sebessége kezdeti 10 Mbit/s-ról mára már meghaladja a 326 Mbit/s-ot. [338] (A 3G kezdetben 2 Mbit/s sebességet biztosított) A 4G internetkapcsolata a vezeték nélküli helyi hálózati (WLAN[339], WiFi), vagy akár az egyéb VoIP alapú hangátvitel, például az egyes alkalmazásszolgáltatásokon.[340] A 4G kompetenciáiban képes kiváltani a jóval alacsonyabb adatátviteli sebességű 3G szolgáltatásokat, így azok globális kivezetése folyamatban van, Magyarországon ez 2022-ben megtörtént.[341]

A 2G, 3G és még az IP alapú 4G mobilszolgáltatások is hagyományos földi, földfelszíni, cellurális hírközlési infrastruktúrát alkalmazzák, szolgáltatás oldaláról pedig általánosságba, hazai viszonylatban legalább is a mobiltelefon, -internet szolgáltatója azonos az infrastruktúra tulajdonosával/üzemeltetőjével.[342] Gondoljunk csak a globális jelenlétű hírközlési szolgáltatók magyarországi disztribútoraira, tagvállalataira, mint például az országos lefedettséget biztosító Magyar Telekom Nyrt., a Vodafone Magyarország Zrt, vagy a Yettel Magyarország Zrt. publikus hírközlési szolgáltatókra. A hagyományos publikus, lakossági célú mobil

[334] LTE: Long Term Evolution – hosszú távú fejlődés
[335] VoLTE: Voice over LTE – LTE feletti hangátvitel
[336] *A 4G hálózat adat mellett már a hangunkat is viszi – Elindítja a 4G Hangot a Magyar Telekom.* Magyar Telekom. 2017. Online: www.telekom.hu/rolunk/sajtoszoba/sajtokozlemenyek/2017/aprilis_27 (Letöltés ideje: 2023. december 19.)
[337] ARORA, Mohit (2012): Long Term Evolution (LTE) Technology. *International Journal of Latest Technology in Engineering Management & Applied Science*, 1(3), 69. Online: www.researchgate.net/publication/319465003_LONG_TERM_EVOLUTION_LTE_TECHNOLOGY (Letöltés ideje: 2023. december 19.)
[338] ALMAZROI, Abdulaleem Ali (2018): Performance analysis of 4G broadband cellular networks. *International Journal of Advanced and Applied Sciences,* 5(9), 13. Online: http://science-gate.com/IJAAS/Articles/2018/2018-5-9/03%202018-5-9-pp.12-17.pdf (Letöltés ideje: 2023. december 19.)
[339] WLAN: Wireles Local Area Network – rádióhullámot használó vezeték nélküli helyi hálózat
[340] TÓTH 2020: 52
[341] DÖMÖS Zsuzsanna (2022): *Megvan, mikor végez a Telekom a 3G kivezetésével*. HWSW. Online: https://www.hwsw.hu/hirek/64508/magyartelekom-3g-halozat-lekapcsolas-datum.html (Letöltés ideje: 2024. február 21.)
[342] Egyes piaci és szolgáltatói belső polgári jogi, egyéb éppen is aktuális akvizíciós jogviszonyokat nem vizsgálva

infrastruktúra nagyvonalúan 3 fő részegységre tagolódik, mégpedig a központi rendszerre, azaz a mag(core)hálózatra, a „kapcsolóközpontra”, mely többek között felel az adatforgalom irányításáért, így a teljes hálózati forgalom keresztül megy rajta. A második elem a celluláris hálózat, a rádiós hozzáférési hálózat (a továbbiakban: RAN[343]) központi eleme a bázisállomás, amely a hálózati lefedettségért felel. A harmadik komponens a felhasználók végponti IKT eszközei, melyek kommunikációjuk során a RAN-on keresztül, a központi(core)rendszer át juttatják el adataikat a vevőhöz, a címzetthez.[344] Ezt a kommunikációs folyamatot, infrastruktúrát biztosítja a végponti eszközig például a 2.7.3. fejezetben ismertetett C2SE koncepció, az azt alkotó különböző protokollok, algoritmusok és eljárások segítségével, melyben a kiszolgálószerver (akár fizikai, akár felhőalapú) lényegében a központi(core)rendszer eleme, így ebből az architektúraelemből valósulhat meg az LI-vel érintett kommunikációs forgalom és kísérőadatainak jogszerű, törvényes ellenőrzése.[345] A mobilhálózat általános infrastruktúrájának szemléltetésére az alábbi 10. ábra hivatott.



10. ábra: Az elektronikus mobil hírközlő hálózat általános infrastruktúrája (Szerk.: A szerző[346])

[343] RAN: Radio Access Network – rádió hozzáférési hálózat

[344] ÇEKINMEZ, Fethi (2023): *Radio Access Network (RAN)*. Medium. Online: https://medium.com/@fthcknmz/radio-access-network-ran-1fb033b708f1 (Letöltés ideje: 2024. február 23.)

[345] *What are the challenges of 5G for Lawful Interception?*. Utimaco. Online: https://utimaco.com/service/knowledge-base/lawful-interception/what-are-challenges-5g-lawful-interception (Letöltés ideje: 2024. február 23.); *Solutons for Next Generation Networks.* SafeSoft. Online: http://www.safesoft.eu/safelims_ngn.htm (Letöltés ideje: 2024. február 23.)

[346] ÇEKINMEZ 2023

Az ipar innovációja, digitalizációja során láthatóvá vált, hogy az alapvetően lakossági célú internet felhasználásra optimalizált mobilhálózatok nem biztosítanak elegendő adatátviteli kapacitást a jóval nagyobb adatátviteli- és lefedettségi-, valamint jóval alacsonyabb késleltetési időigény számára Az okos városok komponenseiben, a high-tech gyártási, közlekedési, e-mobilitási technológiákban kulcsszerepet játszó IoT ökoszisztéma biztonságos vezérlését lehetővé tevő M2M adatkommunikáció az eddigi hálózatokon csak korlátozottan biztosítható paramétereket követel meg. A polgárok életminőségének és a nemzetgazdaság versenyképességének javítása céljából elengedhetetlen a digitális szolgáltatások széles körű elterjedése.[347] Ehhez a hírközlési infrastruktúra további fejlesztése szükséges, amely 2017-től a 4G, 2020-as kereskedelmi forgalomba kerülésével pedig az 5G technológiában ölt testet.

3.1.2. Az újgenerációs mobil hírközlőhálózatok (5G, 6G)

A 4G LTE hálózatokhoz képest az 5G-t jellemzi a jóval nagyobb adatátviteli sebesség, a rendkívül alacsony késleltetési idő, a bázisállomások kapacitásának jelentős növekedése, és a szolgáltatási minőség további javulása.[348] A 3GPP már a szabványosítását megelőzően 2016-ban három fő alkalmazásterületet fektet le az 5G számára, mégpedig:

- a továbbfejlesztett mobil szélessáv, azaz az eMBB (Enhanced Mobile Broadband);
- a kiterjedt gépi kommunikáció, azaz mMTC (Massive Machine-Type Communication);
- a megbízható, alacsony késleltetési idejű kommunikáció, azaz az URLLC (Ultra Reliable Low Latency Communication).[349]

Az 5G szabványosítása a 3GPP és ETSI által 2017 óta zajlik. Ennek keretében kiadásra kerültek a Release 15/16/17 szabványcsomagok, amelyek a kezdeti 4G/5G integrált Non-Standalone (NSA) hálózatoktól ajánlási szinten szabályozzák egészen a saját 5G rádiós és központi(core)rendszerrel rendelkező Standalone (SA) hálózatokat. A 3GPP 2021 decemberében jóváhagyta a Release 18 szabványcsomag összeállítását, amely jelentős fejlődést jelent az 5G Advanced (fejlett 5G) szabványosítása terén.[350] A szabványcsomag elsősorban az

[347] *A jövő lehetősége az 5G*. DJP. 2019. Online: https://digitalisjoletprogram.hu/hu/hirek/a-jovo-lehetosege-az-5g (Letöltés ideje: 2024. február 21.)
[348] ZHANG, XING (2020): *New Retail Marketing Strategy Combining Virtual Reality and 5G Mobile Communication.* Mathematical Problems in Engineering. Online: https://www.hindawi.com/journals/mpe/2021/6632701/ (Letöltés ideje: 2024. február 21.)
[349] MALLINSON, Keith (2016): *The path to 5G: as much evolution as revolution*. 3GPP News. Online: https://www.3gpp.org/news-events/3gpp-news/5g-wiseharbour (Letöltés ideje: 2024. február 21.)
[350] 3GPP RAN RP-213468 2021

MI és gépi tanulás támogatására fókuszál az 5G nyújtotta lehetőség maximális kiaknázása által az adatvezérelt, intelligens hálózati megoldások biztosításával, elsősorban az ipari felhasználás számára. A technológia számos ágazatban, például a közlekedésben, az autóiparban, az egészségügyben, a szórakoztatóiparban fogja elősegíteni az innovatív, diszruptív szolgáltatások, üzleti modellek megjelenését. Az 5G 1-10 Gbit/s sebességet eredményez, a kommunikáció 1-4 milliszekundumos válaszideje, a nagyon magas rendelkezésre állás, a megbízhatóság és a fokozott biztonság mellett. Az 5G képes okostelefonok széles körű elterjedése még várat magára, akárcsak az 5G SA hálózatoké. Jelenleg a lakossági 5G szolgáltatás 4G hálózati infrastruktúrával integrált módon üzemel. A Rel-18 fejlett 5G szabvány várhatóan 2024. júniusára válik implementálhatóvá, míg 2023 decemberében Taipeiben megtartott 5G SA workshopot követően megkezdődött Rel-19 szabványosítási folyamat, mely várhatóan 2025.Q4. – 2026.Q1-re ér véget.[351]

A fentiek alapján az 5G SA jelentősen növeli a mobilhálózatok kapacitását, amely függ a rendelkezésre álló spektrumtól, a cellák sűrűségétől, valamint a spektrális hatékonyságon. Az alaptézésiként megállapítható, hogy a rendelkezésre álló frekvenciák végesek, a cellák – azaz a mobil bázisállomások – földrajzi sűrítése költséges, időigényes és szigorú szabályozási követelményei vannak, így célszerűnek tűnt/ tűnik a spektrális hatékonyság növelése. Erre a publikus, lakossági célú 5G szolgáltatás esetén a Massive MiMo[352] technológia bizonyul megoldásnak, mely az 5G NR[353] hálózatok eleme. A több antennás technológiából álló Massive MiMo felszabadítja az új spektrumban rejlő teljes potenciált, jelentős növekedést biztosítva a hálózati lefedettségben, a kapacitásban és a sávszélességben anélkül, hogy a lefedettségi cellák helyszíni sűrűbbé tétele szükséges lenne.[354] A MiMo a cella szerű lefedettség helyett nyalábtechnológiát alkalmaz, így kihasználva a maximális kapacitást, a cellaspecifikus nyalábformálástól (nagyobb, általánosabb lefedettség), a végponti eszköz optimális fix nyalábválasztától egészen az egyéni nyalábválasztásig, mely lehetőségek a hálózati infrastruktúra komplexitásától függenek. A nyalábtechnológia további pozitív hozadéka, hogy jóval magasabb pontossággal lesz képes a helymeghatározásra a jelenlegi cellás elvhez és egyéb

[351] JAIN, Puneet (2023): Rel-18 Status and Rel-19 Progress in TSG SA. *Highlights*, 3(7), 4-5. Online: https://www.3gpp.org/newsletter-issue-07-nov-2023 (Letöltés ideje: 2024. február 21.)
[352] MiMo: Multiple-input, Multiple-output
[353] NR: New Radio
[354] ASTELY, David - VON BUTOVITSCH, Peter – FAXÉR, Sebastian – LARSSON, Erik (2022): Meeting 5G network requirements with Massive MIMO. *Ericsson Technology Review*, 7(1), 9. Online: https://www.ericsson.com/4917a1/assets/local/reports-papers/ericsson-technology-review/docs/2022/the-role-of-massive-mimo-in-5g-networks.pdf (Letöltés ideje: 2024. február 22.)

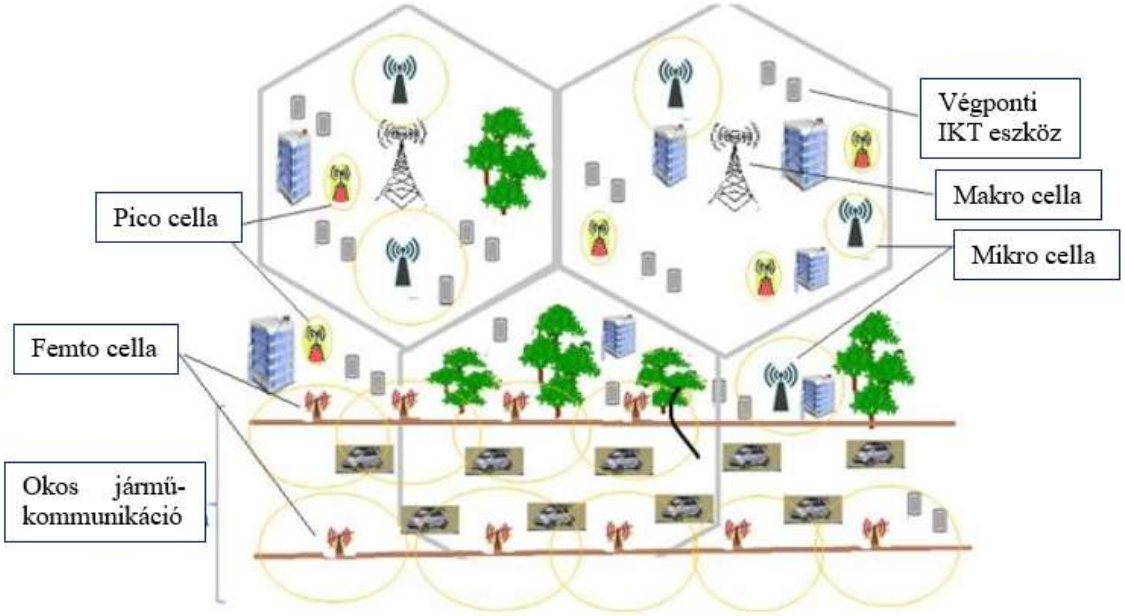
technológiákhoz képest, így elősegítve az e-mobilitás, az okos közlekedés dinamikus fejlődését, összhangban az EU digitalizációs célkitűzéseivel. A MiMo hatékonysága függ az adott terület beépítettségtől, az 5G bázisállomások konfigurációjától és a végponti IKT eszközök eloszlásától, továbbá az antenna és az épületek magasságától, valamint a bázisállomások és az végponti eszközök közötti távolságtól. Az 5G infrastruktúra további lényeges különbsége a 4G-hez képest, hogy a 4G bázisállomások fizikai száloptikai összeköttetést igényelnek, az 5G bázisállomások viszont nem, rádiós úton kommunikálnak egymással.[355] Tehát földfelszíni hírközlési infrastruktúra esetén annak komplexitásától igencsak függ a spektrális hatékonyság növelése, így az 5G SA-ban rejlő lehetőségek kiaknázása a heterogén hálózatokban, továbbá nem mindegy, hogy városi, vagy kevésbé urbanizált környezetben üzemel a hálózat az optimális antennaszám szempontjából sem. Az 5G igen magas frekvencián működik,[356] ami azt jelenti, hogy egymáshoz kifejezetten közel kell elhelyezni a bázisállomásokat vagy mobilhálózati antennákat, hiszen a magasabb frekvenciájú jelek nem jutnak el olyan messzire, mint az alacsonyabb frekvenciájúak. A vizsgált szakirodalom alapján tekintettel arra, hogy az 5G fentiekben meghatározott céljai jellemzően nem teljesíthetők a hagyományos homogén hírközlési hálózati architketúrák segítségével, az elmúlt években egyre inkább a figyelem középpontjába kerültek az ún. heterogén hálózatok (a továbbiakban: HetNets[357]), hiszen maga a hálózati forgalom is egyre heterogénebb, gondoljunk csak a számos digitális platformszolgáltatásra és az okos város komponensekre. A HetNetsek a felhasználói igényekhez és/vagy területi sajátosságokhoz igazodva számos különböző cellaméretű (makro, mikro, nano, piko, femto) szegmensből állhatnak össze.[358] Az 5G HetNets ökoszisztéma modelljét az alábbi 11. ábra hivatott szemléltetni.

[355] KISS Tamás (2018): *Massive MiMo megvalósitása az 5G-ben*. Budapest: HTE Rádiószakosztály Rendezvény. 9-22. Online: https://www.hte.hu/documents/10180/4582184/HTE+MiMo.pdf/b96bc127-afbc-8a1c-001f-a20a907c731b (Letöltés ideje: 2024. február 22.)

[356] Au EU-ban a 24,25-27,5 GHz-es sávtartomány a jóváhagyott, főleg az 5G bázisállomások főleg a 3000–5000 MHz-es frekvenciasávban működnek.

[357] HetNets: Heterogeneous network – heterogén hálózatok: A heterogén/ vegyes hálózat különböző tulajdonságokkal rendelkező cellák sokaságát, gyakorlatilag kisteljesítményű bázisállomások alkalmazását jelenti egy nagycellás hálózatban, összetettebbé téve az architektúra tervezést, mivel szignifikánsan különböző interferencia körülményeket hoz létre, szemben az homogén/ egynemű hálózatokkal.

[358] PRIYANKA, A. – GAUTHAMARAYATHIRUMAL, P. – CHANDRASEKAR, C. (2023): Machine learning algorithms in proactive decision making for handover management from 5G & beyond 5G. *Egyptian Informatics Journal*, 24(3), 1-2. Online: https://www.sciencedirect.com/science/article/pii/S1110866523000452 (Letöltés ideje: 2024. február 22.)



11. ábra: 5G HetNets ökoszisztéma modellje (Szerk.: A szerző[359])

A HetNets kifinomult, innovatív mobilitásmenedzsment megoldásokat követel meg, annak érdekében, hogy a komplex kommunikációs ökoszisztémát képes legyen hatékonyan kezelni, például 5G hálózat esetén. Ezen problémákra a kutatók egy gépi tanulási algoritmus alapú proaktív döntéstámogatással megvalósuló cellakiválasztást célzó MI megoldást vázolnak fel, összhangban az EU digitalizációs törekvéseivel, így az IKT termékek és szolgáltatások általános elterjedésének előmozdításával is.[360] Az 5G hálózatok elsősorban már a smart IoT eszközök M2M kommunikációs igényeinek kielégítésére szolgálnak, azonban a publikus személyközi hírközlési szolgáltatások számára is hozzáadott értéket fognak képezni. Az 5G infrastruktúra lehetővé teszi a hálózat „szeletelését", így a központi hírközlési hálózattól független, decentralizált hálózatok létrejöttét, melynek köszönhetően elsősorban az ipari felhasználás, az üzemek, gyárak képesek a nyilvános hálózattól és annak forgalmától teljesen független 5G hálózatot kialakítani saját működési területükön. A Budapesti Műszaki Egyetem erre irányuló kutatási témájának kiírása szerint „*Az 5G hálózati szeletelés lehetővé teszi ugyanazon fizikai hálózat különböző szolgáltatási rétegei közötti nagy fokú elkülönítést, ami növeli a differenciált szolgáltatások nyújtásának lehetőségeit a hálózat egészében*."[361]

[359] PRIYANKA at al. 2023: 2
[360] PRIYANKA at al. 2023: 9
[361] *5G hálózati szeletelés optimalizációja megerősítéses tanulás segítségével*. BME VIK. Online: https://www.hit.bme.hu/edu/project/data?id=20448 (Letöltés ideje: 2024. február 22.)

Érdemes kitekinteni az 5G által támogatott VR/AR eszközök például helymeghatározást segítő lehetőségeire is. A XR technológia, szemben a VR technológiával, igen hatékony támogatást nyújthat mind a publikus (lakossági), ipari és kormányzati (honvédelmi, nemzetbiztonsági, rendvédelmi, egyéb készenléti) felhasználók számára. A valóságos világon túlmenően az AR számtalan, az egyes alkalmazások használata során keletkező extra információt, például térképet, útvonal javaslatokat és irányítást, metaadatokat a környezetről (például forgalom, hőmérséklet, ember-/jármű-/objektum-azonosítási információk) képesek megjeleníteni a felhasználók számára. A Tampere Egyetem kutatása az 5G-támogatású XR-eszközök hat szabadsági fokú (a továbbiakban: 6DoF[362]) követéssel kapcsolatos kihívását elemzi, javaslatot téve egy új feltöltési vivőfázismréréseken alapuló becslési megközelítésre, amely a következtetések szerint lehetővé teszi az alacsony késleltetési idejű 3 dimenziós (a továbbiakban: 3D) holografikus orientációt, és 3D helymeghatározást/ nyomon követést közvetlenül az 5G bázisállomások segítségével. A javasolt megoldás bemutatásra került egy decentralizált ipari, gyárszerű beltéri környezetben 3.5 GHz-es és 28 GHz-es 5G hálózaton, mely eredményei alapján a 3D-s tájolás esetében egy fok alatti, a 3D-s helymeghatározás esetében pedig egy centiméter alatti pontosság érhető el.[363]

Hazai 5G viszonylatban az Óbudai Egyetem és a Yettel Magyarország Zrt. (a továbbiakban: Yettel) K+F+I együttműködésében Magyarországon elsőként, és világviszonylatban is az élmezőnyben nyilvános ajánlatban tette elérhetővé ügyfelei számára a publikus 5G SA szolgáltatást, összhangban az Unió digitalizációs stratégiai célkitűzéseivel.[364] A Yettel lakossági célú 5G SA szolgáltatásához a teljes hozzáférés biztosítása 2024 első negyedévének végére várható, aminek része a megfelelő ügyfélélmény érdekében a hálózati teljesítmény optimalizálása is.[365]

---

[362] 6DoF: Six Degrees-of-Freedom - hat szabadsági fokú

[363] TALVITIE, Jukka – SÄILY, Mikko – VALKAMA, Mikko (2023) Orientation and Location Tracking of XR Devices: 5G Carrier Phase-Based Methods. *IEEE Journal Of Selected Topics In Signal Processing*, 17(5), 919-934. Online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10232971 (Letöltés ideje: 2024. február 22.)

[364] *„Az önálló 5G-technológiával a mindennapokban egy még gördülékenyebb netezési élményt, szinte valósidejű online kommunikációt élvezhetnek ügyfeleink. Az új technológia jelenléte és lehetőségei pedig nagyban hozzájárulhatnak számos gazdasági ágazat további digitalizációjához Magyarországon, növelve az itt működő cégek és vállalatok hazai és nemzetközi versenyképességét. Hazánkban a Yettel rendelkezik a szupergyors 5G eléréshez szükséges frekvenciasávban a legnagyobb összefüggő tartománnyal, azaz legnagyobb kapacitással, és ezt a műszaki lehetőséget az önálló 5G-vel szeretnénk ügyfeleink, felhasználóink előnyére fordítani.” Az 5G-hálózat jelenleg legfejlettebb változatát indítja ügyfelei számára a Yettel.* IoT Magazin. Online: https://iotmagazin.hu/okoseszkozok/2023/11/22/yettel-mobil-halozat-modern-5g/ (Letöltés ideje: 2024. február 22.)

[365] Uo.

Egyes kutatások alapján az intelligens jelvisszaverő felületek (a továbbiakban: IRS[366]) alkalmazása elsődlegesen az 5G-t követő generációk terjedésével válhat kiemelt jelentőségűvé. Az IRS technológia célja, hogy a mobilkommunikációs jelek szinte mindenhová, az adott felhasználást támogató módon és minőségben eljuthassanak. A szerzők az IRS alkalmazhatóságát vizsgálták a NOMA[367] hozzáférési technológia tükrében. A NOMA támogatja a MiMo által biztosítható aktív kapcsolatok számának növelését azáltal, hogy egyazon erőforrásra utalt felhasználói eszközök jeleit aggregálja, így biztosítva minél több végponti IKT eszköz megfelelő minőségű kiszolgálását adott bázisállomás által, javítva a spektrális hatékonyságot. A kutatók megállapítása szerint, az IRS passzív visszaverődései NOMA technológia esetében lehetőséget kínálnak a forgalmazott adatok jogosulatlan ellenőrzésére is.[368] További kutatási eredmények szerint a Rel-18 és Rel-19 szabványcsomag kiadása tovább javítja az 5G teljesítményét, olyan funkciókat vezet be, amelyek rugalmasabb és hatékonyabb spektrumhasználatot tesznek lehetővé, előmozdítják a különféle IoT eszközök támogatását, fejlesztik a hálózati topológiát, és egyben már adatvezérelt, intelligens hálózati megoldásokat kínálnak. Prognosztizálható, hogy az 5G nem lesz képes a dinamikusan növekvő IKT eszköz és adatmennyiséget, lefedettségi igényt és még alacsonyabb késleltetési időt kezelni, gondoljunk csak az okos városok közösségimédia, szállítási, közlekedési, kommunikációs stb. komponenseinek igényeire – amelyek részletes elemzése nem képezi az értekezés tárgyát –, így elkerülhetetlen a mobilhálózati dimenzióváltás az újgenerációs mobilhálózat, azaz 6G várható megjelenésével. A 6G szabványosítása várhatóan 2025 körül kezdődik a 3GPP-ben. Várhatóan a fejlett 5G-vel végzett innovatív kutatások, mint például a MI és a gépi tanulási technológiák támogatása paradigmaváltást indítanak el, erős alapot teremtve a 6G tervezéséhez, mélyreható hatást gyakorolva a jövő vezeték nélküli hálózati technológiáira[369] A 2023-as Mobil Világkongresszuson elhangzottak alapján a 6G kb. 500-szorosára növelheti majd a hálózati kapacitást, óriási növekedést hozva a sávszélességben, és az adatátvitel sebességben.[370]

[366] IRS: Intelligent Reflecting Surface - intelligens tükröző/ jelvisszaverő felület
[367] NOMA: Non-Orthogonal Multiple Access - nem ortogonális többszörös hozzáférés
[368] WANG, Dawei – LI, Xuanrui - HE, Yixin – ZHOU, Fuhui – WU, Qihui (2023): Intelligent reflecting surface assisted untrusted NOMA transmissions: a secrecy perspective. *Science China Information Sciences Research Paper*, 66(192302). Online: https://doi.org/10.1007/s11432-022-3653-y (Letöltés ideje: 2024. február 22.)
[369] LIN 2021: 82.
[370] *Ready to talk 6G?* 2023

A 12. ábra Sallai Gyula nyomán az egyes okos város-alkalmazások, komponensek rendszertani besorolását hivatott szemléltetni, mindazért, hogy bizonyíthatóvá váljon azok rendkívül komplex, heterogén digitális ökoszisztémája. Ezen ökoszisztéma mind az 5G, mind a 6G technológiák tekintetében is kihívást jelent a végeláthatatlan számosságú hálózathoz csatlakozó IKT eszköz, azok konnektivitása, az abból adódó gigászi mennyiségű egyidejű adat, a maximális hálózati területi lefedettség, a rendkívül nagy adatátviteli sebesség, a minimális késleltetési idő okán, túl az IoT eszközök M2M kommunikációján, az ipari gépi kommunikáción, egészen a lakossági célú IKT szolgáltatások igénybevételéig, így a titkosított online kommunikációt biztosító alkalmazásszolgáltatásokig. A fenti szempontok természetesen az LI rendszerek oldalán is jelentkezni fognak, így azok fejlesztése elengedhetetlen.

12. ábra: Okos város-alkalmazások rendszertani besorolása (Szerk.: A forrás[371])

A fölfelszíni cellás mobilhálózatoktól eltérően a 6G esetében már nem terület, hanem légköbméter alapon (100 eszköz/ m3) határozzák meg az adott térben kiszolgálandó IKT eszközök számát. A nagytömegű eszközök jelenléte megalapozza az „ember-gép-IoT" ökoszisztéma teljes megvalósulását, összhangban az okos város koncepcióval, mely egyben a metaverzum[372] egyik lábát is képezi. Azonban, ezen komplex digitális ökoszisztéma képesség

[371] SALLAI 2018: 19

[372] A metaverzum az Internet egy lehetséges jövőbeli változata, ahol 3 dimenziós virtuális környezetben, a személyes találkozásokhoz hasonló módon lehetünk jelen, és tehetünk meg dolgokat, amiket jelenleg a monitor előtt ülve vagy a való világban csinálunk. A metaverzum kifejezést néha szélesebb értelemben véve használják, és a kiterjesztett valóságot is beleértik. A kifejezés a meta- (=mögött) előtag és az univerzum (=világmindenség)

az aktuális technológiákkal nem biztosítható. A Cornell Egyetemen kutatásában vizsgálni kezdte a tömeges hírközlési hozzáférés irányába tett legújabb fejlesztéseket az ipari szférában, az ún. tömörítéses érzékelésen[373] alapuló, engedélymentes[374] tömeges hozzáférés kérdéskörére összpontosítva. A kutatók azonosítják a véletlen hozzáférésű rendszerek korlátait és ismertetik a vizsgált technológiát a teljes (pilot)hálózati architektúrák és felhasználási lehetőségek széles skálájának figyelembevételével. A kutatás a nagy tömegű IKT eszközök jelenlétéből adódó 6G alapú „ember-gép-IoT" komplex digitális ökoszisztémára, mint a metaverzum egyik lábának megvalósulására irányuló további eredménye kellően rávilágít a 6G infrastruktúrán, még az 5G hálózatnál is nagyobb mennyiségű adatfolyam megkeletkezésének várhatóságára.[375] A 6G (sötétkék) és az 5G (világoskék) közötti vizsgált főbb szempontok szerinti különbségeit a Samsung kutatási eredményeiben publikált alábbi 13. ábra szemlélteti.[376] Ez alapján a 6G-vel cél, hogy el lehessen érni az 1 Tbit/s-os maximális adatátviteli sebességet, a késleltetés 100 mikroszekundum alá legyen csökkenthető, azaz a maximális átviteli sebesség az 5G-hez képest 100-szor nagyobb, a késleltetés pedig 10-szer kisebb legyen.

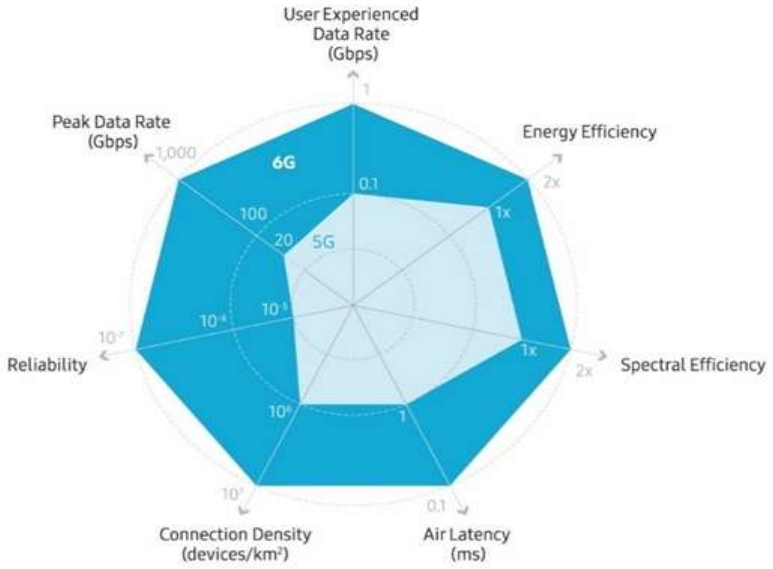
szavak összetételéből ered, és Neal Stephenson 1992-es Snow Crash című regényéből származik, ahol egy számítógép által létrehozott univerzumot jelöl. Forrás: *Metaverzum*. Lexiq.hu. Online: https://lexiq.hu/metaverzum (Letöltés ideje: 2024. június 22.)

[373] Új mintavételezési elméleti kutatási módszer, amely a Nyquist-mintavételnél jóval kisebb gyakoriság mellett, véletlenszerűen mintavételez a jelet leíró részleges információ kinyerése érdekében, melynek alapján képes a teljes jel helyreállítására egy nem lineáris rekonstrukciós algoritmus segítségével.

[374] A hálózat az adott végponti IKT eszköz igényeihez konfigurálja a rádiós erőforrásokat az adott hálózat anélkül, hogy egy problémamentes kommunikációt biztosító adatcserefolyamatra legyen szükség a hálózat két csomópontja között.

[375] GAO, Zhen - KE, Malong - MEI, Yikun- QIAO, Li (2023): Compressive Sensing-Based Grant-Free Massive Access for 6G Massive Communication. *IEEE Internet of Things Journal*, 10(5), 7411 – 7435. Online: https://arxiv.org/pdf/2311.06770.pdf (Letöltés ideje: 2024. február 22.)

[376] MU-HYUN, Cho (2020): *Samsung expects 6G to launch as early as 2028*. ZDNET. Online: https://www.zdnet.com/article/samsung-expects-6g-to-launch-as-early-as-2028/ (Letöltés ideje: 2024. február 22.)



13. ábra: Az 5G és 6G fő teljesítménykövetelményeinek összehasonlítása (Szerk.: A forrás[377])

A Samsung egy másik előrejelzése számos, a 6G-vel kapcsolatos szempontot vetít előre, ideértve a műszaki és társadalmi megatrendeket, új szolgáltatásokat, technológiákat is. A 6G-nél jelenleg a fő fejlesztési irány a dinamikus frekvenciahasználat, további cél a még nagyobb párhuzamosan csatlakoztatható eszközök számának növelése is. A 6G szabvány publikálása 2028-ban, míg a technológia tömeges kereskedelmi forgalomba hozatal 2030 körül várható. Előreláthatólag mind az emberek, mind pedig a gépek egyaránt a 6G felhasználói lesznek, ugyanis olyan fejlett szolgáltatások biztosítása jellemezheti majd, mint például a VR/AR, a mobil hologram és a digitális replika technológia elterjedése.[378] A német Szövetségi Kutatási és Oktatási Minisztérium által finanszírozott komplex rendszer és kiegészítő technológiák fejlesztésére létrehozott 6Ga 6G NeXt projekt már az 5G-n túlmutatóan vizsgálja a 6G mobil hírközlési technológiára épülő valós 3D (holografikus) kommunikáció megvalósíthatóságát, elemezve az ezt megalapozó hírközlési infrastruktúra követelményrendszerét. A kutatás eredményei alapján a holografikus kommunikáció elterjedt alkalmazás lesz az egymással együttműködni kívánó személyek között a jövőben. A tervezett szolgáltatás megvalósításához elengedhetetlen egy nagyszámítási kapacitással és átviteli sebességgel rendelkező megosztott IKT gerinc-infrastruktúra, amely képes a megosztott adatfeldolgozás[379] megvalósítására. A

[377] MU-HYUN 2020
[378] SUNGHYUN, Choi (2022): *6G - Spectrum Expanding the Frontier* IEEE International Conference on Communications 2022. Online: https://news.samsung.com/global/samsung-unveils-6g-spectrum-white-paper-and-6g-research-findings (Letöltés ideje: 2024. február 22.)
[379] Az adatfeldolgozás folyamata megoszlik a végponti eszköz és az EDGE peremoldali számítási kapacitás között.

kutatók kidolgozták a holografikus 3D-s kommunikáció megvalósításának egy lehetséges módját, követelményrendszerét, azaz a holografikus hírközlés informatikai architektúráját.[380]

Az Európai Űrügynökség álláspontja alapján a földfelszíni és a műholdas hálózatok konvergenciája segítheti elő a 6G bevezetésének fejlesztését. A 6G esetében a műholdas összeköttetés igényét az indokolja, hogy általános teljes körű lefedettségre van szükség, melyet a földi infrastruktúra nem tud kiszolgálni. Példaként hozhatók az önvezető járművek, melyek nemcsak autópályákon, hanem városi, és urbanizálatlan környezetben is közlekednek, ezért szinte mindenhol szükséges számukra hálózati lefedettség.[381] A 6G bevezetése terén, akárcsak 2005-ben a 4G-nél, 2012-ben a 4G/VoLTE-nél és 2019-ben az 5G-nél szintén Dél-Korea kíván globálisan vezető szerephez jutni, annak 2030-ra történő lakossági bevezetésére irányuló kormányzati szándék alapján. A Tudományos és IKT Minisztérium 2023. február 20-ai nyilatkozata alapján „*A K-Network 2030 terv keretében a dél-koreai kormány [2030-hoz képest] két évvel előmozdítja a 6G hálózat kereskedelmi szolgáltatásának elindítását a világszínvonalú 6G technológiák biztosításával, a szoftveralapú újgenerációs mobilhálózat fejlesztésével és a hálózati ellátási lánc megerősítésével.*”[382]

A magyar nemzeti érdekek ágazati érvényesítése, valamint az űriparban rejlő lehetőségek kiaknázása érdekében a magyar kormány 1606/2021. (VIII. 18.) határozatával kihirdette Magyarország 2030-ig szóló Űrstratégiáját (a továbbiakban: Űrstratégia). Az Űrstratégia célrendszere meghatározza. „*az innovációt és fenntartható gazdasági növekedést ösztönző lehetőségek kiaknázását, Magyarország nemzetközi szerepének erősítését, valamint az űrszektor prosperálásához elengedhetetlen tudásalapú társadalmi és gazdasági feltételek, és a szükséges infrastruktúra fejlesztését.*”[383] Kiemelt jelentőségű az Űrstratégia *Önálló műholdprogram* című fejezete, amely célként határozza meg, hogy a piaci szektor szereplőjeként az állami tulajdonú CharpathiaSat Zrt. 2024-ben geostacionárius pályára állítsa

[380] FRIESE, Ingo - GALKOW-SCHNEIDER, Mandy – BASSBOUSS, Louay – ZOUBAREV, Alexander (2024): *True 3D Holography: A Communication Service of Tomorrow and Its Requirements for a New Converged Cloud and Network Architecture on the Path to 6G*. Paris: IEEE 2023 2nd International Conference on 6G Networking (6GNet). Online: https://pfandzelter.com/publication/2023-6gnet/holography-6gnet2023.pdf (Letöltés ideje: 2024. február 22.)

[381] HURST, Luke (2023): *How will 6G change the world? This is what experts at Mobile World Congress think*. Euronews.next. Online: https://www.euronews.com/next/2023/02/28/how-will-6g-change-the-world-this-is-what-experts-at-mobile-world-congress-think (Letöltés ideje: 2024. február 22.)

[382] BORAM, Kim (2023): *S. Korea plans to launch 6G network service in 2028*. Seul:Yohnap News. Online: https://en.yna.co.kr/view/AEN20230220003000320 (Letöltés ideje: 2024. február 22.)

[383] TÓTH 2022: 88-89

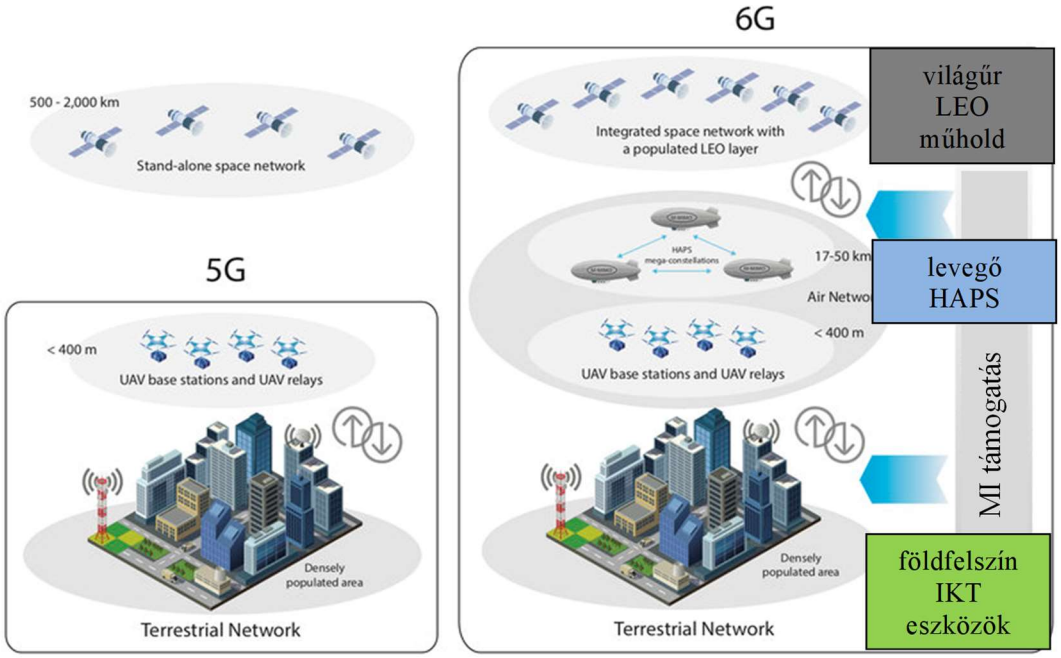
Magyarország első kereskedelmi műholdját. Ezen projektek mellett kiemelendő a földi vevőállomások kapacitásbővítése és korszerű antennarendszer kiépítése.[384]

A műhold-alapú kommunikációs rendszerek – már az 5G, de elemi szinten – a 6G hálózatok kulcsfontosságú elemei lesznek, tekintettel a teljes területi lefedettséget biztosító mindenhol hozzáérhető szolgáltatás iránti EU-es elvárásokra is. A Bolognai Egyetem[385] kapcsolódó kutatásának fókuszában az 5G, de a 6G által is potenciálisan alkalmazandó MiMo digitális nyalábképzéssel kapcsolatos kihívások álltak az alacsony földkörüli pályán keringő kommunikációs műholdak tekintetében. A nyalábképzési vektorok közötti optimalizálási problémák kiküszöbölése és az eljárási hatékonyság növelése érdekében a kutatók egy a felhasználók jel-szivárgás/zaj arányának maximalizálásán alapuló, az alacsony földkörüli pályán keringő (a továbbiakban: LEO[386]) műholdak és szatellitek sajátosságait figyelembe vevő nyalábképzési algoritmusra tettek javaslatot a spektrális hatékonyság növelése érdekében.[387]

A fentiek alapján megállapítható, hogy a 6G hálózatok erőteljesen támaszkodni fognak a földi és légi, világűr hálózatok integrált alkalmazására a kiemelt területi lefedettség biztosítás érdekében. Az elektronikus hírközlési hálózat, infrastruktúra alapvető elemei lesznek a nagymagasságú kommunikációs platformállomások (a továbbiakban: HAPS[388]), amelyek egyfajta relé szerepet fognak betölteni a műholdak, valamint a légi és a földi IKT végpontok között. A jövő 6G hálózatában – az 5G-től eltérő 2 vertikális szintű helyett – egy olyan MI-vel támogatott, integrált, háromrétegű vertikálisan heterogén elektronikus hírközlési hálózati (a továbbiakban: VHetNet[389]) modell megvalósulás vetíthető előre, amely világűr (LEO műholdak), légi (HAPS) és földfelszíni (IKT eszközök – kiszolgáló és végponti) hálózati infrastruktúra elemekből fog összetevődni. A VHetNet infrastruktúrában az antennahálózat a magasságtól és a funkcióktól függően két alrétegből fog állni, az első alréteget a HAPS-ok, míg a második alréteget a pilóta nélküli légijárművek (a továbbiakban: UAV[390]) csomópontjai, relái

[384] Űrstratégia 78-80. pont
[385] Mely egyben a római jog középkori restitúciójának, a glosszátorok kiemelkedő szellemi műhelye volt. A kutatás alapján a 21. századra a technológiai innovációs kutatásokban is jeleskedik a kutatóhely.
[386] LEO: low Earth orbit – alacsony földkörüli pálya
[387] DAKKAK, M. Rabih - RIVIELLO, Daniel Gaetano - GUIDOTTI, Alessandro - VANELLI-CORALLI, Alessandro (2023): Evaluation of multi-user multiple-input multiple-output digital beamforming algorithms in B5G/6G low Earth orbit satellite systems. *International Journal of Satellite Communications and NetworkingEarly View*, Special Issue, 1-16. Online: https://onlinelibrary.wiley.com/doi/epdf/10.1002/sat.1493 (Letöltés ideje: 2024. február 22.)
[388] HAPS: High-Altitude Platform Station - nagymagasságú platformállomás
[389] VHetNet: Vertical Heterogeneous Network - vertikálisan heterogén elektronikus hírközlési hálózat
[390] UAV: Unmanned Aerial Vehicles – pilóta nélküli légijármű

alkotják majd. Ebben az architektúrában a kapcsolatot a szabadtéri optikai (a továbbiakban: FSO[391]) kommunikáció biztosíthatja.[392] A 6G alapú, MI támogatott, integrált VHetNet infrastruktúra összehasonlítására az 5G 2 rétegű infrastruktúrával az alábbi 14. ábra hivatott.

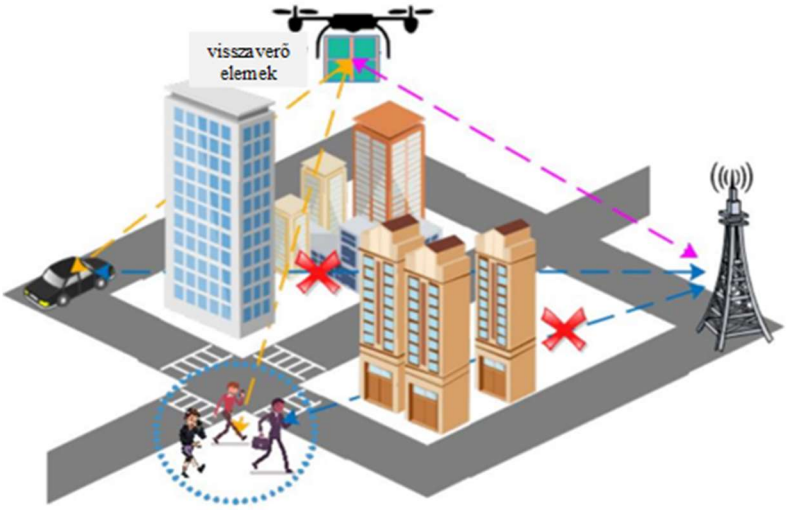


14. ábra: 6G alapú, MI támogatott, integrált VHetNet infrastruktúra összehasonlítása az 5G 2 vertikális rétegű infrastruktúrájával (Szerk.: A szerző[393])

A 6G VHetNet-nél az IRS egy ígéretes technológia, amely támogatja az intelligens vezeték nélküli hálózati kommunikációt. Az IRS adaptív módon az adott RAN elem felületére integrált nagyszámú „tükör" révén képes a rádióhullámfaktorok módosítására (például fázis, frekvencia, amplitúdó, polarizáció tekintetében) anélkül, hogy a rádióláncokat módosítaná. Röviden, az IRS egy olyan eszköz, relé, amely képes lehet a rádiójelek hatékony, intelligens, adaptív közvetítésére, így a kommunikációs teljesítmény növelésére az adó és a vevő között, egyben a spektrum- és energiahatékonyságot növelve, és csökkentve az üzemeltetés költségeit. Az IRS-sel kapcsolatos kutatások rohamosan terjednek szerte a világon, kiemelten az IRS integrált alkalmazására egy komplex digitális IKT ökoszisztémában, például az UAV-k, mint alacsony magasságú HAPS-ok tekintetében. A Cornell Egyetem kutatói megállapították, hogy az UAV-

[391] FSO: Free-space Optical – szabadtéri optika
[392] KUR, Gunes Karabulut at al. (2021): A Vision and Framework for the High Altitude Platform Station (HAPS) Networks of the Future. *IEEE Communications Surveys & Tutorials*, 23(2), 731. Online: https://ieeexplore.ieee.org/document/9380673 (Letöltés ideje: 2024. február 22.)
[393] KUR 2021: 3

vel integrált mobil kommunikáció valós idejű felhasználás esetén kitett számos biztonsági kihívásnak, sérülékenységnek, melyek egy részére az IRS támogatott UAV technológia együttes alkalmazás kínálhat megoldási lehetőséget[394]. Az UAV elemekkel rendelkező VHetNet kommunikációs folyamatát az alábbi 15. ábra hivatott szemléltetni.



15. ábra: IRS támogatott UAV VHetNet kommunikáció (Szerk.: A forrás[395])

A kutatás rávilágít ezen új 6G alapú 3 rétegű elektronikus hírközlési hálózatok FSO kommunikációjának kiberbiztonsági kihívásaira, hiszen az előrejelzések szerint szinte az összes mobil hírközlési szolgáltatás légi interfészen keresztül fog megvalósulni ebben a konstrukcióban. A közelmúltban a hagyományos kriptográfiai eljárások, algoritmusok helyett a kutatók egy alternatív technológiát, a fizikai rétegbiztonság (a továbbiakban: PLS[396]) koncepciót javasolták a HAPS alapú vezeték nélküli hírközlő hálózatok biztonsági kihívásaink megoldására.[397]

---

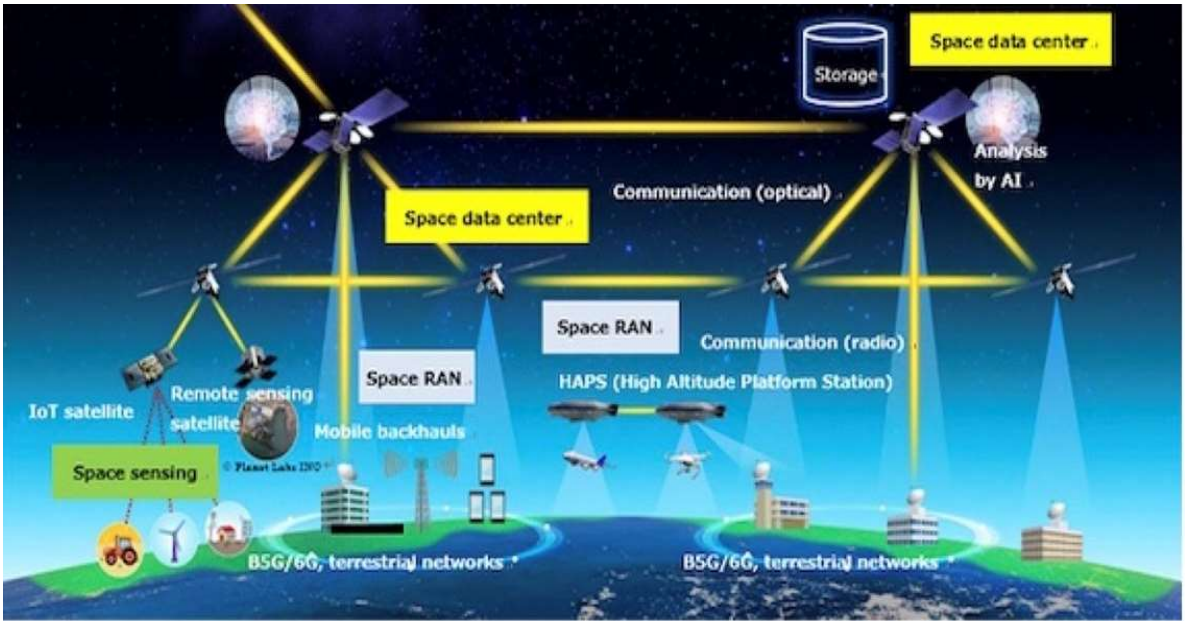
[394] MOHSAN, Syed Agha Hassnain – LI, Yanlong (2023): *IRS-assisted UAV Communications: A Comprehensive Review*. New York: Cornell University. 11. Online: https://arxiv.org/ftp/arxiv/papers/2306/2306.15838.pdf (Letöltés ideje: 2024. február 22.)

[395] MOHSAN 2023

[396] PLS: Physical layer security – fizikai rétegbiztonság. Lásd: ARA, Israt – KELLEY, Brian (2023): 6G Physical Layer Security. PH.D. DOMÍNGUEZ-MORALES, Manuel Jesus at al. (edit.): *Deep Learning - Recent Findings and Researches*. London: IntechOpen. Online: https://www.intechopen.com/online-first/88429 (Letöltés ideje: 2024. február 22.); SANENGA, Abraham – MAPUNDA, Galefang Allycan – JACOB, Tshepiso Merapelo Ludo – CHUMA, Joseph Monamati at al. (2020): An Overview of Key Technologies in Physical Layer Security. *Entropy Reviews*, 22(11), 1261. Online: https://www.mdpi.com/1099-4300/22/11/1261 (Letöltés ideje: 2024. február 22.)

[397] A kutatók rámutatva az FSO-ra épülő HAPS-ok jelentőségére, három feltételezett lehallgatási módszer, támadás forgatókönyve alapján elemezték a HAPS PLS biztonsági koncepcióját. Ennek keretében elemezték a PLS hatékonyságának számszerűsítése érdekében a titkosítási zavarok valószínűségét (POS2), a pozitív titkosítási kapacitás valószínűségét (PPSC), az átlagos titkosítási kapacitást, teljesítményt (ST). Továbbá, javaslatokat

A fenti kutatási eredmények alapján megállapítható, hogy a nem is olyan távoli jövő MI-vel támogatott, integrált, VHetNet rendszerek LI-je mind a 3 rétegű föld/levegő/világűr infrastruktúrán, mind a kriptográfiai környezet fejlődésén túl, a személyes adatvédelem, -adatkezelés terén is kihívásokkal fog szembesülni, ami pedig vizsgálandó normatív jellegű kérdéseket is felvet a jövő LI technológiái szempontjából.[398] A 6G alapú, MI támogatott, integrált VHetNet infrastruktúra űradatközpontokkal kiegészített sematikus ábráját az alábbi 16. ábra hivatott szemléltetni.



16. ábra: A VHetNet infrastruktúra űradatközpontokkal kiegészített sematikus ábrája (Szerk.: A forrás[399])

A fentiekben levezetett IKT „boom”-ot információelméleti oldalról megvizsgálva megállapítható, hogy a Claude Shannon által 1948-ban felállított klasszikus három szintű (technológia, szemantika, hatékonyság) információelmélet matematikai modellje[400] elavulttá válik, hiszen az IKT környezet fejlődése következtében, már az 5G mobilkommunikációs hálózat és attribútumai is számos szűk keresztmetszettel néznek szembe. A hálózati kapacitás

tettek a biztonságos HAPS rendszerek megvalósítására vonatkozóan. Lásd: ERDOGAN, Eylem at al. (2023): Optical HAPS Eavesdropping in Vertical Heterogeneous Networks. *IEEE Open Journal of Vehicular Technology*, 4(1), 208-216. Online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10004986 (Letöltés ideje: 2024. február 22.)

[398] Ezen a ponton szükséges kitérni az Eht. 188. § 129. pontja szerinti űrszegmens fogalmára, „*mely műholdas távközlési rendszer része, amely magában foglalja a műholdat és a műholdkövetési, távmérési és távvezérlési funkciókat, valamint a műholdak részére logisztikai támogatást nyújtó földi berendezéseket.*”, tehát integrált VHetNet rendszernél a felső vertikális réteg eszközeit és a földi kiszolgáló rendszerelemeket is.

[399] LE MAISTRE 2022

[400] SHANNON, Claude E. (2001): A mathematical theory of communication. *Computing and Communications Review*, 5(1) 3–55. Online: https://dl.acm.org/doi/10.1145/584091.584093 (Letöltés ideje: 2024. február 22.)

közeledik a „Shannon-határhoz”, a forráskódolási hatékonyság közel áll a „Shannon-információhoz” és az entrópia/sebesség torzítási függvény határértékéhez. A hálózati kapacitásoptimalizáció kapcsán a legújabb kutatási eredmények az ún. szemantikus kommunikációt a 6G egyik potenciális, kulcsfontosságú lehetőségeként tartják számon. Kutatása dinamikusan zajlik, hiszen a jövő feltörekvő, diszruptív technológiái esetében a K+F+I igények kielégítése, a kommunikáció hatékonyságának és átviteli kapacitásának javítása érdekében fokozottan szükség van új információ-reprezentációs térre, melyre potenciál a szemantikus kommunikáció[401] elmélete.[402] A jelen és előző részfejezetben feltüntetett egyes mobil hírközlési technológiák főbb jellemzőinek összefoglalására az alábbi 17. ábra hivatott.

Jeltípus	Technológia	Megjelenés éve	Sávszélesség	Közlemény típusa
Analóg	1G	1980	9,6 kbit/s	hang
Digitális	2G (GSM)	1990	14,4 kbit/s – 236 kbit/s	hang, SMS, MMS
	3G	1998 (Mo.:2001)	384 kbit/s – 14,4 Mbit/s	hang, SMS, MMS, internetes tartalom (weboldalak, fájl, szöveg, kép, hang, [korlátozottan, és nem valós időben] videó)
IP-alapú	4G/LTE	2005 (Mo.: 2012)	10 Mbit/s – 326 Mbit/s	+ internetes tartalom – hang és élő videostream
	4G/VoLTE	2012 (Mo.: 2017)		+ hang és élő videostream
	5G	2017 (Mo.: 2019)	1 Gbit/s – 10 Gbit/s	+ rendkívül nagyméretű internetes tartalom
	6G	2030?	1 Tbit/s	VR, AR, IoT, SmartTech

17. ábra: A mobil hírközlési technológiák főbb jellemzőinek összefoglaló ábrája (Szerk.: A szerző)

Részkövetkeztetésként megállapítható, hogy a mobiltechnológiák terén kb. 10 évente tapasztalható egy generációugrás, amely a sávszélesség bővülése, az adatátviteli sebesség növelése, és a késleltetési idő csökkentése terén érzékelhető fejlődést mutat, a hálózati forgalom folyamatos heterogenizációja mellett, a fogyasztói igények, és az új IKT szolgáltatások

[401] A szemantikus kommunikáció szemantikai jellemzőket von ki a nyers adatokból, majd kódolja és továbbítja azokat. Ez várhatóan mérsékli a hálózatokban detektálható és az 5G, 6G kapcsán csak fokozódó szűk adatátviteli kapacitás kihívásait a hírközlő hálózatokon.

[402] SHAO, Yulin- CAO, Qi – GUNDUZ, Deniz (2023): *A Theory of Semantic Communication*. New York: Cornell University. Online: https://arxiv.org/pdf/2303.05181.pdf Letöltés ideje: 2024. február 22.)

kiszolgálása érdekében, mely a jövőben a VR/AR terén is hozzáadott értéket produkálhat, az okos város infrastruktúrákban rejlő lakossági célú szolgáltatások igénybevételének lehetősége mellett, így haladva az EU által is meghatározott társadalmi digitalizáció irányába. A hazai 5G fejlesztés és bevezetés kapcsán megállapításra került, hogy a Yettel publikus 5G SA szolgáltatásához a hozzáférést 2024-ben kívánja kialakítani. Megállapításra került az egyes okos város-alkalmazások, komponensek rendkívül komplex, heterogén digitális ökoszisztémája. Az ezeket kiszolgálni képes 5G, de inkább már 6G alapú, MI támogatott, integrált VHetNet elektronikus hírközlő technológiák tekintetében is kihívást jelent a végeláthatatlan számosságú hálózathoz csatlakozó IKT eszköz, azok konnektivitása, az abból adódó gigászi mennyiségű egyidejű adat, a maximális hálózati területi lefedettség, a rendkívül nagy adatátviteli sebesség, a minimális késleltetési idő. A fejlett 5G-nél is, de szintén inkább az azt követő technológiáknál a személyközi hírközlés során már megjelenik a VR/AR kommunikáció, a holografikus hírközlés igénye. A MiMo technológia a frekvenciahatékonyság fokozásán túl lehetőséget biztosít például az okosközlekedés fejlődésére. A 6G bevezetése terén, akárcsak 2005-ben a 4G-nél, 2012-ben a 4G/VoLTE-nél és 2019-ben az 5G-nél szintén Dél-Korea kíván globálisan vezető szerephez jutni, annak 2028/2030-ra történő lakossági bevezetésére irányuló kormányzati szándék alapján. Magyarország Űrstratégiájának célrendszere meghatározza a gazdasági növekedést elősegítő űriparban rejlő lehetőségek kiaknázását, illetve az ehhez szükséges társadalmi, gazdasági, és ipari fejlesztéseket.

3.1.3. Mobil hírközlőhálózatok kriptográfia evolúciója, és az LI szabványosítás

A digitális, kódolt és a levegő interfészen is titkosított 2G (GSM) hálózatokon a beszédhang, valamint az adatok továbbítása sokkal biztonságosabbá vált, mint az analóg rendszerek esetében, többek között köszönhetően az akkor modern A5/1, /2 blokkrejtjelező kriptográfiai algoritmusoknak.[403] A GSM A5 egy titkosítási algoritmus, amelyet a 2G mobiltelefon hálózatokban alkalmaznak a hanghívások és a szöveges üzenetek titkosítására. Az A5 algoritmusok a SIM kártyán lévő kulcsot alkalmazzák a hívó fél és a fogadó fél közötti kommunikáció titkosításra. Az A5/2-t az 1990-es évektől az USA-ban a CDMA hálózatokon alkalmazták először, azonban az a 2000-es évekre sérülékennyé vált.[404]

[403] KULKARNI, Mandar M.– BHIDE, Prof. A. S. – CHAUDHARI, Prafull P. (2013): Encryption Algorithm Addressing GSM Security Issues - A Review. *International Journal of Latest Trends in Engineering and Technology*, 2(2), 268. Online: https://www.ijltet.org/wp-content/uploads/2013/04/40.pdf (Letöltés ideje: 2024. február 21.)
[404] KULKARNI at al. 2013: 268

A 3G hálózatok titkosítási algoritmusai különböznek a GSM-től. A 3GPP egyesítette az összes 3G biztonsági szabványt, amelynek köszönhetően az összes 3G hálózat ugyanúgy az A5/3[405] kriptográfiai algoritmust használja. Az A5/3, vagy másnéven KASUMI[406] egy kulcs- vagy adatfolyam rejtjelező algoritmus, melyet a rejtjelfejtő módszerek fejlődése okán az AES[407] algoritmus kiegészített. A KASUMI egy 128 bites blokkrejtjelező, amely 128 bites kulcsot használ, továbbá a MAC-kal ellátott, a 3GPP által szabványosított MILENAGE[408] autentikációs és véletlenszám-generátor algoritmust[409] alkalmazza a bizalmasság és hitelesség biztosítása érdekében a légi interfészen történő kommunikáció során. Noha a KASUMI-ról bebizonyosodott, hogy vannak sérülékenységei, még mindig viszonylag erős titkosítási algoritmusnak tekintik, és világszerte használják a 3G, valamint a 4G hálózatokban is egyaránt. A 128 bites KASUMI-t 2010-ben az izraeli Weizmann Tudományos Intézetben igazoltan fel tudták törni.[410]

A 4G LTE már az AES blokkrejtjelező algoritmus mellett a KASUMI-t kiváltó 128 bites SNOW 3G[411] és ZUC[412] kulcsfolyam rejtjelező algoritmust is integrálja, amelyek célja, hogy biztonságosabbá tegyék a 2G és 3G hálózatoknál alkalmazott, az idő során elavuló algoritmusokat. A Thomas Johansson és Patrik Ekdahl által a svédországi Lund Egyetemen kifejlesztett, és a 3GPP által szabványosított SNOW 3G egy 128 bites kulcsfolyamrejtjelező, amelyet az 5G mobiltelefonhálózatokban alkalmazott rejtjelező eljárások egyikeként is kiválasztottak.[413] A SNOW 3G-t lényegében a hálózatok belső kommunikációinak titkosítására használják, és ezt kiegészíthetik más titkosítási és hitelesítési eljárásokkal is. A SNOW 3G két

[405] 3GPP TR 33.908 - 3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms; 3GPP TS 55.216 - Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS

[406] 3GPP TS 35.202. - Key Allocation and Stream ciphering UMTS Interface - kulcskiosztás és adatfolyam titkosítás UMTS interfész

[407] Advanced Encryption Standard - fejlett titkosítási szabvány (NIST Special Publication 800-38B (2005))

[408] MILENAGE: MIcrosoft Local Exchange Network Access GEnerator -

[409] 3GPP TS 35.205 - 3G Security: Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*.

[410] LAI, Richard (2010): *3G GSM encryption cracked in less than two hours*. Engadget. Online: https://www.engadget.com/2010-01-15-3g-gsm-encryption-cracked-in-less-than-two-hours.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAALBTMnOk12PZGvXoKxD4BbP5rBK7GxrdAmBAQrudtQ4QvbrqmrWwrDcDZj4CIhtgHQSCD2nU0Ih8i4IXPaUN7745YYiIi6y4Op5jE0myIJgMUkygjkbGuM9xfN2BRL2GLriURK5d3g-Yz5YScK20sxevexbdmmzhLJAAad0aLErc (Letöltés ideje: 2024. április 1.)

[411] 3GPP TS 35.215 - SNOW 3G

[412] 3GPP TS 35.221 – ZUC: Zu Chongzhi stream Chiper –ZU adatfolyam titkosítás

[413] TAKIELDEEN, Ali - ASHRAF, Eman - FAYEZ, Nihal - MOHAMED, Mohamed Abdel-Azim (2017): Novel Cryptographic Algorithm for 4G / LTE-A. *International Journal of Computer Applications*, 143(1), 5. Online:https://www.researchgate.net/publication/316220876_Novel_Cryptographic_Algorithm_for_4G_LTE-A (Letöltés ideje: 2024. február 22.)

részből áll, azaz a SNOW kulcsfolyamrejtjelező algoritmusból és az LFSR[414] véletlenszámgenerátorból. Az LFSR azonban csak korlátozott számú állapotot generálhat, ami azt jelenti, hogy a generált bit-sorozatok előbb vagy utóbb ismétlődnek.[415] A SNOW 3G használata javítja a hálózatok biztonságát például DPI támadása szemben. A ZUC egy modern szinkronizációs kulcsfolyamrejtjelező, amely az inicializálást és a kulcsgenerálását tartalmazza, a 128 bites titkosítási kulcs/integritáskulcs és az inicializálási vektor protokolljai szerint.[416]

Az 5G szabványosítása a 3GPP és az ETSI által 2017 óta zajlik. A Release 17 5G szabványcsomag 5G biztonsági szabványa[417] alapján a technológia a 128 bites kulcsfolyam rejtjelező SNOW 3G és ZUC, valamint a blokkrejtjelező AES algoritmusokon kívül integrálja a webes forgalom védelmére a JWE[418] kriptográfiai protokollt is, amely keretrendszer támogatja az új, innovatív 5G-AKA[419] üzenethitelesítő és kulcscsere protokoll[420] használatát. Továbbá a SIM kártya IMSI[421] és az új SUPI[422] azonosítók védelmére az ajánlás megfogalmazza az ECIES[423] elliptikus görbetitkosítás alkalmazását. [424]Az 5G-AKA protokoll több lépésből áll, beleértve a mobileszköz és a hálózat közötti kommunikációs rejtjelezését, a rejtjelkulcsok generálását és elosztását. A protokoll megosztott titkos kulcsot hoz létre a felhasználói végponti IKT eszközök és az 5G rádiós hálózati vezérlőelemei (RNC[425]) között, amelyet aztán a rejtjelezés és a megoldás során alkalmaz. A protokollt úgy tervezték, hogy teljes körű biztonságot és adatvédelmet biztosítson, védje a felhasználói adatokat és megakadályozza az illetéktelen hozzáférést. A protokoll szimmetrikus és aszimmetrikus titkosítási algoritmusok

[414] LFSR: Linear Feedback Shift Register

[415] KIRCANSKI, Aleksandar – YOUSSEF, Amr M. (2012): *On the Sliding Property of SNOW 3G and SNOW 2.0*. Montreal: IET Information Security, 4(5), 199-206. Online: https://users.encs.concordia.ca/~youssef/Publications/Papers/On%20the%20Sliding%20Property%20of%20SNOW%203G%20and%20SNOW.pdf (Letöltés ideje: 2024. február 21.)

[416] HASSAN, Zakaria Abdelwahab - ELGARF1, Talaat A. – ZEKRY, Abdelhalim (2020): Analyzing SNOW and ZUC Security Algorithms Using NIST SP 800-22 and Enhancing their Randomness.. *Journal of Cyber Security and Mobility* 9(4), 535–576. Online: https://journals.riverpublishers.com/index.php/JCSANDM/article/view/2963/5089 (Letöltés ideje: 2024. február 21.)

[417] 3GPP TS 33.501 version 17.5.0 Release 17; ETSI TS 133 501 V17.5.0 (2022-05.): 39, 47-49, 221-227

[418] JWE: JavaScript Object Notation Web Encryption – JavaScript web kriptográfia

[419] 5G-AKA: 5G Authentication and Key Agreement – 5G autentiákciós és kulcs tanúsítvány

[420] 3GPP TS 33.535. - Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)

[421] IMSI: International Mobile Subscriber Identity - nemzetközi mobil-előfizetői azonosító

[422]Subscription Permanent Identifier - előfizetés állandó azonosítója: (Az 5G hálózatokban használt új azonosító, amely az IMSI-t váltja fel, az előfizető azonosítására és a hálózaton való hitelesítésére szolgál.)

[423] Elliptic Curve Integrated Encryption Scheme - elliptikus görbével integrált titkosítási séma

[424] KOUTSOS, Adrien (2019): *The 5G-AKA Authentication Protocol Privacy*. Stockholm: IEEE Institute of Electrical and Electronics Engineers. 464-479. Online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8806761 (Letöltés ideje: 2024. február 21.)

[425] RNC: Radio Network Controller – rádiós hálózati vezérlő

kombinációját használja, beleértve az elliptikusgörbéket, mint például az ECDH-t, valamint a HMAC-et is. Ezenkívül az 5G számos biztonsági funkciót tartalmaz a támadások megelőzésére és a kommunikációs csatorna integritásának biztosítására, beleértve a digitális tanúsítványok használatát, a biztonságos rendszerindítást és az érzékeny adatok biztonságos tárolását is.[426] Összességében az 5G titkosítási mechanizmus magas szintű biztonságot nyújt az eszközökön és a hálózati kommunikációhoz, így megfelelve egyben az uniós digitalizációs törekvések keretében érvényesülő szigorú adatvédelmi előírásoknak a kibervédelem logikai védelmi elemeként. A 6G hálózatok kapcsán pedig már megjelenik a hagyományos kriptográfiai eljárások, algoritmusok helyett az alternatív fizikai rétegbiztonsági (PLS[427]) koncepció, mely szabványosítása várható.

Mint az az előzőekben már ismertetésre került, az elektronikus hírközlő hálózatok vonatozásában akár 2G, 3G, 4G, 5G technológiáról beszélünk, az LI monitoring alrendszerrel szemben támasztott általánosan elvárt technológiai követelmények nemzetközileg szabványosított, transzparens formában kerülnek definiálásra a szolgáltatók számára. Ahhoz, hogy ezek közül mely követelményrendszert fogalmazza meg az adott állami LI szervezet a szolgáltatók irányába, nincsen kötve. A 3GPP és az ETSI az 1990-es elején az elektronikus hírközlő szolgáltatásokra vonatkozó követelmények mellett szabvány szintjén kezdték el rendezni az LI számára szükséges forgalomkicsatolási műszaki megoldásokat, azaz a LEA[428] interfészeket, mint minden szolgáltató számára nyilvános és számonkérhető műszaki követelményrendszert. A 3GPP transzparens tájékoztatása szerint 2G, 3G, 4G és 5G mobilhálózatok vonatkozásában is rendelkezik LI-hez szükséges nemzetközi műszaki ajánlással.[429] Az FBI a szabványok kapcsán például az USA Bűnüldözési Ügynökségek Akkreditációs Bizottsága (a továbbiakban: CALEA[430]) által jegyzet iparági ajánlásokat

[426] NAIR, Suresh – KHARE, Saurabh – PING, Jing (2022): Authentication and Key Management for Applications (AKMA) in 5G. *Highlights,* 2(5), 4-5. Online: https://www.3gpp.org/newsletter-issue-05-oct-2022 (Letöltés ideje: 2024. február 21.)

[427] PLS: Physical layer security – fizikai rétegbiztonság. Lásd: ARA, Israt – KELLEY, Brian (2023): 6G Physical Layer Security. PH.D. DOMÍNGUEZ-MORALES, Manuel Jesus at al (edit.): *Deep Learning - Recent Findings and Researches*. London: IntechOpen. Online: https://www.intechopen.com/online-first/88429 (Letöltés ideje: 2024. február 22.); SANENGA, Abraham – MAPUNDA, Galefang Allycan – JACOB, Tshepiso Merapelo Ludo – CHUMA, Joseph Monamati at al. (2020): An Overview of Key Technologies in Physical Layer Security. *Entropy Reviews*, 22(11), 1261. Online: https://www.mdpi.com/1099-4300/22/11/1261 (Letöltés ideje: 2024. február 22.)

[428] LEA: Law enforcement agency – rendévdelmi szerv

[429] RIZZO, Carmine (2022): *Lawful Interception in mobile networks*, 3GPP MCC. Online: https://www.3gpp.org/technologies/li (Letöltés ideje: 2023. július 27.)

[430] CALEA: Commission on Accreditation for Law Enforcement Agencies, Inc. - Bünüldözési Ügynökségek Akkreditációs Bizottsága

fogalmaz meg az USA bűnüldöző szerveivel való LI célú együttműködés támogatása, a diskurzus kialakítása érdekében.[431] A korábbi hálózati technológiákon túlmenően már az 5G hálózatok LI-jének biztosítása érdekében támasztható technológiai követelményeket a 3GPP TS 33.126 szabvány, az LI architektúrával és funkciókkal kapcsolatos követelményeket az ETSI 133.127 szabvány, míg az LI protokollokkal kapcsolatos követelményeket a 3GPP TS 33.128 szabvány definiálja. A 3GPP szerveztén belül a 2G, 3G, 4G, 5G mobilhálózatok LI szabványosításával kapcsolatos feladatokat a SA3-LI[432] almunkacsoport végzi, amely publikációjában be is mutatja az LI architektúra magas szintű általános folyamatát, architektúráját,[433] amelyben további szabványosított funkciók is megjelennek.[434]

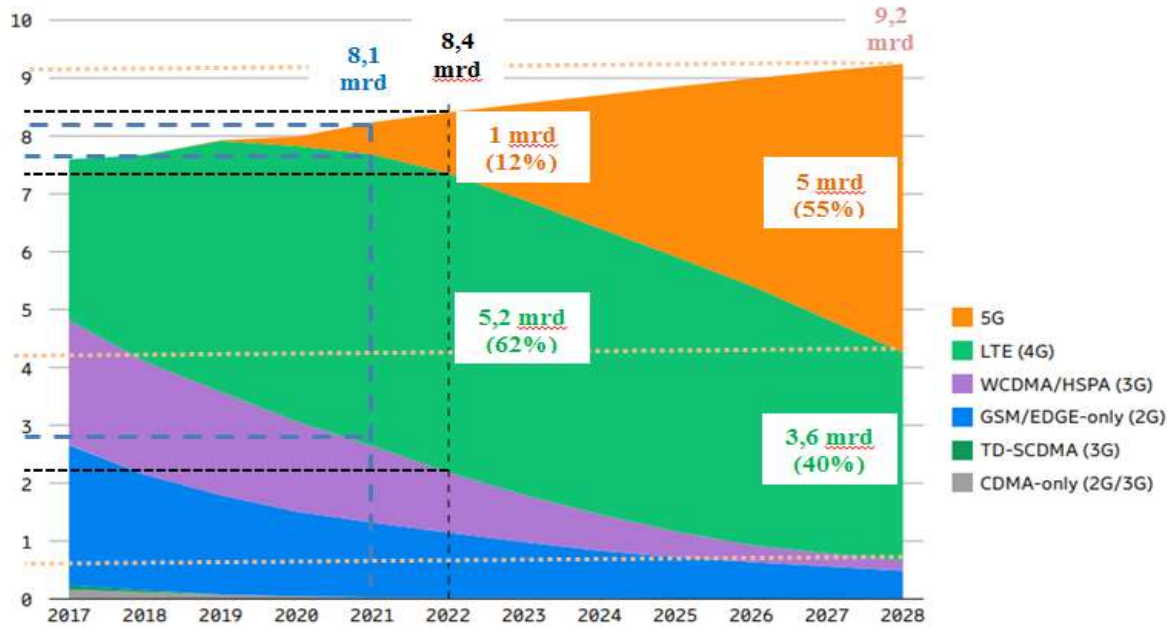
3.2. Mobilhálózatok felhasználói trendjei, tendenciái

Jelen alfejezetben vizsgálat tárgyát fogja képezni elsősorban a trend- és tendenciaelemzés módszerét alkalmazva az egyes személyközi hírközlési szolgáltatásokra jellemző főbb nemzetközi és hazai felhasználói IKT trendek, tendenciák – az IoT trendekre csak kitekintve, a személyközi és IoT kommunikációs trendek összehasonlítása érdekében.[435] Az általános személyközi kommunikációs trendek vizsgálata azért szükséges, hogy megállapítható legyen az IKT szolgáltatások, illetve a mobil hírközlés globális, regionális, illetve hazai várható felhasználói trendjei, melyek prognosztikus szemléletben képesek megalapozni a titkos információgyűjtés, azon belül is az LI szempontjából lényeges stratégiai fejlesztési irányokat.

[431] *Lawful Intercept Standards.* National Domestic Communications Assistance Center. Online: https://ndcac.fbi.gov/calea/lawful-intercept-standards (Letöltés ideje: 2023. július 31.)
[432] SA3-LI: Services and System Aspects 3 (Security) – Lawful Interception - Szolgáltatások és rendszerszempontok 3 (Biztonság) – Törvényes lehallgatás
[433] RIZZO 2022
[434] *EVE Explains: 5G and Lawful Interception*. Hága: EVE. Online: https://www.lawfulinterception.com/explains/5g-and-lawful-interception/ (Letöltés ideje: 2024. február 23.)
[435] Az altémakörrel kapcsolatos korábbi kutatási eredményeimet lásd: TÓTH Tamás (2022): Az információgyűjtés új típusú kihívásai a mobil hírközlési hálózatok technológiai fejlődésének aspektusából. In SZELEI Ildikó (szerk.): *A hadtudomány aktuális kérdései napjainkban*. Budapest: Ludovika Egyetemi Kiadó. 105-122. Online: https://webshop.ludovika.hu/termek/konyvek/hadtudomany/a-hadtudomany-aktualis-kerdesei-napjainkban-ii/ (Letöltés ideje: 2024. február 23.)

3.2.1. Nemzetközi mobil hírközlési kitekintés

Az IKT piac értéke 2022-ben elérte az 5500 Mrd dollárt, 2023-ra pedig 6000 Mrd dollárra tehető az érték.[436] A jövőre nézve a globális ipar növekedése 2024-ig várhatóan öt százalékos összetett éves növekedési rátával folytatódik.[437] 2023-as elemzések szerint az IKT infrastruktúra beruházások értéke globálisan 9%-kal emelkedett. Azonban 2022-ben az orosz-ukrán fegyveres konfliktus hatására az IKT ipar bővülése 2% körülire tehető, amely elmaradt a kb. 4%-os várakozásoktól, „*A kutatók szerint a katonai konfliktus az IKT-ellátási láncok megszakadásához és magasan képzett szakemberek hiányához vezet Oroszországban és Közép-Kelet-Európában.*”[438] Előzetesen szükséges megvizsgálni a mobil előfizetések globális alakulását technológiánként 2030-ig, melyet a 18. ábra hivatott szemléltetni, kiegészítve azt a svédországi Ericsson globális IKT vállalat legfrissebb előrejelzéseivel.



18. ábra: Globális mobil előfizetések megosztása technológiánkként (Szerk.: A szerző[439])

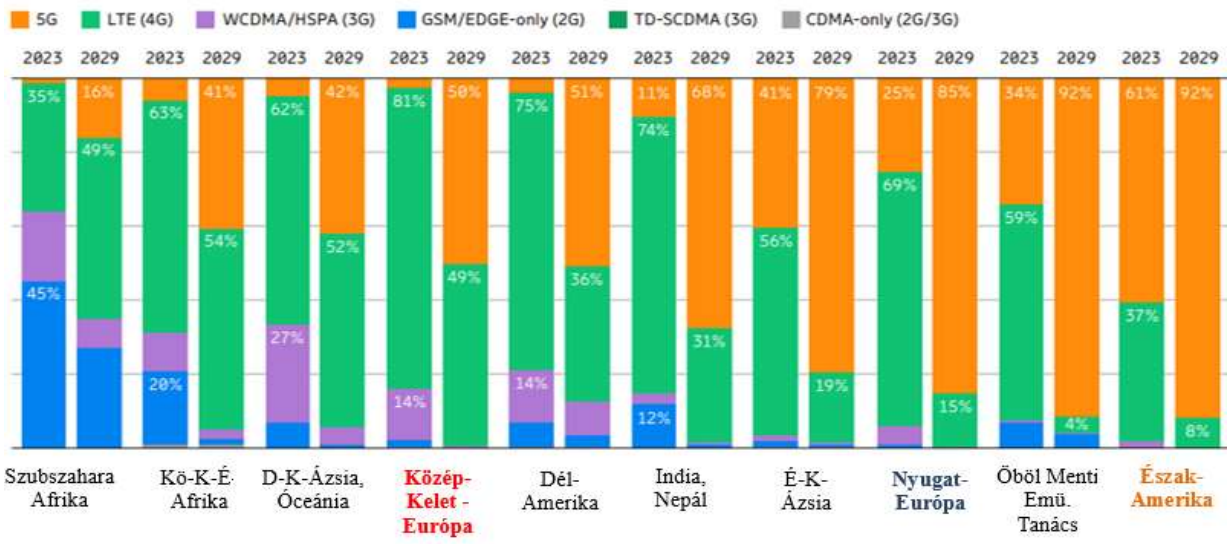
[436] *Global ICT market share 2013-2022, by selected country*. Statista Research Department. 2023. Online: https://www.statista.com/statistics/263801/global-market-share-held-by-selected-countries-in-the-ict-market/ (Letöltés ideje: 2023. november 2.)

[437] SHERIF, Ahmed (2024): *Global information technology industry forecast 2019-2022, by region*. Statista. Online: https://www.statista.com/statistics/507365/worldwide-information-technology-industry-by-region/ (Letöltés ideje: 2024. február 23.)

[438] *ICT (Global Market).* TAdviser. 2023. Online: https://tadviser.com/index.php/Article:ICT_(Global_Market) (Letöltés ideje: 2023. november 2.)

[439] *Ericsson Mobility Report.* Ericsson. 2022. 4. Online: https://www.ericsson.com/4ae28d/assets/local/reports-papers/mobility-report/documents/2022/ericsson-mobility-report-november-2022.pdf (Letöltés ideje: 2024. november 2.)

A 18. ábra alapján látható, hogy 2022-ben globális szinten 8,4 Mrd mobil előfizetés volt, ezek közül a 4G előfizetések számára kb. 5,2 Mrd, ami 62%-os piaci részesedést jelent, míg az 5G előfizetések száma 1 Mrd volt, ami 12%-os részesedést jelent. 2022-ben tehát a 4G alapú mobiltechnológia volt globális szinten a piacvezető. A becsült előrejelzések alapján azonban 2028-ra a 4G előfizetések száma kb. 3,6 Mrd-ra esik vissza, így a technológia részesedése 40%-ra, míg az 5G előfizetések száma kb. 5 Mrd-ra nő, mely egyben 55%-os globális részesedésével piacvezetővé fog válni. Tehát trendszerűen tapasztalható egyfajta kiszorító hatása az újgenerációs mobiltechnológiáknak. A tendenciát elő fogja segíteni a fejlett 5G SA hálózatok szabványosítása, elterjedése és várható népszerűsége. 2023-ra a 2022-es tendenciák nem változtak, ezek alapján a piac 2023-ban 8,5 Mrd mobil előfizetőt realizált globálisan, azonban 2029-re – a 2028-as szinttel azonosan – 9,2 Mrd felhasználót prognosztizálnak az előrejelzések, egyetemben a 4G előfizetések további csökkenésével, az 5G előfizetések további növekedésével, a 6G előfizetések várható alakulását még nem szemléltetve.[440] A fenti globális mobil-előfizetések tendenciájának technológiánkénti regionális megoszlása azonban eltérő, így indokolt azok régiók szerint vizsgálata a 19. ábra szemléltetésével.



19. ábra: Globális mobil-előfizetések százalékos megoszlása régió és technológia szerint 2023/2029-ben (Szerk.: A szerző[441])

[440] *Ericsson Mobility Report*. Ericcson. 2023. 4. Online: https://www.ericsson.com/4ae12c/assets/local/reports-papers/mobility-report/documents/2023/ericsson-mobility-report-november-2023.pdf (Letöltés ideje: 2024. február 23.)
[441] *Ericsson Mobility Report* 2023: 6

2028-ban Közép-Kelet-Európában (a továbbiakban: KKE) az előrejelzés szerint továbbra is a 4G lesz a piacvezető 2028-ban a mintegy 56%-os részesedésével, míg az 5G előfizetések várhatóan 43% körül fognak alakulni.[442] Azonban 2029-ra várhatóan az 5G, mintegy 50%-os piaci részesedésével átveszi a vezető szerepet, a 4G-t 49%-os részesedésre visszaszorítva.[443] 2029-ban Nyugat-Európában (a továbbiakban: NYE) azonban 85%, míg Észak-Amerikában 92% piaci részesedést prognosztizálnak az 5G tekintetében.[444] NYE-ban a szolgáltatások igénybevétele és az adatforgalom növekedése várhatóan szintén hasonló mintát fog követni, mint Észak-Amerikában. Bár a széttagoltabb piaci helyzet az 5G későbbi tömegpiaci bevezetéséhez vezethet, az előrejelzések szerint 2028-ra az okostelefononkénti adatforgalom eléri a havi 52 GB-ot, ami szinte azonos a prognosztizált észak-amerikai mutatókkal. Ez 2022-2028 időszak vonatkozásában 21%-os növekedést mutat, tekintettel arra, hogy a 2022-es NYE-i átlag 17 GB körül alakult. KKE tekintetében az előrejelzett 2028 évi érték 35 GB havi mobil adatfogalom/okostelefon, amely kb. 18 %-kal több a 2022-es 13 GB/hó-nál. Ami figyelemre méltó, hogy az egy okostelefonra jutó havi adatforgalom világátlaga 2022-ben 15 GB/hó volt (2GB-vel maradt el KKE), mely az előrejelzések szerint 2028-ra 46 GB-ra fog nőni (11 GB-vel marad el várhatóan KKE), mintegy 21%-os átlagos bővülést eredményezve (4GB-vel marad el várhatóan KKE). [445] Ugyanezek a tendenciák prognosztizálhatóak 2029-re is.[446]

Tehát 2029-ra KKE várhatóan lényegesen le fog maradni a világátlag egy okostelefonra jutó havi adatforgalmától NYE-hez képest. Ez a lemaradás a publikus, azaz lakossági célú 5G mobil-előfizetések százalékos alakulásában is érzékelhető, hiszen KKE 50%-os, míg NYE 85%-os rátát fog a magáénak tudni várhatóan az adott régióra vonatkozó technológia szerinti prognosztikus megoszlás adatai alapján, ami a 4G tekintetében KKE vonatkozásában 49%-ot, míg NYE esetében 15%-ot mutat. Tehát a fentiek alapján megállapítható, hogy a lakossági mobil hírközlés piacán még inkább nyílni fog az „olló" Közép-Kelet- (így Magyarország) és Nyugat-Európa között. 2029-re NYE a 2. legnagyobb 5G mobil-előfizetési rátát fogja magáénak tudni globális szinten az előrejelzések szerint. Ami azonban még relevánsabb adat, hogy KKE a 2029-es 5G versenybe az utolsó előtti 4. helyezettként be fog ékelődni a fejlődő országok államai és a fejlődő társadalmak közé. Azonban a 2028-as adatokkal összevetve KKE várhatóan 2029-re javít pozícióin, mivel 2028-ra az utolsó előtti 3. helyezést jelezték előre a

[442] *Ericsson Mobility Report* 2022. 6
[443] *Ericsson Mobility Report* 2023: 6
[444] *Ericsson Mobility Report* 2023: 6
[445] *Ericsson Mobility Report* 2022: 23
[446] *Ericsson Mobility Report* 2023: 13

szakértők,[447] azonban Dél-Kelet-Ázsiát, és Óceániát 2029-re meg fogja előzni. Ami pedig összefoglalóan KKE-t illeti, a statisztikai adatok alapján megállapítható, hogy várhatóan az elkövetkező 5-6 évben a 4G mobil hírközlési szolgáltatás lesz a piacvezető, így az LI technológiák tekintetében is erre szükséges koncentrálni. 2029-re az 5G mobil-előfizetések számának versenyét Észak-Amerika fogja nyerni, csaknem 92%-kal, ami azonban kiemelendő, hogy mindezt holtversenyben a Perzsa-öböl menti arab olajmonarchia által 1981-ben létrehozott közös piac, azaz az Öböl Menti Együttműködés Tanácsának[448] országaival, úgymint Kuvait, Bahrein, Katar, az Egyesült Arab Emírségek, Omán és Szaúd-Arábia. Ez azért is érdekes, mert a statisztikai előrejelzések 2028-ra 86%-ot jósoltak a Tanács országainak, mellyel akkor NYE-nak jósolt 88% mögött helyezkedett el,[449] azonban a 2023-as statisztikai becslések szerint megfordul a tendencia.[450]

Az internethez kapcsolódó eszközök tekintetében is indokolt egyfajta összehasonlító jellegű globális kitekintés. Az IoT Analytics kutatása szerint az internethez csatlakoztatott eszközök számának növekedése 2021-ben lelassult, de 2022-től újra felgyorsult. Míg az IoT piacon új kihívások, például infláció és elhúzódó ellátási zavarok jelentek meg, az általános hangulat továbbra is viszonylag pozitív volt, a csatlakoztatott IoT eszközök száma a teljes ipari és lakossági szegmensben az előrejelzéseknek megfelelően 2022 végére elérte a 14,4 milliárdot.[451] Az előrejelzések szerint az IoT eszközök száma 2030-ra világszerte csaknem megháromszorozódik, a 2020-as 9,7 milliárdról 2030-ra több mint 29 milliárd IoT eszközre nő majd, ami havi szinten több ezer exabájtban kifejezhető adatmennyiséget jelent. 2020-ban a lakossági fogyasztói IoT szegmens az összes IoT-hez csatlakoztatott eszköz mintegy 60 százalékát tette ki. Ez az arány az előrejelzések szerint a következő tíz évben is ezen a szinten marad. Az iparági IoT eszközök száma az előrejelzések szerint 2030-ra több mint nyolcmilliárdra nő. A lakossági szegmenst vizsgálva megállapítható, hogy az egyes okoseszközök száma az előrejelzések szerint 2030-ra több mint 17 milliárdra nő.[452] A Samsung Research UK 6G kutatása szerint 2030-ra mintegy 500 milliárd csatlakoztatott gép lesz (ez több

[447] *Ericsson Mobility Report* 2022: 6
[448] *Secretariat General of the Gulf Cooperation Council.* Online: https://www.gcc-sg.org/en-us/Pages/default.aspx (Letöltés ideje: 2024. február 23.)
[449] *Ericsson Mobility Report* 2022: 6
[450] *Ericsson Mobility Report* 2023: 6
[451] HASSAN, Mohammad (2022): *Az IoT-felhő: Microsoft Azure vs. AWS vs. Google Cloud.* IoT Analtics. Online: https://iot-analytics.com/iot-cloud/ (Letöltés ideje: 2024. február 23.)
[452] VAILSHERY, Lionel Sujay (2022): *Number of IoT connected devices worldwide 2019-2021, with forecasts to 2030*. Statista. Online: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (Letöltés ideje: 2024. február 23.)

mint a 10-szerese a fenti előrejelzéseknek), ami a világ népességének 59-szerese. A kutatás szerint mobil- és internetforgalom éves szinten 55%-kal nő, mivel a világ egyre inkább összekapcsolódik az autonóm járművekkel, valamint a VR/AR szolgáltatások száma is növekvő tendenciát mutat. A műholdas hírközlési szolgáltatás keretében nyújtott LEO műholdas kapcsolat az IoT tekintetében is egyre népszerűbb, mivel kiterjedt lefedettséget, minimális késleltetést és magas megbízhatóságot biztosít a szolgáltatást igénybe vevő felhasználók számára. A technológia különösen hasznos a mezőgazdaságban, a tengerészetben és a logisztikai iparágakban. A LEO alapú IoT műholdas kapcsolat fejlesztése továbbra is optimalizálja a teljesítményt és javítja a felhasználói élményt. A LEO műholdas IoT kapcsolatok várhatóan 6 millióról 22 millióra nőnek 2022 és 2027 között, 25%-os éves emelkedési ráta mellett.[453] A Huawei globális IKT vállalat elemzése szerint „*2030-ra a mobilinternet piac teljesen átalakul. A digitális és a fizikai világ mélyebben integrálódik, és szinte valós élményeket teremt [VR/AR]. A digitális gazdaság a reálgazdaság elsődleges mozgatórugója is lesz [összhangban az uniós törekvésekkel], és az ipari szegmens az eszközök hatékonyságáról a döntéshozatali hatékonyságra helyezi át a hangsúlyt [MI]. De ezek célkitűzéseknek az eléréséhez szükség lesz az első hálózatbiztonság megteremtéséhez, és az az energiahatékonyság növeléséhez, hogy a zöld növekedés révén megóvjuk a környezetet.*”[454]

A részfejezetben megállapításra került, hogy globális szinten kb. 2030-ra az 5G lakossági mobil-előfizetések átveszik a vezető szerepet a 4G-vel szemben. Összességében a mobil-előfizetések száma folyamatosan emelkedő tendenciát mutat, míg 2023-ban 8,5 Mrd előfizetést mutatnak a statisztikák, addig ez 2029-re várhatóan eléri a 9,2 Mrd-ot. Az európai régiót vizsgálva tapasztalható egy IKT piaci megosztottság a nyugat- és a közép-kelet-európai térség között, ami abban is megnyilvánul, hogy az EU-s digitalizációs törekvések a nyugat-európai országokban jobban érvényesülhetnek, mint a közép-keleti régióban. Ez a mobil előfizetések technológiai hozzáférésének tükrében azt jelenti, hogy míg 2023-ban 2-3% a lakossági 5G előfizetések számra KKE-ban, addig NYE-ban 25%. 2029-re KKE-ban kb. 50-50%-os lesz a lakossági 4G és 5G előfizetések megoszlása, míg NYE-ban az 5G 84%-os piaci részesedést fog produkálni, 15%-os 4G részesedéssel és a 2G, 3G teljes kiszorulásával a piacról. A közép-kelet-európai adatok azért lényeges Magyarország, így a hazai LI számára, mivel a fentiek alapján

[453] *State of IoT – Spring 2023. - Market Report*. IoT Analtics. 2023. Online: https://iot-analytics.com/number-connected-iot-devices/ (Letöltés ideje: 2024. február 23.)

[454] *Roads to Mobile 2030: 10 Wireless Industry Trends*. Huawei. 2021. Online: https://www.huawei.com/en/huaweitech/industry-insights/outlook/mobile-2030-10-wireless-industry-trends (Letöltés ideje: 2024. február 23.)

megállapítható az elektronikus hírközlési szolgáltatások állami jellegének eltolódása a régiós, globalizálódó jelleg irányába, melyet alátámaszt a 6G alapú, MI támogatott, integrált VHetNet elektronikus hírközlő koncepció várható megjelenése, elterjedése. Így a hírközlési LI tekintetében indokolt és szükséges legalább a régiós prognosztikus előrejelzések figyelembevétele a képességfejlesztés, -optimalizáció szempontjából, amelyek az elkövetkező 6 éves időszakban – összhangban az EU Digitalizációs Stratégiájának, a Stratégia, és a Világűrstratégia 2030-as időtávjával – a közép-kelet-európai régióban a publikus személyközi kommunikációt érintően a 4G vezető szerepét vetítik előre, az 5G exponenciális erősödése mellett. A lakossági IoT eszközök száma az előrejelzések szerint 2030-ra több mint 17 milliárdra nő. A LEO műholdas IoT kapcsolatok várhatóan 6-ról 22 millióra nőnek 2027-ig.

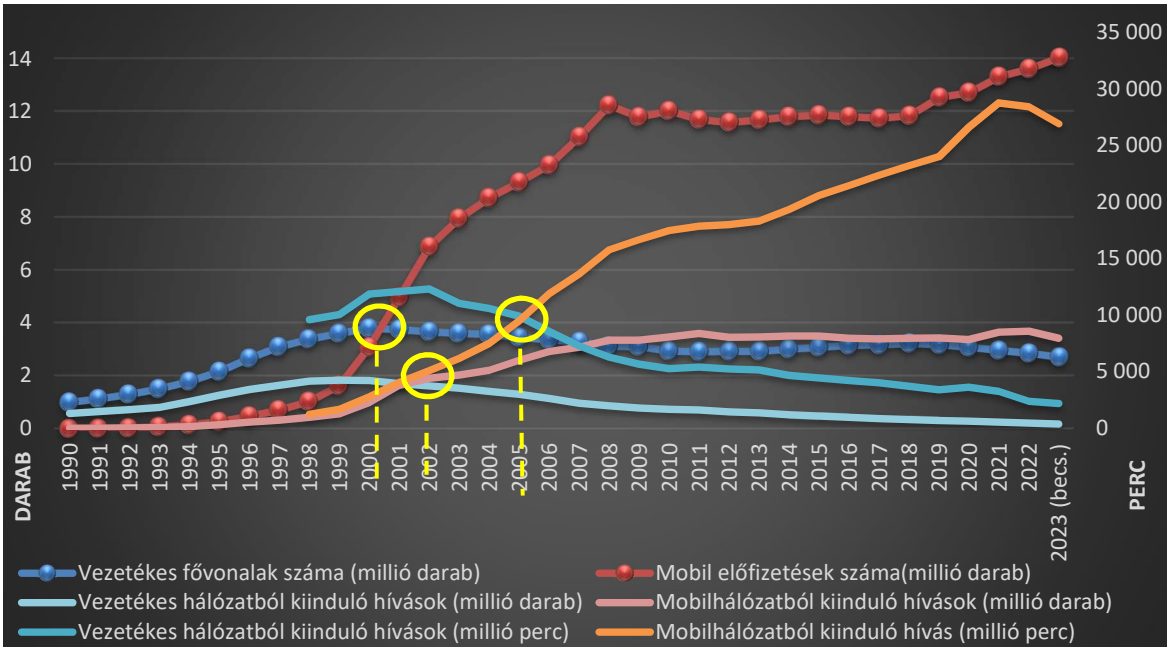
3.2.2. Hazai mobil hírközlési helyzetkép

A fenti globális és regionális, azon belül is elsősorban a közép-kelet- és nyugat-európai régiós mobil hírközlési trendelemzést követően a hazai hírközlési LI képesség fejlesztése stratégiai irányainak meghatározásához szükséges a magyarországi publikus, azaz lakossági célú mobil hírközlési trendek, tendenciák elemzése, elsősorban az NMHH és a KSH statisztikai adatai alapján. A részfejezetben elsősorban a nyilvános releváns statisztikai adatok alapján összeállított saját készítésű komplex grafikonokkal és az azokból levonható következtetésekkel kívánom szemléltetni a fejlődés tendenciális folyamatait az egyes alábbi trendtípusok tekintetében:

- vezetékes telefon fővonalak és mobil előfizetések számának hazai alakulása;
- vezetékes és mobil hálózatból kiinduló hívások számának hazai alakulása;
- vezetékes és mobil hálózatból kiinduló hívások időtartamának hazai alakulása.

Ezt követően szemléltetni kívánom a belföldi mobilinternet forgalom, majd mobilinternetre csatlakozott mobiltelefonok és táblagépek megoszlásának alakulását hálózat típusonként (2G, 3G, 4G, 5G). Meg kívánom vizsgálni a mobilinternet fogalom hazai alakulását, annak 2006-os indulásától kezdődően. Egy komplex szemléltető ábrán kívánom bemutatni az indított mobil hívás-, küldött SMS és mobilinternet fogalom hazai alakulását. Végezetül pedig az internetforgalmat bonyolított okostelefonos SIM-kártyák számának és fajlagos forgalmának tendenciáit kívánom elemezni, a rendelkezésre álló statisztikai adatok alapján.

A 20. ábra alapján következtetések vonhatóak le a vezetékes telefon fővonalak és a mobil előfizetések számának alakulásáról, a vezetékes és a mobiltelefon hálózatból kiinduló hívások számának összehasonlításáról, valamint a vezetékes és a mobil hálózatból kiinduló hívások időtartamáról. Továbbá összehasonlítható mind a vezetékes, mind a mobil hálózatból kiinduló hívások számának és időtartamának alakulása a vizsgált időszakban.



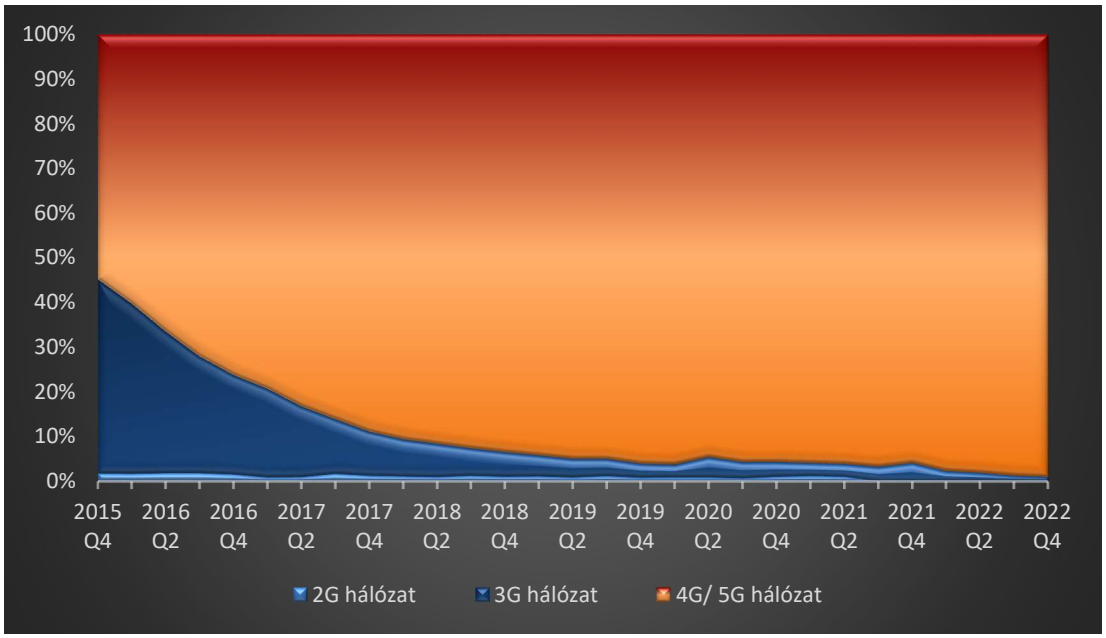
20. ábra: Vezetékes és mobil előfizetések/ kiinduló hívások számának/ időtartamának hazai összesített alakulása 1990-2023 között (Szerk.: A szerző[455])

A vezetékes telefon fővonalak és a mobil elfizetések számának alakulása kapcsán megállapítható, hogy kb. a 2000-es évtől kezdődően a mobilszolgáltatás vette át a vezető szerepet, mely azóta exponenciális ütemben nő, a vezetéke szolgáltatás csökkenése, stagnálása

[455] *12.1.1.2. A távközlés (vezetékes, mobil) fontosabb adatai.* KSH. 2023.
Online: https://www.ksh.hu/stadat_files/ikt/hu/ikt0002.html (Letöltés ideje: 2023. július 29.);
12.1.1.5. A mobil-előfizetések száma és a mobilhálózatból kiinduló hívások száma és időtartama, adatforgalma. KSH. 2023.
Online: https://www.ksh.hu/stadat_files/ikt/hu/ikt0005.html (Letöltés ideje: 2023. július 29.);
12.2.1.2. Bekapcsolt vezetékes telefon fővonalak és hívások száma negyedévente. KSH. 2024.
Online: https://www.ksh.hu/stadat_files/ikt/hu/ikt0030.html (Letöltés ideje: 2024. február 23.);
12.2.1.4. Mobil-előfizetések és hívások száma, mobil adatforgalom negyedévente. KSH. 2024.
Online: https://www.ksh.hu/stadat_files/ikt/hu/ikt0032.html (Letöltés ideje: 2024. február 23.);
A mobilpiaci jelentés adattáblái – 2023. II. negyedév. NMHH. 2024.
Online: https://nmhh.hu/dokumentum/243792/mobilpiaci_jelentes_adattablak_2023_ii_negyedev.xlsx (Letöltés ideje: 2023. július 29.);
Mobil rádiótelefon-hívások jellemzői: Hívások időtartama (1990-2001). NMHH: EHMMSA. 2023.
Online: http://ehmmsa.nmhh.hu/mobil-tavkozlesi-szolgaltatas/3-02/006/#3-02 (Letöltés ideje: 2023. július 29.)

mellett. A vezetékes fővonalak száma 2000-ben volt a legmagasabb, míg a mobil előfizetések száma 2023-ban a növekvő tendencia miatt kb. 3,5-szerese lett a legmagasabb fővonal számnak. A vezetékes és a mobiltelefon hálózatból kiinduló hívások számának alakulása kapcsán megállapítható, hogy kb. a 2001-es évtől kezdődően a mobilszolgáltatás vette át a vezető szerepet, mely azóta nőt, majd 2009-től stagnál, a vezetékes szolgáltatás lassú csökkenése mellett. A vezetékes hívások száma 1999-ben volt a legmagasabb, míg a mobil hívások száma 2023-ban a növekvő tendencia miatt kb. 2-szerese lett a legmagasabb vonalas hívásszámnak. A vezetékes és a mobiltelefon hálózatból kiinduló hívások időtartamának alakulása kapcsán megállapítható, hogy kb. a 2005-ös évtől kezdődően a mobilszolgáltatás vette át a vezető szerepet, mely azóta folyamatosan nőtt, majd 2009-től csökkeni kezdett, a vezetékes szolgáltatás stabil csökkenése mellett. A vezetékes hívások időtartama 2002-ben volt a legmagasabb, míg a mobil hívások időtartama 2021-ben a növekvő tendencia miatt kb. 2-szerese lett a legmagasabb vonalas időtartamnak. A mobil hívások időtartama 2021 után csökkeni kezdett. A vezetékes hálózatból kiinduló hívások számának és időtartamának alakulása kapcsán megállapítható, hogy azok 1999/2002-től csökkenő tendenciát mutatnak. Míg a mobil hálózaból kiinduló hívások számnak és időtartalmának alakulása kapcsán megállapítható, hogy a hívásszám ugyan 2009-től stagnál, azonban a hívások időtartama 2021-ig folyamatosan nőtt, tehát adott felhasználó lényegesen több forgalmat bonyolított mobiltelefonon, mint korábban. 2009-ben átlagosan 1 hívás átlagos 1,2 perc időtartamú volt, míg 2021-ben 1 hívás átlagos időtartama 3,4 perc volt. Ez az arány nagyjából megegyezik a vonalas telefonon bonyolított hívások számának/időtartamának 2002-es csúcsértékével.

A nemzetközi kitekintésen túl érdemes hazai viszonylatban is megvizsgálni a belföldi mobilinternet forgalom megoszlásának alakulását hálózattípusonként a 21. ábra alapján, majd a mobilinternetre csatlakozott mobiltelefonok és táblagépek alakulása hálózat típusonként a 22. ábra alapján.

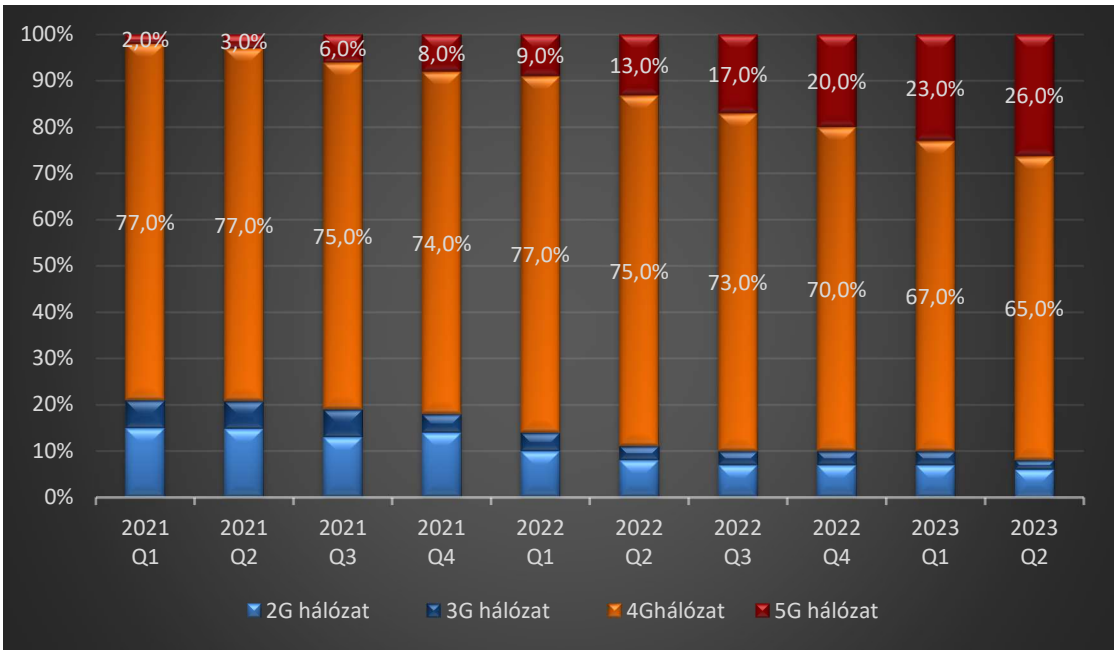


21. ábra: Belföldi mobilinternet forgalom megoszlásának alakulása hálózat típusonként 2015-2022. (Szerk.: A szerző[456])

A 21. ábra, valamint az NMHH 2022. második féléves mobilpiac jelentése alapján megállapítható, hogy „*A 4G vagy 5G képes készülékek állományának növekedése és a 4G (és 5G) hálózati lefedettség bővülése egyre több előfizető számára teszi lehetővé a mobilinternet-szolgáltatás 4G vagy 5G hálózaton történő igénybevételét. Mindez a 4G vagy 5G hálózatra (is) csatlakozott SIM-kártyák arányának 2021 végéig tartó gyakorlatilag folyamatos növekedésében is visszatükröződik. 2022-re a 3G szolgáltatások lekapcsolása és a régi készülékek lecserélődése miatt, szinte teljesen kiszorult a 4G-nél alacsonyabb szintű szolgáltatás. (A 4G használat terjedését volt hivatott segíteni az NMHH Netre fel! programja is, mely során 40.000 Ft támogatással lehetett régi készüléket 4G képes készülékre cserélni 2022-2023-ban. Közel 120.000 készülékcsere történt a pályázat keretében.)*”[457] Tehát az EU rendkívül nagy kapacitású hálózati szolgáltatások elterjesztésére vonatkozó törekvéseit az NMHH lakossági ösztönzéssel is elő kívánta segíteni. A fentiek alapján az újgenerációs mobilszolgáltatások elterjedése azonos tendenciát mutat a globális és regionális trendekkel.

[456] *A mobilpiaci jelentés adattáblái – 2022. II. félé. 22.* NMHH. 2023. 22. ábra. Online: https://nmhh.hu/cikk/238782/A_mobilpiaci_jelentes_adattablai__2022_II_felev (Letöltés ideje: 2023. július 29.)

[457] *Az NMHH mobilpiaci jelentése - 2022. II. félév.* NMHH. 2023: 26



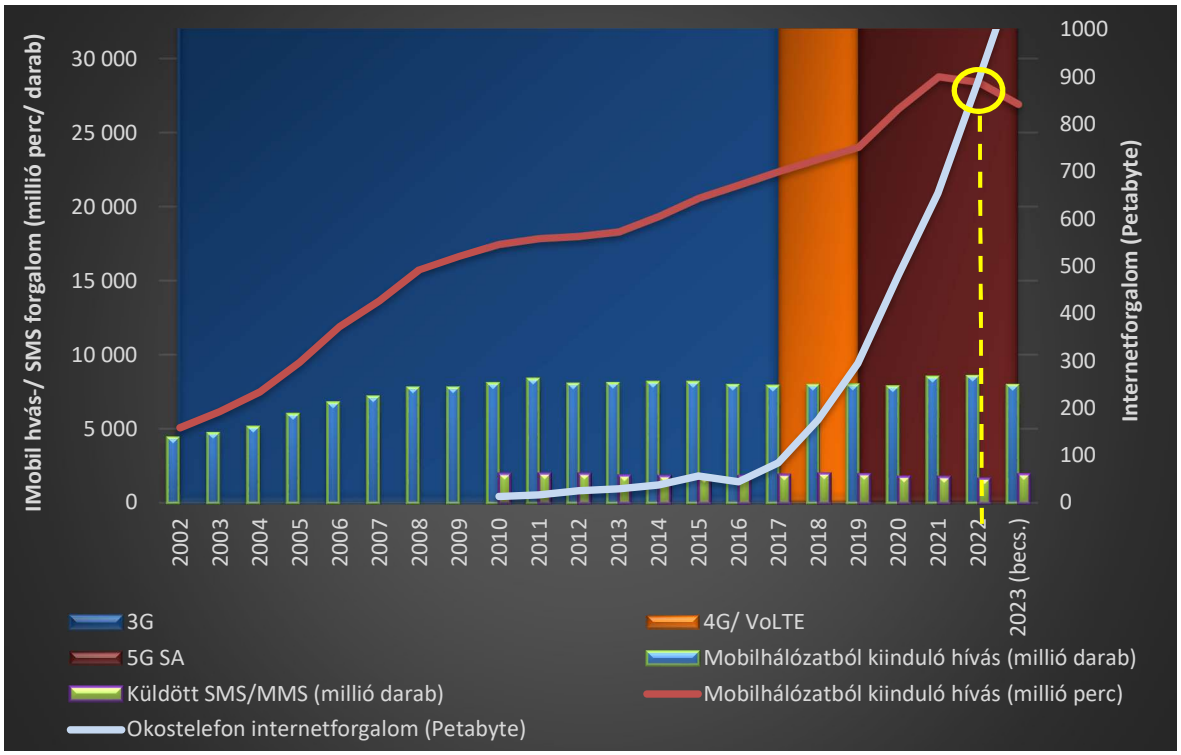
22. ábra: Mobilinternetre csatlakozott mobiltelefonok és táblagépek alakulása hálózat típusonként 2021.Q1. – 2023.Q2. (Szerk.: A szerző[458])

A 22. ábra, valamint az NMHH 2022. második féléves mobilpiac jelentése alapján megállapítható, hogy „*A 4G és 5G képes készülékek arányának növekedése és a megfelelő hálózatok folyamatos fejlesztése lehetővé tette a mobilszolgáltatók számára, hogy a forgalom egyre jelentősebb részét tereljék a 4G vagy 5G hálózatokra. Ennek következtében 2018 elejére a korábbi dinamikus növekedés következtében az adatforgalomnak már 91 százaléka 4G vagy 5G hálózaton zajlott.*”[459] A 22. ábra, valamint az NMHH 2023. második negyedéves mobilpiac jelentése alapján megállapítható, hogy „*A magyar mobilinternet-hálózatra csatlakozó, közel 12 millió darab mobiltelefon és táblagép 91 százaléka lehet képes a napjainkban elfogadható felhasználói élményt lehetővé tevő negyedik (4G) vagy ötödik generációs (5G) mobilinternet használatára. 2021 és 2023 között jelentősen lecsökkent azon készülékek aránya, melyek csak az ennél alacsonyabb szintű hálózatra képesek csatlakozni, de még így is körülbelül 1 millió ilyen eszközről beszélhetünk. [..]. Míg a 4G alatti szabványokkal működő készülékek aránya lecsökkent, az 5G képeseké 2 százalékról 26 százalékra emelkedett.*”[460] A regionális 5G trendeket vizsgálva azonban megállapítható, hogy 2023-ban Magyarország jócskán

[458] *A mobilpiaci jelentés adattáblái – 2023. II. negyedév.* NMHH. 2024: 28. ábra
[459] *Az NMHH mobilpiaci jelentése - 2022. II. félév.* NMHH. 2023: 27
[460] *Az NMHH mobilpiaci jelentése - 2023. II. negyedév.* NMHH. 2024. 27. Online: https://nmhh.hu/dokumentum/243790/nmhh_mobilpiaci_jelentes_2023_ii_negyedev.pdf (Letöltés ideje: 2024. február 24.)

túlszárnyalta a KKE átlagot. Míg KKE kb 2,5%-os 5G mobil előfizetési értéket produkált, addig Magyarországon 2023 második negyedévben ez az érték 26% volt, a 4G 65%-os dominanciája mellett.

A 23. ábra alapján össze kívánom vetni az indított mobil hívásforgalom, a küldött SMS és mobil (okostelefon) internetfogalom hazai alakulását.



23. ábra: Indított mobil hívás-, küldött SMS és mobil (okostelefon) internetforgalom hazai alakulása 2002-2023 között (Szerk.: A szerző[461])

A 23. ábrán is látható a 20. ábra szerinti következtetés, miszerint a mobil hívásszám ugyan 2009-től stagnál, azonban a hívások időtartama 2021-ig folyamatosan nőtt, tehát adott felhasználó lényegesen több forgalmat bonyolított mobiltelefonon. A mobil hívások stagnáló

[461] *Távközlés, internet, 2015. IV. negyedév*. KSH. 2016.
Online: https://www.ksh.hu/docs/hun/xftp/gyor/tav/tav21412.pdf (Letöltés ideje: 2023. július 29.);
12.1.1.2. A távközlés (vezetékes, mobil) fontosabb adatai. KSH. 2023.;
12.1.1.5. A mobil-előfizetések száma és a mobilhálózatból kiinduló hívások száma és időtartama, adatforgalma. KSH. 2023.;
12.2.1.2. Bekapcsolt vezetékes telefon fővonalak és hívások száma negyedévente. KSH. 2024.;
12.2.1.4. Mobil-előfizetések és hívások száma, mobil adatforgalom negyedévente. KSH. 2024.;
A mobilpiaci jelentés adattáblái – 2022. II. félé. NMHH. 2023.
Mobil rádiótelefon-hívások jellemzői: Hívások időtartama (1990-2001). NMHH: EHMMSA. 2023.

szintjével azonos tendenciát mutat az SMS-ek száma is. Azonban a mobil adatforgalom 2016-ot követően egy rendkívül dinamikus exponenciális növekedést produkál összhangban a nemzetközi trendekkel, 2016 és 2023 második negyedéve között, mintegy 25-szörösére növelve az értékét, mely láthatóan összefügg a 4G szolgáltatás magyarországi bevezetésének időpontjával. Tehát az újgenerációs mobilhálózatok egyfajta IKT boom-ot okoztak hazai viszonylatban a kereslet kielégítése során.

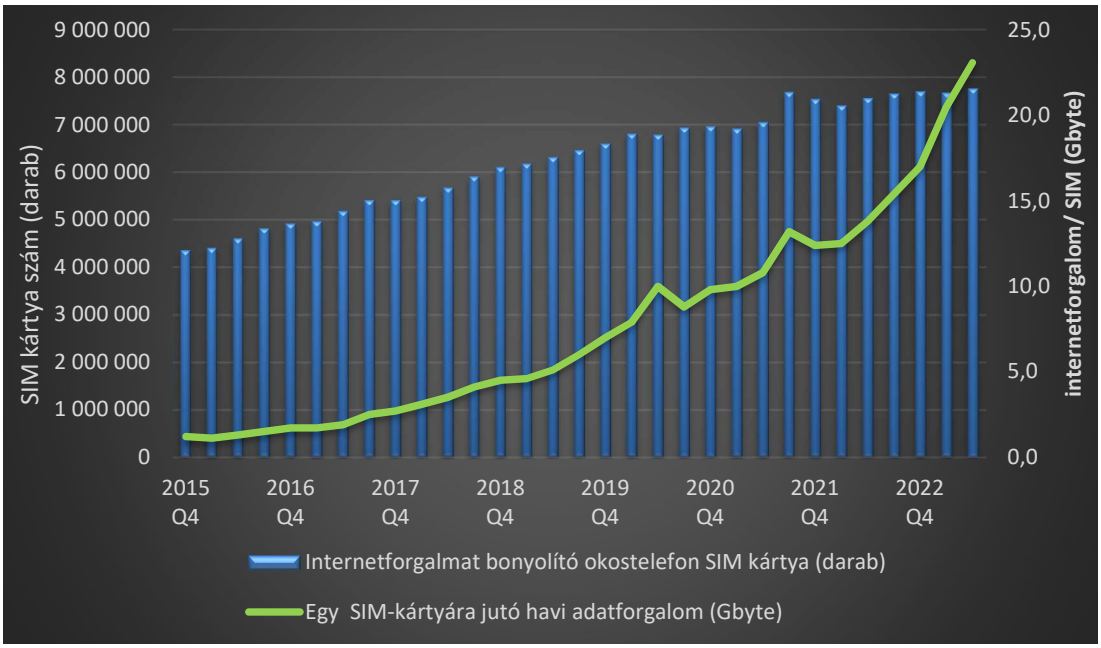
Az NMHH 2022. második féléve mobilpiac jelentése jelentés szerint: *„Az összes (nem M2M) mobilinternet-forgalom a vizsgált négyéves időszakban nagy ütemben, évente átlagosan 35 százalékkal növekedett, 2022 második negyedévében 246 millió GByte-ot tett ki. Mindez az okostelefonok terjedésével, a nagy adatmennyiséget tartalmazó, vagy bizonyos forgalomtípusokat (pl. cset szolgáltatásokat, közösségi oldalak elérését) korlátlanul engedő díjcsomagokkal, a streamelt média fogyasztásával, az online videotelefonálás növekvő használatával magyarázhatjuk.*”[462] Tehát az NMHH megállapítása alapján a titkosított online kommunikációt biztosító alkalmazásszolgáltatások keresletének fejlődésével magyarázza többek között a hazai mobilinternetes adatfogalom drasztikus megnövekedését a 2022 év végi időszaktól, mely releváns az értekezés LI szempontú vizsgálata szempontjából. A KSH legfrissebb statisztikai adatai alapján 2022.Q1. és 2023.Q1. között „*A mobiladat-forgalom több mint ötödével bővült egy év alatt. A helyhez kötött interneten keresztüli letöltési forgalom 17%-kal nőtt az előző év azonos időszakához képest.*”[463] Továbbá a KSH 2023.Q2-es megállapításai alapján „*A mobiladat-forgalom több mint negyedével bővült egy év alatt. Egy internetelérést biztosító mobil-előfizetésre átlagosan 31 Gbyte adatforgalom jutott.*”[464] Tehát a mobil adatfogalom 2023-ban is dinamikusan bővült.

Ezen hazai piaci trendnek egyedi SIM kártyákra történő levetítését, azaz az internetforgalmat bonyolított okostelefonos SIM-kártyák számának és fajlagos adatforgalmának alakulását az alábbi 24. ábra hivatott szemléltetni.

[462] *Az NMHH mobilpiaci jelentése – 2022. I. félév*. NMHH. 2023: 5-6

[463] *Internetszolgáltatás, 2023. I. negyedév*. KSH. Online: https://www.ksh.hu/infografika/2023/internet_infografika_20231.pdf (Letöltés ideje: 2024. február 24.)

[464] *Internetszolgáltatás, 2023. III. negyedév*. KSH. Online: https://www.ksh.hu/infografika/2023/internet_infografika_20233.pdf (Letöltés ideje: 2024. február 24.)



24. ábra: Internetforgalmat bonyolított okostelefonos SIM-kártyák számának és fajlagos forgalmának alakulása 2016-2023 (Szerk.: A szerző[465])

A 24. ábra, valamint az NMHH 2022. második féléves mobilpiac jelentése alapján megállapítható, hogy „*Az okostelefonos szegmens post paid [havi díjas] előfizetéshez tartozó SIM-kártyáinak aránya a teljes vizsgált időszak alatt 81-ről 84 százalékra növekedett. A fajlagos forgalmak mindkét előfizetési típus esetében nőttek a vizsgált időszakban. Post paid esetben a növekedés jelentős és egyenletes, évente átlagosan 44 százalék volt, 2022 negyedik negyedévére egy post paid SIM-kártya már átlagosan 12 GByte mobiladat-forgalmat bonyolított. […] kiszámítható, hogy 2022 negyedik negyedévében az okostelefonos szegmens teljes internetforgalmának 93 százalékát bonyolították le post paid előfizetésekről.”*[466] Az NMHH legfrissebb mobilpiac jelentése és a 24. ábra alapján megállapítható, hogy továbbra is a lakossági „havidíjas” előfizetésű felhasználók a legaktívabb felhasználók a mobil adatforgalom tekintetében, a lakossági „havidíjas” előfizetésű mobilinternetes adatforgalom 31%-os volt 2023 első félévében. „*Ennek az lehet az oka, hogy a leginkább adatigényes tevékenységek szabadidős jellegűek (pl. a közösségi oldalak videóinak nézése vagy a játék), mintsem a munkához köthető tevékenységek. Egy mobilinternetet forgalmazó lakossági*

[465] *Az NMHH mobilpiaci jelentése - 2018. II. félév.* NMHH. 2019. Online: https://nmhh.hu/dokumentum/203075/NMHH_mobilpiaci_jelentes_2015Q42018Q4.pdf (Letöltés ideje: 2024. július 15.);
A mobilpiaci jelentés adattáblái – 2022. II. félév. NMHH. 2023.;
A mobilpiaci jelentés adattáblái – 2023. II. negyedév. NMHH. 2024.

[466] *Az NMHH mobilpiaci jelentése - 2022. II. félév.* NMHH. 2023: 22

postpaid SIM-kártyával átlagosan havi 16 gigabájtot forgalmaztak […]."[467] Az NMHH jelentése alapaján az egyes magas adatforgalomigényű szórakoztató, mobilkommunikációs alkalmazásokhoz köthető a mobilinternet szegmens bővülése. A KSH adatai alapján kissé visszatekintve 2020-ban az EU-t összevetve a hazai IKT szegmenssel megállapítható, hogy lakosság kb. 68%-a bonyolított hang, vagy videóhívást mobilinterneten keresztül, míg az uniós átlag 60% volt, a közösségi oldalak használatában az arány 74%:56% volt Magyarország és az EU-s átlag között. [468] Ez nem is meglepő, hiszen „*napjainkban ugyanis markánsan megjelenik a technológiák konvergenciája, összeolvadása, amit az eszközöknél és az azokkal igénybe vett szolgáltatásoknál egyaránt megfigyelhetünk. Az eszközök esetében láthatjuk, hogy ma már egy kisméretű okostelefon biztosítja a hang- és adatkommunikációt, valamint szinte az összes, korábban dedikált számítógéppel ellátott funkciót.*"[469]

A részfejezet következtetésként megállapítható hazai viszonylatban mind a mobilszolgáltatás elfőzetői számában, az indított hívások számában és a hívások időtartalmában is 2000/2005-ös időszaktól kezdődően napjainkra fokozatosan kiszorították a helyhez kötött vonalas telefónia szolgáltatásokat. A mobil hívások stagnáló szintjével azonos tendenciát mutat az SMS-ek száma is. Azonban a mobil adatforgalom 2016-ot követően egy rendkívül dinamikus exponenciális növekedést produkált összhangban a nemzetközi trendekkel, 2016 és 2023 második negyedéve között, mintegy 25-szörösére növelve az értékét, mely láthatóan összefügg a 4G szolgáltatás magyarországi bevezetésének időpontjával. A tendenciaelemzés során megállapításra került, hogy az újgenerációs mobilszolgáltatások elterjedése elsősorban a 4G és 5G azonos tendenciát mutat a globális és regionális trendekkel. A regionális 5G trendeket vizsgálva azonban megállapítható, hogy 2023-ban Magyarország jócskán túlszárnyalta a közép-kelet-európai átlagot, hiszen míg a vizsgált régió kb. 2,5%-os 5G mobil előfizetési értéket produkált, addig Magyarországon 2023 második negyedévében ez az érték 26% volt, a 4G 65%-os dominanciája mellett. Tehát az újgenerációs mobilhálózatok egyfajta IKT boom-ot okoztak hazai viszonylatban a kereslet kielégítése során. A mobil hívások időtartama 2021-ig a növekvő tendenciát mutatott, mely ezután csökkeni kezdett. Ezt a vizsgált trendek és

[467] *Az NMHH mobilpiaci jelentése - 2023. II. negyedév*. NMHH. 2024. 21

[468] E*gyre jobban terjed az internethasználat hazánkban*. KSH. 2021. Online: https://www.ksh.hu/infografika/2021/internethasznalat_2021.pdf (Letöltés ideje: 2023. július 29.)

[469] KOVÁCS Zoltán (2020): Bűnügyi technikai hírszerzés – A mobilhírközlő hálózatok törvényes ellenőrzésének jövője. In RUZSONYI Péter (szerk.): *Közbiztonság: Fenntartható biztonság és társadalmi környezet tanulmányok III*. Budapest: Ludovika Kiadó. 907. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16197/TKP_Kozbiztonsag.pdf#page=900;jsessionid=F91F1F5C208E65004CE571CB742794DB?sequence=1 (Letöltés ideje: 2024. február 25.)

elemzések alapján egyértelműen a titkosított kommunikációt biztosító alkalmazásszolgáltatások térnyerése okozza, melyet mind a teljes hazai mobilinternet piacra kivetített adatforgalom, mind az egy SIM kártyára jutó fajlagos mobilinternetes adatforgalom exponenciális növekedése alátámaszt. Az NMHH vonatkozó jelentése alapján is az egyes magas adatforgalomigényű szórakoztató, mobilkommunikációs alkalmazásokhoz köthető a mobilinternet szegmens bővülése. A KSH adatai alapján kissé visszatekintve 2020-ban az EU-t összevetve a hazai IKT szegmenssel megállapítható, hogy a mobilinterneten bonyolított hang- és videóhívások tekintetében megelőzte Magyarország az uniós átlagot. A mobilinternet térnyerésével, így a kommunikáció „internetalapúságával" kapcsolatos trendek az LI szempontjából is kiemelten lényegesek, így az értekezés vizsgálatának szempontjából is mérvadók, elsősorban a hírközlési LI szempontjából.

3.3. A hazai hírközlési LI normatív, szervezeti, technológiai evolúciója, trendjei

Jelen alfejezet a hazai hírközlési LI normatív, szervezeti, technológiai evolúcióját hivatott vizsgálni az Eht. 2004-es hatálybalépését követően, majd LI jellegű következtetéseket kíván levonni a 3.1. és a 3.2. alfejezetekben feltárt technológiai, felhasználói trendek vonatkozásában, erősen építve a 2. fejezet következtetéseire. A tárgykör evolúcióját, várhatóságait már csak a GDPR (26) preambulumbekezdésében foglaltak alapján is indokolt vizsgálni, miszerint „*Az elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatóknak olyan megfelelő eljárásokat kell biztosítaniuk, amelyek lehetővé teszik az illetékes hatóságok jogos [LI célú] kéréseinek teljesítését.*"

3.3.1. Az Eht. hatálybalépésétől a napjainkig

A hazai elektronikus hírközlés ágazat általános törvényi szintű szabályozását ma is a 2004. január 01-jén hatályba lépett Eht. alkotja, amely előzményeihez nemzetközi és hazai jogalkotási, technológiafejlődési, és piacszervezési folyamatok is hozzájárultak. A sikeres piaci liberalizációt követően az EU-ban szabályozási törekvésként jelent meg a hírközlés és infokommunikációs szolgáltatás előre tekintő, a dinamikus technológiai fejlődés kihívásaira megfelelő válaszokat adó, és a piaci verseny élénkítésének szabályozást elősegítő, időtálló normarendszer megteremtése. Ennek egyik alapja a 2003 októberében hatályba lépett elektronikus hírközlési adatvédelmi irányelv, amely egyben a GDPR elektronikus hírközlési adatkezelés végrehajtási rendeleteként is tekinthető. Az Eht. hazai fő elősegítője nem volt más,

mint a jogalkalmazói tapasztalatok, hiszen a hírközlési és a postai szolgáltatások egy joganyagban történő szabályozása nem váltotta be a hozzá fűzött reményeket. Az elektronikus hírközlés az IKT környezet fejlődése okán a postai szolgáltatásoktól eltérően, előrelátó szemléletű normarendszert követelt meg, amely végül az Eht.-ben testesült meg.

Az Eht. szigorította és részletezte a szolgáltatói együttműködési kötelezettséget a titkos információgyűjtő eszközök, módszerek, így az LI szempontjából az arra jogosult szervekkel. Az Eht. 76. § (1) bek. alapján az elektronikus hírközlési szolgáltatás nyújtásának megkezdésére irányuló szándékot, valamint a megkezdés tervezett időpontját a szolgáltatónak nyilvántartásba vétel céljából be kell jelentenie az NMHH-nál, ami az Eht. 76. § (8) bek. alapján értesíti az NBSZ-t. Az Eht. 92. § (1) bek. kimondja a hírközlési szolgáltatói együttműködési kötelezettséget a titkos információgyűjtés folytatására jogosult szervekkel, valamint, hogy szolgáltatásnyújtás során nem lehetetlenítheti el azt. Az Eht. 92.§ (2) bek. együttműködési megállapodási kötelezettséget ír elő a szolgáltató számára az NBSZ-szel titkos információgyűjtő tevékenység, azazon belül is az LI vonatkozásában, a 92. § (3) bek. alapján a szolgáltatónak kötelezettsége minden olyan működésből, szolgáltatásnyújtásból adódó változást az NBSZ irányába bejelenteni, ami befolyásolja a titkos információgyűjtés biztosítását. Az Eht. 92. § (4) bek. alapján a szolgáltató „*a szolgáltatás megkezdésével egyidejűleg az általa használt, működtetett berendezések, helyiségek és az együttműködő személyek tekintetében – külön jogszabályban meghatározottak szerint – köteles biztosítani az elektronikus hírközlő hálózatban továbbított küldemények, közlések, továbbá a szolgáltató által kezelt adatok titkos információgyűjtéssel, illetve leplezett eszközök alkalmazásával történő megismeréséhez szükséges eszközök és módszerek alkalmazási feltételeit.”*– azaz az LI-t. Ennek érdekében az Eht. 92. § (5) bek. kimondja, hogy a hírközlési szolgáltató az LI biztosítása érdekében saját erőforrásból, finanszírozásból az NBSZ által meghatározott – vélhetően szabványosított – műszaki követelmények alapján alapkiépítésű monitoring alrendszer kialakítására kötelezett, a kezdeményezésétől számított 6 hónapon belül – azaz hálózati oldalon megvalósuló technikai passzív LI képesség (DPI) kialakításának kötelezettségét írja elő az Eht. A korábban már említett, például a 3GPP vagy az ETSI által kiadott mobilkommunikációs LI szabványok ezen rendelkezés vonatkozásában nyerik el gyakorlati jelentőségüket, hiszen transzparens, nyíltan hozzáférhető műszaki követelményként támaszthatóak. A kísérő adatokhoz való nemzetbiztonsági célú hozzáférés, azaz az alapjogi garanciáknak megfelelő, egyedi kérelmen alapuló adatszolgáltatás érdekében az Eht. 92. § (6) bek. szintén az NBSZ által meghatározott műszaki követelmények szerinti, közvetlen elektronikus adatkapcsolat útján

megvalósuló rendszer kialakításának követelményét határozza meg a szolgáltató számára. Az Eht. 48. § szerinti új eleme az NMHH általi bírság alapú szankció az elektronikus hírközlési szolgáltatóval szemben együttműködési kötelezettségének megsértése esetén.

Az Eht.-ben az egyidejű ellenőrzés alá vonható azonosítók számának kimutatható növekedése is megfigyelhető a monitoring alrendszer tekintetében, az Eht.-t megelőzően hatályos hírközlésről szóló 2001. évi XL. törvényt (a továbbiakban: Hkt.) 110. § 2. pontja szerinti 2 sávos és alacsonyabb százalékos besorolási osztályozásához képest. Az Eht. 188. § 1. pontja szerinti alapkiépítésű monitoring alrendszernek lehetővé kell tennie az elektronikus hírközlési szolgáltató előfizetői, illetve felhasználói köréből tetszőlegesen kiválasztható, az előfizetők (felhasználók) összlétszámának legalább 0,1–0,6%-át kitevő; de

- 150 000 előfizetői létszám alatt 0,6%, de legalább 60;
- 150 000–1 000 000 előfizetői létszám között 0,3%, de legalább 900;
- 1 000 000 előfizetői létszám felett 0,1%, de legalább 3000

előfizető vagy felhasználó kommunikációjának egyidejű ellenőrizhetőségét és azok kísérőadatainak késedelem nélküli, teljes körű, folyamatos, egyidejű kiválasztását és kiadását a kilépési pontra. Tapasztalható, hogy a jogalkotó előrelátó szemlélete miként tükröződik a jogszabályban az előfizetői szám várható növekedésének tekintetében. Az Eht. hatálybalépést követő évben, azaz 2005-ben az NMHH statisztikai adatai alapján 9.320.000 darab[470] mobiltelefon előfizetést produkált a hazai piac, míg helyhez kötött internetelőfizetés vonatkozásában 1.000.737 darab[471] előfizetésről beszélhetünk. Tehát a fentiek alapján megállapítható, hogy az LI végzésére jogosult szervezet által üzemeltetett közleményellenőrző rendszernek 2004-ben az Eht. 188. § 1. pont alapján a jogalkotó a Hkt. LI kapacitás maximalizáló, „-tól/-ig” szemléletével ellentétben már egzakt százalékos értékeket azonosít, optimalizálva azt az előfizetők, felhasználók várható bővüléséhez. Megállapítható, hogy a Hkt. szerinti szabályozás kapacitási szempontból túlzónak és a túl tágnak bizonyult, így az Eht.-ben jogállamiási, költség/hatékonysági és alkalmazhatósági szempontból optimalizálásra, egzakt meghatározásra került az egyidejű ellenőrzés alá vonható előfizetők mennyisége, mely a jogalkalmazást is elősegítette.

[470] *Mobil rádiótelefon szolgáltatás (1990-2008)*. NMH EHMMSA. 2009. Online: http://ehmmsa.nmhh.hu/mobil-tavkozlesi-szolgaltatas/3-04/001,002,003,004,005,a/#3-04 (Letöltés ideje: 2023. július 29.)

[471] *Internet-előfizetések száma hozzáférés szerint, az év végén (1999-2020)*. NMHH EHMMSA. 2021. Online: http://ehmmsa.nmhh.hu/informatika-internet/6-02/013,001,002,003,006,008,014,009,007,015,010,a/#6-02 (Letöltés ideje: 2023. július 29.)

Az elektronikus hírközlési szolgáltató LI jellegű együttműködési kötelezettségének részletszabályait az Nbtv., az Eht., és a Be. felhatalmazórendelkezési alapján a 180/2004. (V.26.) Korm. rend. szabályozza. Rendelkezései közül kiemelendő a 5. § (1) bek., amely szerint az adatszolgáltatást a jogosult szerv vagy az NBSZ igénybevételével, vagy közvetlenül hajtja végre a szolgáltató irányába. Azonban a 6. § (1) bek. alapján „*Amennyiben az elektronikus hírközlő hálózaton folytatott kommunikáció tartalma és a kísérőadatok megismeréséhez az igazságügyért felelős miniszter vagy bíró engedélye szükséges, a titkos információgyűjtésre felhatalmazott szervezetek igényeinek kielégítését - külön törvényben meghatározott feltételek mellett - az NBSZ látja el*.” Tehát a tartalomellenőrzésre irányuló LI-t, illetve az olyan esetet amikor a kísérőadathozzáférés is külső engedélyezéshez kötött, mint például az Nbtv. 56. §. e) pont szerinti információs rendszeren kezelt adatra esetében, a jogalkotó az NBSZ-nél összpontosította, jogalkotási szinten megalapozva a koncentrált LI szervezeti modell érvényesülését.

A 2005-2015 közötti időszak meghatározó a hazai hírközlési szabályozás, valamint az LI szempontjából. Az Eht. által meghatározott előfizetői számlázási, kísérő, és helymeghatározási adatok kezelésére, tárolására és nemzetbiztonsági, bűnüldözési célú szolgáltatására vonatkozó szabályokat az EU 2006/24/EK irányelv[472] szerinti jogharmonizációs követelményeknek eleget téve az Eht. módosításáról szóló 2007. évi CLXXIV. törvényben implementálta a jogalkotó. Az irányelv az adatmegőrzés és szolgáltatás kérdéskörét volt hivatott szabályozni, amely egyik célja a tagállamközi bűnüldözési célú információcsere és együttműködés elősegítése volt. A 2006/24/EK irányelv (5) – (6) preambulumbekezdései alapján a bűnüldözési célú szolgáltatói adatmegőrzés tagállami szabályozásai jelentős eltéréseket mutattak egymástól, amelyek közötti jogi és technikai különbségek akadályokat jelentettek az elektronikus hírközlés belső piaca számára, mivel a szolgáltatókra eltérő követelmények vonatkoztak a megőrizendő forgalmi és helymeghatározó adatok típusait, valamint a megőrzés feltételeit és idejét illetően. A szabályozás egységesítésének indokoltsága a 2006/24/EK irányelv (10) preambulumbekezdése alapján a Londont ért terrortámadásokkal kapcsolatban feltárt hiányosságok okán is fennállt. A 2006/24/EK irányelv adatmegőrzési kötelezettsége az Eht. 159/A. § bek. szerint a „*helyhez kötött telefon- vagy mobil rádiótelefon szolgáltatás, internet hozzáférési szolgáltatás, internetes telefon-, internetes levelezési szolgáltatás*”-okra terjed ki. Az implementálást követően az

[472] Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról. L 105/54 13.4.2006

utóbbi 2 tevékenység csak abban az esetben tartozik az Eht. hatálya alá, ha azt az elektronikus hírközlési szolgáltató végzi, egyéb esetben azokat elkülönült módon az Ekertv. szabályozza (alkalmazásszolgáltatás), amely a DMA és a Hírközlési Kódex alkalmazása alapján egyfelől mégiscsak az Eht. hatálya alá tartozó NI-ICS.

A 2007. évi CLXXIV. törvény módosító rendelkezéseire figyelemmel a forgalmi-, azaz a kísérő- és az előfizetői számlázási adatok tárolásának, kezelésének szabályait az Eht. 157. § rendezte, azok nemzetbiztonsági, bűnüldözési célú szolgáltatására pedig az Eht. 157. § (10) bek. alapján van kötelezettsége a szolgáltatónak. „*Azonban először az Eht.-ban jelent meg az IP-alapú szolgáltatások kapcsán az adatmegőrzési kötelezettség is. […] 2003-ban a lakosság vonatkozásában végzett felmérés megmutatja, hogy Magyarországon a háztartások 12%-a*[473] *rendelkezett internetelléréssel, az oktatási intézményekben jóval magasabb számot mértek.”*[474] Internet hálózat esetén ilyen adat például az IP cím, portszám, egyéb azonosítók. Az Eht. az IMEI[475] mellett további mobil azonosítókat is definiál és velük kapcsolatban nemzetbiztonsági, bűnüldözési célú adatszolgáltatási kötelezettséget írt elő, mit például az IMSI tekintetében. A szolgáltatók nemzetbiztonsági, bűnüldözési és honvédelmi célú adatmegőrzési és -szolgáltatási kötelezettségét az Eht. 159/A. § (1) bek. rendezte és 1 éves adattárolási időt ír elő a sikeres hívások tekintetében, a módosítást megelőző 3 évvel szemben. A helymeghatározási adatok[476] szolgáltatásával kapcsolatos kötelezettséget az Eht. 2011 majd 2015 évi módosításával[477] rendezte a jogalkotó. A 2015-ös módosítást követően az Eht. 156. § (18) bek. alapján „*az elektronikus hírközlési szolgáltató a (16)–(17) bekezdés szerinti helymeghatározási adatok szolgáltatását a hálózatában, a Nemzetbiztonsági Szakszolgálat által meghatározott követelményrendszer szerint rendelkezésre álló helymeghatározási adatoknak a Nemzetbiztonsági Szakszolgálat által előírt technikai szempontok szerinti továbbításával köteles teljesíteni*”. Tehát az Eht. 2015-ös módosítását követően az NBSZ által

[473] DESSEWFFY, Tibor (2003): *Mapping the future*. Budapest: ITTK-TÁRKI. 7. Online: www.tarki.hu/adatbank-h/kutjel/pdf/a687.pdf (Letöltés ideje: 2023. július 30.)

[474] NÉMETH Attila (2018): Az infokommunikáció szabályozási környezetének fejlődése a nemzetbiztonsági tevékenység vonatkozásában. *Szakmai Szemle*, 16(2), 60. Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2018_2_szam.pdf (Letöltés ideje: 2023. április 9.)

[475] IMEI: International Mobile Equipment Identity - nemzetközi mobil készülék azonosító

[476] Eht. 188. § 59. „*Helymeghatározási adat: a nyilvános mobilhálózatokon a hálózati infrastruktúrából vagy mobil készülékekből származó mindazon feldolgozott adat, amely meghatározza a végfelhasználó mobil végberendezésének földrajzi helyzetét, illetve nyilvános helyhez kötött hálózatokon a hálózati végpont nyilvántartásban rögzített címét.”*

[477] 2011. évi CVII. törvény az egyes elektronikus hírközlési tárgyú törvények módosításáról 51. §; 2015. évi CLXXXVIII. törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről 25. §

központosítottan, koncentráltan ellátott LI tevékenység kibővült a helymeghatározási adatok nemzetbiztonsági, bűnüldözési célú ellenőrzésével.

Eközben a mobilszolgáltatások és azok LI-jének vonatozásában is evolúciós lépések következtek be. 2006-ban a 3G-nek köszönhetően az NMHH statisztikai adatai alapján Magyarországon elkezdett emelkedni a mobilinternet előfizetések száma, 2006-ban 199.784 darab előfizetésről beszélhetünk, amely szám 2010-re elérte a 1.306.912 előfizetést[478], mely 2010-ben 14 Petabyte összesített adatforgalmat eredményezett az okostelefonok tekintetében[479]. 2006-ban 9.966.000 millió mobil előfizetést produkált a piac, míg 2010-ben már 12.012.000 darabot.[480] Az össz internetelőfizetés száma 2006-ban 1.329.625 volt, míg 2010-re elérte a 3.341.464. Az időszakban szükségessé vált az internetfogalom LI képességének kialakítása, tekintettel a mobilinternet előfizetők számának dinamikus emelkedésére.[481] Továbbá egyéb titkos információgyűjtő eszközök számára is megteremtette az Eht. a jogalapot, gondoljunk csak a helymeghatározási adatok nemzetbiztonsági célú szolgáltatására, vagy akár az IMEI/IMSI tárolási és adatszolgáltatási kötelezettségre.[482] A 2011-2016. időszakban fokozódó helyhez kötött és mobilinternet térnyerése, az azt kihasználó bűnelkövetői csoportok magatartása, és az innovatív technológiai trendek, piaci jellemzők szükségessé tették az ilyen kihívásokra is reagálni képes, integrált modern ellenőrző rendszer fejlesztését, „*Mindeközben: fokozott terrorfenyegetettség és soha nem látott mértékű illegális migráció*" jellemezte az európai, hazai biztonsági környezetet.[483] A mobiltechnológiák hazai piacán is fejlődés állt be, 2017-ben megjelent hazánkban a már IP alapú 4G mobilszolgáltatás, mely újabb kihívást jelentett a hírközlési LI számára, a növekvő adatmennyiségen, a csökkenő késeltetési időn és a bővülő sávszélességen túl, a mobilinternet hálózat egyre heterogénebb adattípusai okán. Az éppen aktuális 5G-, digitalizációs törekvések is technológiai kihívások elé

---

[478] *Internet-előfizetések száma hozzáférés szerint, az év végén (1999-2020)*. NMHH EHMMSA. 2021. http://ehmmsa.nmhh.hu/informatika-internet/6-02/013,001,002,003,006,008,014,009,007,015,010,a/#6-02 (Letöltés ideje: 2023. április 9.)

[479] *A mobilpiaci jelentés adattáblái – 2022. II. félév.* NMHH. 2023.

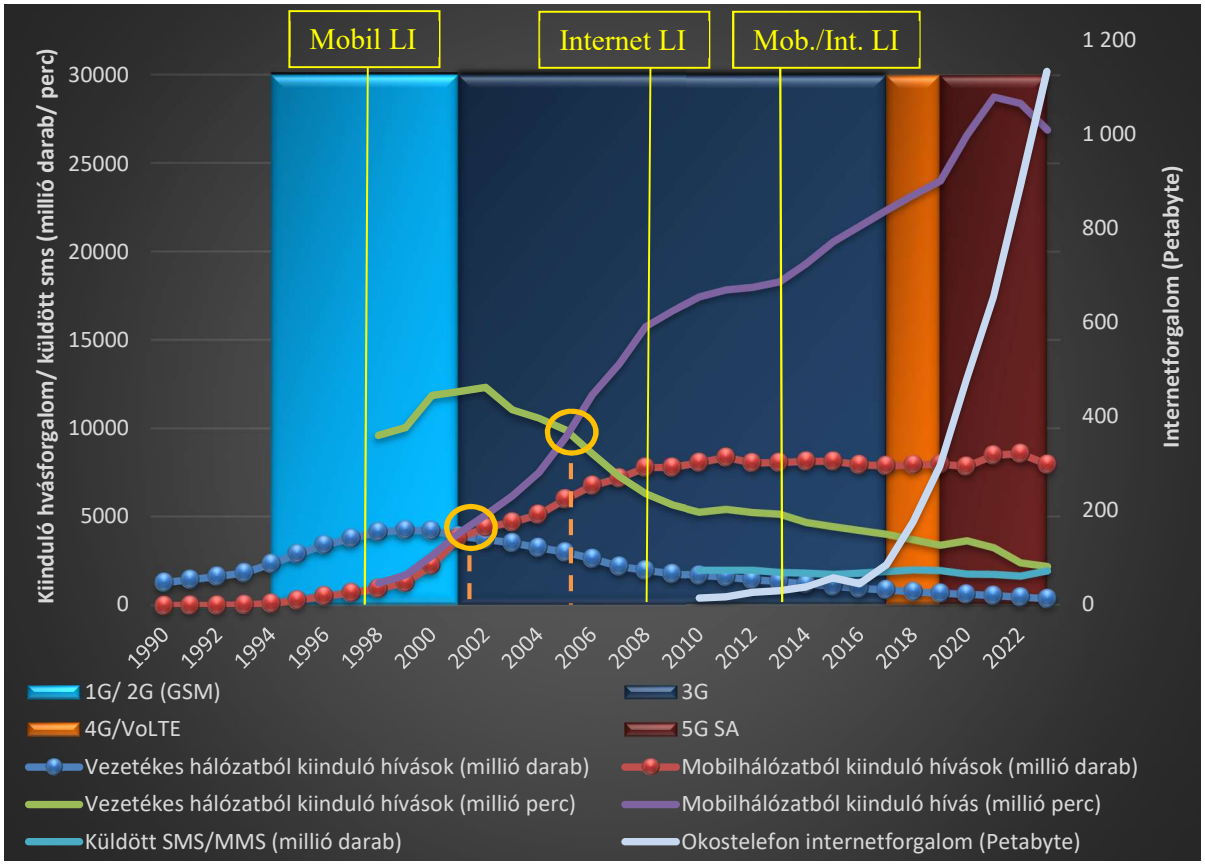
[480] *Mobiltelefon előfizetések száma (1990-2020)*. NMHH EHMMSA. 2021)

[481] *20 éves a Nemzetbiztonsági Szakszolgálat*. Budapest: NBSZ. 2016. 13.

[482] „*Fontos információ lehet az IMEI szám és a hozzá kapcsolható IMSI számok (telefonszámok) a felderítést és a nyomozást végző hatóságok számára. A célszemély (az érintett) legtöbbször úgy taktikázik, hogy cserélgeti a telefonszámait, melyet a meglévő (állandó) telefonkészülékébe helyez be. Továbbá előfordulhat, hogy a dual kártyás telefonkészülék esetén, ún. „dobós" SIM kártyát cserélget az elkövető az állandó telefonszáma mellett és a „dobós" SIM kártyán bonyolítja le a bűnös tevékenységét. A telefonlehallgatás elsősorban a felderítést teszi lehetővé, a megállapított és az ellenőrzött közlemény későbbiekben bizonyítékká válhat okirat formában*." DR. NYITRAI Endre (2014): titkos információgyűjtés és a titkos adatszerzés alkalmazása során felmerülő kérdések. *Büntetőjogi Szemle*, 4(3), 37-38. Online: https://ujbtk.hu/wp-content/uploads/2014/12/bjsz_201403_Nyitrai_Endre.pdf (Letöltés ideje: 2024. február 22.)

[483] *20 éves a Nemzetbiztonsági Szakszolgálat*. Budapest: NBSZ. 2016. 14.

állítják az LI-t, már kiegészülve a lakossági célú műholdas infrastruktúrára épülő hírközlési dimenzióváltás előszelével. A 3.2. alfejezetben és jelen alfejezetben eddig vizsgált hazai IKT és LI trendek, tendenciák komplex szemléltetésére az alábbi 25. ábra hivatott.



25. ábra: A mobil elektronikus hírközlés tendenciái és összefüggése a hazai LI evolúciójával napjainkig (Szerk.: A szerző[484])

A részfejezet következtetéseként megállapítható, hogy a hazai hírközlési ágazat evolúciójára a politikai, társadalmi, gazdasági elvárások, és az IKT környezet fejlődése egyaránt befolyással voltak, melyek így hatást gyakoroltak a technológia kritikus LI képességek hatékonyságára,

[484] *12.1.1.2. A távközlés (vezetékes, mobil) fontosabb adatai.* KSH. 2023.;
12.1.1.5. A mobil-előfizetések száma és a mobilhálózatból kiinduló hívások száma és időtartama, adatforgalma. KSH. 2023.;
12.2.1.2. Bekapcsolt vezetékes telefon fővonalak és hívások száma negyedévente. KSH. 2024.;
12.2.1.4. Mobil-előfizetések és hívások száma, mobil adatforgalom negyedévente. KSH. 2024.;
A mobilpiaci jelentés adattáblái – 2023. II. negyedév. NMHH. 2024.;
Mobil rádiótelefon-hívások jellemzői: Hívások időtartama (1990-2001). NMHH: EHMMSA. 2023.;
A mobilpiaci jelentés adattáblái – 2022. II. félé. 22. NMHH. 2023.;
Az NMHH mobilpiaci jelentése - 2023. II. negyedév. NMHH. 2024.;
Távközlés, internet, 2015. IV. negyedév. KSH. 2016. *Az NMHH mobilpiaci jelentése - 2018. II. félév.* NMHH. 2019.;
20 éves a Nemzetbiztonsági Szakszolgálat. Budapest: NBSZ. 2016:11-14

fejlődésére. A mobil hírközlési generációugrások és azok szabályozása, valamint az LI (technológia, szabályozás) összefüggéseiben megállapítást és alátámasztást nyert, hogy az IKT fejlődéshez képest a hírközlési szabályozás és az LI szabályozása követő tendenciát mutat, a képességfejlesztés pedig szintén utólagos. Azonban mind a Hkt., mind az Eht. alapján megállapítást nyert, hogy a hírközlési ágazati szabályozás a rendszerváltást követő időszakban együttesen valósult meg az LI törvényi szintű szabályozásával, azaz a hírközlési LI szerves részévé vált a hírközlési ágazatai szabályozásnak, így megvalósítva a transzparens hírközlési LI ágazati szabályozást, mely a 21. században egyfajta jogpolitikai irányvonal is egyben.

A hírközlési LI tekintetében látható, hogy a gyakorlat alakította a szabályozást annak felülvizsgálatakor, hiszen az Eht. már a hírközlési szolgáltatás előfizetői számához mérten százalékosan határozza meg a monitoring alrendszer kapacitását, így előrelátó normaalkotó, jogpolitikai szemléletmódot képviselve. A tartalomellenőrzésre irányuló hírközlési LI-t, illetve az olyan esetet amikor a kísérőadathozzáférés is külső engedélyezéshez kötött, a jogalkotó az NBSZ-nél összpontosította, kvázi jogalkotási szinten megerősítve a hazai koncentrált LI szervezeti modell működését (összhangban a 2. fejezet részkövetkeztetéseivel). Az új IKT technológiai fejlesztésekben rejlő titkos információgyűjtő lehetőségek is integrálásra kerültek a hazai szabályozásba, gondoljunk csak az egyes mobilazonosító adatok (IMEI/IMSI), helymeghatározási adatok és előfizetői számlázási adatok nemzetbiztonsági, bűnüldözési célú adatszolgáltatásának szolgáltatói kötelezettségére. Az Eht. 2015-ös módosítását követően az NBSZ által központosítottan, koncentráltan ellátott LI tevékenység kibővült a helymeghatározási adatok nemzetbiztonsági, bűnüldözési célú ellenőrzésével. Ezen a ponton szükséges azon következtetés megállapítása, miszerint az Eht. és a 180/2004. (V.26.) Korm. rendelet is az NBSZ-t jelöli ki az LI hazai koncentrált végrehajtói, és szolgáltatói szerepkörének betöltésére (a továbbiakban: hazai központi LI szerv), melyet a 3.1.1. fejezetben ismertetett elektronikus hírközlő hálózati séma szerinti, az Eht. vonatkozó rendelkezésein alapuló, vélhetően a nyilvános nemzetközi szabványok szerinti monitoring LI alrendszerrel biztosít, a jogszabályok adata további lehetőségek mellett.

Ezen túlmenően mind a hírközlés globalizációja, mind a határokon átívelő bűnözés erősödése magával hozta a nemzetközi, európai bűnüldözési célú együttműködés fokozásának, és a jogharmonizáció szükségességét az elektronikus hírközlő hálózatokon megkeletkezett fenti adatkörök tekintetében. Az Unió az EU 2006/24/EK irányelvében összehangolta szabályozást, egyben implementációs kötelezettséget is teremtve a tagállamok számára. Tehát

részkövetkeztetésként megállapítható, hogy az uniós jog hatálya alá tartozó bűnüldözési célú LI tekintetében a hírközlés globalizációja, valamint a határokon átívelő bűnözés erősödése, a 2015-től fokozódó terrorizmus és illegális migráció magával hozta az uniós jogalkotást, valamint a szorosabb együttműködést a tagállamok bűnüldöző szervei között. Azonban az értekezés szempontjából lényeges nemzetbiztonsági érdekkörben jelentkező, nemzetbiztonsági célú együttműködésre az uniós jog hatálya nem terjedhetett ki.

3.3.2. Az „IKT boom" várható hatásai az elektronikus mobil hírközlési LI-re

Jelen fejezet fenti szakma- és szabályozástörténeti, valamint az aktuális helyzetképet vizsgáló részelemzéseit követően szükséges a hírközlési LI jövőjébe tekintő következtetések levonása is a távlati hírközlési LI képesség K+F+I-jének megalapozás érdekében. A 3.1.2. részfejezetben vizsgált újgenerációs (5G, 6G) mobilhálózatok tekintetében bemutatásra került számos többletlehetőség és kihívás, mely LI aspektusú vonatkozásai jelen részfejezetben kerülnek vizsgáltra, összhangban a mobilkommunikációs trendelemzés eredményeivel, tekintettel az ember-gép-IoT digitális IKT ökoszisztémában, az okos város koncepcióban rejlő többlet LI lehetőségekre, az azok kiaknázására képes innovatív, integrált LI rendszer aspektusából.

Az 5G, 6G hálózatok elterjedésére irányuló EU-s digitalizációs törekvések alapján megállapított 2029/2030-ig előreláthatólag kitartó 5G „dömping" számos új LI lehetőséget és egyben kihívást is hordoz magában. A MiMo nyalábtechnológiának pozitív hozadéka az információgyűjtés és az LI kapcsán, hogy jóval pontosabb helymeghatározási adatokat lesz képes biztosítani, mint a jelenlegi 2G/3G/4G technológiák.[485] A legújabb 5G alapú, AR 3D technológia helymeghatározási képességének[486] nemzetbiztonsági célú LI keretében történő kiaknázása esetén lehetőség nyílik a hálózati oldalon megvalósuló helymeghatározási képesség innovációjára, már az 5G nyalábtechnológián alapuló helymeghatározási képességfejlesztésen túlmutatóan is, mely illegális migrációmegelőző-, terrormegelőző, -felderítő hozzáadott értéke szignifikáns lehet. Az e-mobilitási okos város részökoszisztéma keretében alkalmazott IRS passzív visszaverődései NOMA technológia esetében lehetőséget kínálnak a forgalmazott adatok jogosulatlan ellenőrzésére is.[487] Az IRS támadásának egyik lehetséges metódusa az „ál-

[485] ASTELY at al. 2022; KISS 2018
[486] TALVITIE, 2023: 919-934
[487] WANG at al. 2023; MOHSAN – LI 2023

IRS” felületek kihelyezése,[488] amely elvi szinten az „IMSI elfogó” szerinti ellenőrzéssel hasonlóságokat mutat. Ez a jogosult, például nemzetbiztonsági célú LI tekintetében egyben az IKT környezet fejlődéséből adódó többlet képességfejlesztési lehetőséget is teremt, például transznacionális jellegű szervezett bűnözés elleni tevékenység során.

Az egyes okos város-alkalmazások, komponensek rendkívül komplex, heterogén digitális ökoszisztémája, mind az 5G, mind a 6G technológiák tekintetében is kihívást jelent a 3.1.2. részfejezetben ismertetett IoT és ipari kommunikáció hálózati tulajdonságain túl, a lakossági célú IKT szolgáltatások igénybevételéig, így a titkosított online kommunikációt biztosító alkalmazásszolgáltatásokig. A fenti szempontok természetesen az LI rendszerek oldalán is jelentkezni fognak, így azok optimalizációja mind a kapacitás, mind az MI támogatott kiválasztás/feldolgozás kapcsán elengedhetetlen, amely érdekében a kutatások nagy lehetőséget prognosztizálnak a szemantikus, szimbólum alapú kommunikációnak[489] az egyes releváns adatfolyamok, adatcsomagok jelölése/kiválasztása kapcsán. Az 5G infrastruktúra lehetővé teszi a hálózat „szeletelését”, így a központi hírközlési hálózattól független, decentralizált hálózatok létrejöttét, melynek köszönhetően elsősorban az ipari felhasználás, az üzemek, gyárak képesek a nyilvános, publikus hálózattól és annak forgalmától teljesen független 5G hálózatot kialakítani saját működési területükön belül.[490] Ez a központi monitoring alrendszer alapú DPI LI szempontjából egy kihívás, hiszen a kommunikáció a központi publikus elektronikus hírközlő hálózattól elszigetelten zajlik A Cornell Egyetem nagy tömegű IKT eszközök jelenlétéből adódó 6G alapú „ember-gép-IoT” komplex digitális ökoszisztémára, mint a metaverzum egyik lábának megvalósulására irányuló kutatása kellően rávilágít a 6G infrastruktúrán, még az 5G hálózatnál is nagyobb mennyiségű adatfolyam megkeletkezésére,[491] melyre mind kapacitási oldalról, mind az adatok minőségi értelmezhetőségének oldaláról szükséges felkészíteni az LI rendszereket. Az 5G-nél már fejlettebb 6G alapú holografikus 3D kommunikáció merőben új távlatokat nyithat a nemzetbiztonsági célú LI számára, hiszen az eddigi hang, szöveg, kép, élő videóstream 2D-s síkjáról kiléphet a 3D-s LI új technológiájára.

[488] HUANG at al. 2024
[489] SHAO at al. 2023
[490] *5G hálózati szeletelés optimalizációja megerősítéses tanulás segítségével*. BME VIK.
[491] GAO at al. 2023: 7411 – 7435

Továbbá már az 5G technológia vonatkozásában is megállapítható, hogy az Utimaco 5G LI-vel kapcsolatos tudományos közleménye,[492] a Cornell Egyetem témakört érintő kutatása,[493] valamint a 2. fejezetben részletezett szigorodó alapvető jog védelmi szabályozási követelmények okán érvényesülő, a 3.1.3. részfejezetben ismertetett kriptográfiai szabványkörnyezet lényegében ellentmondóak a biztonsághoz fűződő közérdek, mint alapvető jog korlátozó ok érvényesíthetőségével az LI során. Azaz kibillen az egyensúlyból a magánszféra védelméhez fűződő alapvető jog védelme és a nemzet-, közbiztonság garantálásához fűződő közérdek. „*Az 5G a korábbi technológiáknál jobban védi a végfelhasználók anonimitását mind a rádiós, mind a mag[core]hálózaton belül. Ezt úgy érik el, hogy a rádiós interfészen kikényszerítik a személyazonosság elrejtését és az 5G mag[core]hálózaton belüli titkosítást, és ennek eredményeként a hagyományos LI képességek nem tudják ellenőrzés alá vonni a kommunikáció kísérő adatait, továbbá nem tudják eredeti formában ellenőrzés alá vonni a közlemények tartalmát, amikor az áthalad a hálózati infrastruktúrán*.” [494] Tehát mivel a hírközlési szolgáltatók egyedi biztonsági intézkedéseket vezetnek be saját előfizetőik adatvédelme érdekében, korlátozódik az előfizetői, kommunikációs adatokhoz való jogszerű hozzáférés lehetősége.[495]

A fentiek alapján érzékelhető, hogy a nemzetbiztonsági, bűnüldözési érdeket hátrányosan érintő – EU-s digitális gazdasági törekvések okán érvényesülő – fokozott adatvédelmi követelmények során jelentkező „biztonság-deficit” jog- és szakpolitikai tekintetben is orvosolásra szorul, hiszen álláspontom szerint ez egy igen kontraproduktív folyamatként prognosztizálható gazdaságnövekedési, társadalomdigitalizációs szempontból az Unió területén. Ennek oka, hogy az Unió éppen a gazdasági növekedés érdekében fogalmazza meg az IKT termékeket és szolgáltatásokat érintő fokozott adatvédelmi követelményeket a felhasználói bizalom erősítése, így végsősoron a többlet fogyasztás elősegítése érdekében. Azonban, ha ezáltal a nemzetbiztonsági, bűnüldözési célú LI korlátozottsága okán végsősoron közvetve sérül az egyes tagállamok, így összességében az EU biztonsághoz fűződő közérdek érvényesítését célzó eszközrendszerének hatékonysága, akkor össztársadalmi szinten csökken a komplex biztonság, mely az IKT termékek keresletének visszaesésén keresztül hátrányosan érinti az uniós és

[492] *What are the challenges of 5G for Lawful Interception?* Utimaco.
[493] INTOCI, Francesco - STURM, Julian - FRAUNHOLZ, Daniel – PYRGELIS, Apostolos – BARSCHEL, Colin (2023): *P3LI5: Practical and confidEntial Lawful Interception on the 5G core.* New York: Cornell University. Online: https://www.researchgate.net/publication/373451462_P3LI5_Practical_and_Confidential_Lawful_Interception_on_the_5G_Core (Letöltés ideje: 2024. február 23.)
[494] *What are the challenges of 5G for Lawful Interception?* Utimaco.
[495] INTOCI at al. 2023

tagállami gazdaságnövekedési törekvéseket, így az általános digitális ökoszisztéma, a digitális társadalom megteremtésének uniós szakpolitikai, stratégiai célját. (A fentiek a továbbiakban: „IKT adatvédelmi biztonság-deficit".)

A 5G-nél már megjelenő, de várhatóan a 6G-nél kicsúcsosodó világűrinfrastruktúra elemeket integráló hálózatok diszruptív módon fogják átalakítani a hagyományos hírközlést és egyben a hírközlési LI-t.[496] A nem is olyan távoli jövő MI-vel támogatott, integrált, VHetNet rendszerek LI-je mind a 3 rétegű föld/levegő/világűr infrastruktúrán[497], mind a kriptográfiai környezet fejlődésén túl[498], a személyes adatvédelem, -adatkezelés terén is kihívásokkal fog szembesülni, ami pedig vizsgálandó normatív jellegű kérdéseket is felvet a jövő LI technológiái szempontjából. Az Űrstratégia célrendszerével összhangban a hazai űriparágazati aktorok legújabb döntése értelmében űripari- és műholdfejlesztési, UAV gyártási és védelmi, valamint védelmi digitalizációs tevékenységet ellátó vállalat bejegyzése történt 2024. február hónapban, továbbá a globális űriparban való hazai szerepvállalás erősítése okán 2024. február 22-én megjelent sajtóinformációk alapján hazai állami hátterű vállalat jelentős tulajdonrészt szerzett a REDMED Technológia Fejlesztő Zrt-ben, ami beszállítója az Európai Unió Űrügynökségnek (a továbbiakban: EASA[499]), a NASA[500]-nak, valamint a Japán Űrügynökségnek is.[501] Az előrejelzések szerint „*maga a műholdas távközlés, a távérzékelés, az adatok továbbítása a közeli jövőben már nem a földön fog történni, 2030–2040 táján a nagyhatalmak a vezetési pontjaikat kitelepítik a világűrbe.*"[502] Az idézet jól szemlélteti, hogy Magyarország nemzeti érdeke az űrfelderítő képesség kialakítása a haderőreform keretében, mely LI vonzatokkal is bírhat, így ennek a technológiai fejlesztéseken túl humánerőforrás vonzata is speciális. A Magyar Honvédség egyetemi és civil partnerségi együttműködés keretében megkezdte az

[496] „*A műholdas technológia fejlődése olyan szolgáltatási ágazatot hozott létre, amely különféle szolgáltatásokat kínál a műsorszolgáltatók, internetszolgáltatók (ISP), kormányok, katonaság és egyéb szektorok számára. A műholdak háromféle kommunikációs szolgáltatást nyújtanak: telekommunikáció, műsorszórás és adat kommunikáció. A telekommunikációs szolgáltatások magukban foglalják a telefonhívásokat és a telefonszolgáltatóknak, valamint a vezeték nélküli, mobil- és mobiltelefon-szolgáltatóknak nyújtott szolgáltatásokat*." VÁRI Péter (2020): *Ég és Föld közötti kapcsolatok – Az űrtávközlés története, elmélete és gyakorlata*. Budapest: Wolters Kluwer. 12.

[497] PRIYANKA at al. 2023; DAKKAK at al. 2023: 1-16; KUR at al. 2021; MOHSAN – LI 2023; ERDOGAN at al. 2023: 208-216

[498] ERDOGAN at al. 2023: 208-216

[499] EASA: European Union Aviation Safety Agency - Európai (Unió) Űrügynökség

[500] NASA: National Aeronautics and Space Administration - Nemzeti Repülési és Űrhajózási Hivata (USA)

[501] TAMÁSI Dávid (2024): Sajtóközlemény: *A 4iG csoport önálló vállalatba szervezi űr- és technológiai portfólióját*. SpaceJunkie. Online: https://spacejunkie.hu/sajtokozlemeny-a-4ig-csoport-onallo-vallalatba-szervezi-ur-es-technologiai-portfoliojat/ (Letöltés ideje: 2024. február 25.)

[502] *„Elsőnek lenni dicsőség, elsőnek lenni felelősség"*. Magyarország Kormánya. 2021. Online: https://kormany.hu/hirek/elsonek-lenni-dicsoseg-elsonek-lenni-felelosseg (Letöltés ideje: 2024. február 25.)

űrhadviselésre dedikált katonai állomány kiképzését.[503] Az egyetemi szférában kiemelendő az NKE Világűrjog és -Politika Kutatóintézet létrejötte, valamint az interdiszciplináris űrképzés beindítása 17 hazai egyetem, köztük az NKE és BME együttműködésében.[504] Ezen hazai űripari fejlődési törekvés összhangban áll Stratégia 167. pontjával és egyben nemzetbiztonsági érdek is, miszerint „a *magas hozzáadott értékű, magas technológiai know-how-t biztosító, innováción alapuló űrszektorban való megjelenés rendkívül fontos, ami feltétele a világűr gazdasági, nemzetbiztonsági és védelmi területeihez történő hozzáférésnek."* A hazai űripari törekvésekkel integrált UAV fejlesztési irány összhangban álla a 6G alapú VHetNet koncepciójával a HAPS-ok tekintetében, miszerint abba az UAV-knek is kiemelt szerepe van, mobil LI esetén például az IRS modulok jelvisszaverődésének ellenőrzése esetén is. Tehát megállapítható Magyarország fokozott és erőteljes stratégiai törekvése az űriparban rejlő IKT és biztonsági lehetőségek kiaknázása, a kihívások kezelése, így az értekezés során indokolt vizsgálni a világűrinfrastruktúrára épülő jövőbeli elektronikus hírközlő hálózatok LI-jével kapcsolatos lehetőségeket és kihívásokat technológiai, és normatív oldalról egyaránt.

A 6G alapú VHetNet infrastruktúra LI-je szempontjából összefoglalóan az alábbi hírközléstechnológiai, elektronikus- és normatív adatvédelmi, valamint LI szabályozási és technológiai kihívásokat azonosítom:

- **Hírközlés technológia:** lényegében a földi végponti IKT eszközök a 6G alapú VHetNet infrastruktúrán nem a 3.1.1. részfejezetben bemutatott hagyományos földfelszíni hírközlő hálózaton a RAN és központi (core)rendszerelemeken keresztül kommunikálnának egymással, hanem a végponti IKT eszköz a HAPS-okhoz integrált RAN-okon keresztül egymással direkt kommunikációt folytathatnak. Illetve, ha a HAPS nem biztosítja a kellő spektrumnyaláb lefedettséget a kommunikáló végponti eszközök tekintetében, akkor a világűrbe telepített LEO műholdakat is igénybe vehetik, így kihasználva mind a 3 vertikális réteg technológiai lehetőségeit. Így az állami lefedettség helyett már statikus geostacionális regionális jellegű, vagy dinamikus regionális, globális műholdas területi lefedettségről beszélünk. Ebben az esetben a hálózati forgalom akár elkerülheti a hagyományos központi (core)rendszert, így a hagyományos monitoring LI alrendszert is, tehát a hálózati forgalom ellenőrzése korlátozottá válik;

[503] *Új elitfegyvernem született.* Magyar Nemzet. 2021. Online: https://magyarnemzet.hu/belfold/2021/05/uj-elitfegyvernem-szuletett (Letöltés ideje: 2024. február 25.)
[504] *Interdiszciplináris "űrképzés" indul 17 hazai egyetem együttműködésében*. NKE. 2021. Online: https://vtkm.uni-nke.hu/hirek/2021/12/19/interdiszciplinaris-urkepzes-indul-17-hazai-egyetem-egyuttmukodeseben (Letöltés ideje: 2024. február 25.)

- **Elektronikus információvédelem (kriptográfia):** az FSO infrastruktúra kriptográfiai tulajdonságai nem ellenállóak az algoritmikus támadásokkal szemben, így azok fejlesztése szükséges. Kibervédelmi szempontból lényeges kérdés az UAV-k HAPS infrastrukturális támogató szerepe is, mely szintén vizsgálandó adatvédelmi körülmény;
- **Normatív személyes adatvédelem**: a hagyományos földi hírközlési infrastruktúra viszonylag jól lehatárolhatóvá tette az adatkezelés joghatósági szabályait, a tagállami jogforrások területi hatálya alapján, mely adott ország – vagy a *sui genesis* EU – területét, illetve a hatáselv alapján az ott igénybe vehető szolgáltatósokat érintette. Például az IKT piacon akár uniós vonatozásában a DMA, a GDPR tekintetében, hazai vonatkozásban az Eht., Ekertv. tekintetében. Továbbá felmerül a GDPR szerinti európai állampolgár EU-n kívüli adatkezelésének tilalmával kapcsolatos dilemma;
- **LI szabályozás**: kérdés vetődik fel a jogosult LI szerv feladatvégrehajtásának területi hatálya kapcsán a HAPS-ok, LEO műholdak légi, űrbéli elhelyezkedése okán felmerülő hagyományos hírközlő központi (core)rendszert elkerülő adatfolyamok kicsatolása és ellenőrzése esetén. Hiszen ezek már nem országon belüli, hanem regionális, akár globális hírközlési forgalmat bonyolítanának. Ez az elektronikus hírközlés globalizációjához vezetne, mely drasztikusan korlátozná az állami joghatóságot és előtérbe helyezné a nemzetközi, uniós joghatóság szupranacionális terrénumát a hírközlési tevékenység, az adatkezelés és az LI szabályozása terén egyaránt. Ennek okán mind a nemzeti, mind a nemzetközi, uniós hírközlés jog felülvizsgálata indokolttá válhat;
- **LI technológia:** a fentiek alapján megállapítható, hogy a 6G alapú VHetNet infrastruktúra esetén a hírközlési adatfolyamok jelentős részben elkerülhetik a hagyományos elektronikus hírközlő infrastruktúra központi (core)rendszerét, és azok a HAPS-okon, LEO műholdakon folyhatnak át. Így szükséges lehet a hagyományos központi monitoring alrendszerű DPI típusú LI architektúra felülvizsgálata és optimalizálása a megváltozó, innovatív műhold alapú hírközléshez, amely képes áthidalni a fejlődő kriptográfiai szabványokban rejlő kihívásokat is egyaránt.

A fentiek alapján tehát megállapításra és bizonyításra került, hogy már a napjaink hírközlő hálózatain is, de igazán a jövőben az 5G, 6G mobilhálózatokon rendkívül nagy mennyiségű, és rendkívül heterogén típusú adat (kommunikációs tartalom, kísérő- és metaadat, jel) fog megjelenni, például az okos város komplex digitális ökoszisztéma egyes olyan szolgálatásai, mint az e-mobilitás, okos pénzügyi szolgáltatások, okos egészségügy, kommunikációs

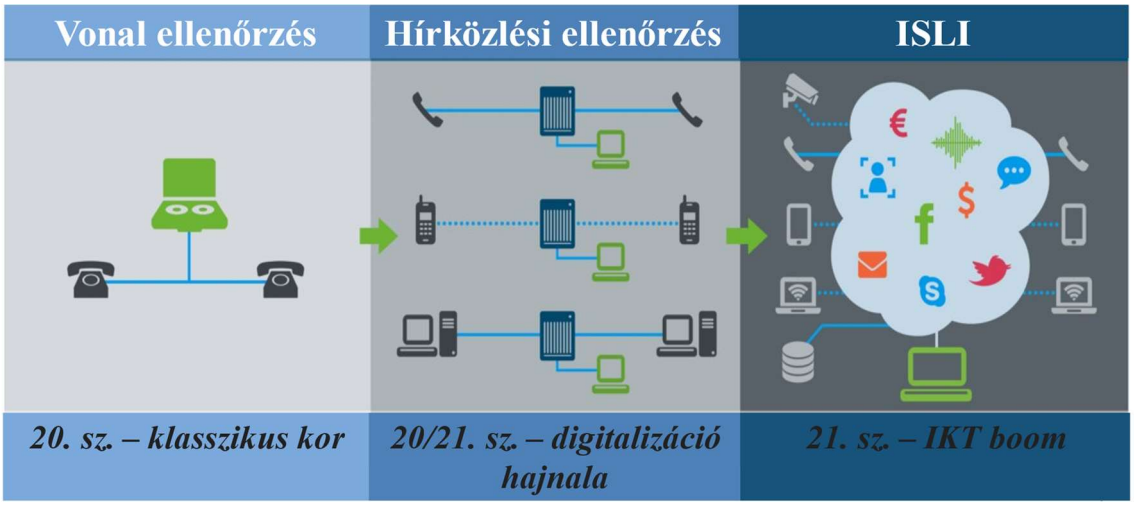
szolgáltatások (alkalmazásszolgáltatások), szórakoztató szolgáltatások (videóplatformok, lekérhető média, közösségi média), vagy akár a VR/AR tekintetében. Így a hírközlő hálózatokon megjelenő egyre heterogénebb adattípusok okán az LI fogalmának még tágabb értelmezése válik indokolttá az IKT környezet fejlődéséből adódóan. A mobilhálózatokon a személyközi kommunikáció során jelenlévő hang, szöveges, multimédiás IP adatforgalom mellett a 21. században folyamatosan bővül a természetes személyek információs társadalommal összefüggő egyes smart szolgáltatásainak igénybevétele – ember-gép kommunikáció – során keletkező adattípusok köre. Tekintettel arra, hogy ezen adatok jelentős része természetes személy kommunikációjához köthető, és titkos információgyűjtés során relevanciával bírhat például szokások, kapcsolati háló, felkeresett helyek stb. azonosítása érdekében, indokolt integrált módon az LI fogalomkörén belül értelmezni azokat, hiszen azok ellenőrzésére a hírközlő hálózati adatforgalom kicsatolásával lehetőség nyílhat.

Ezen szolgáltatások igénybevételével keletkező információk ellenőrzése a titkos információgyűjtéssel érintett (cél)személyek vonatkozásában, például mind a terrorizmus, illegális migráció, szervezett bűnözés visszaszorítás érdekében hozzáadott értéket képezhetnek a jövő LI képességei számára. Stratégiai fejlesztési irányként javaslom, már csak a meglévő Eht. 92. § szerinti törvényi háttér miatt is, hogy a hagyományos elektronikus hírközlő hálózat vonatkozásában a titkos információgyűjtés erőforrásoptimalizációs és hatékonysági szempontokból, összadatforrású (a továbbiakban: ASI[505]) jelleggel a hírközlő hálózat központi (core)rendszeréhez integrált monitoring DPI típusú alrendszeren keresztüli megvalósítása legyen prioritás. Hiszen általánosságban itt átfolyik minden személyközi kommunikációval, és szolgáltatásigénybevétellel kapcsolatos adatforgalom. Ezzel a megoldással tekintettel a C2SE-t áthidaló LI szabványosításra a közlemények és az adatok elméletben a hálózati rejtjelezéstől mentesen válnak ellenőrizhetővé. Azonban vizsgálandó az egyes végponti alkalmazások, szoftverek kriptográfiai környezete (első sorban az E2EE), az alkalmazásszolgáltatások tekintetében erre az értekezés következő fejezetében sor is kerül, valamint az újgenerációs hálózatoknál a további LI-t nem ellehetetlenítő kriptográfiai megoldások kialakítása. Az adatok fokozódó mennyiségére tekintettel előreláthatólag szükségessé fog válni egyfajta adaptív[506] MI alapú intelligens „smart” rendszerezési, jelölési (például a szemantika keretében

[505] ASI: All-Source Intelligence – összadatforrású felderítés. Lásd: *Glossary of Terms and Definitions AAP-06 (2021)*. NATO Standardization Office, 2021. 10.

[506] Lásd: DELI Tamás (2021): *Adaptív moduláció támogatása gépi tanulási módszerekkel műholdas rádiócsatornán*. Budapest: BME VIK. Online: https://tdk.bme.hu/VIK/DownloadPaper/Adaptiv-modulacio-tamogatasa-gepi-tanulasi3 (Letöltés ideje: 2024. február 25.)

szimbolizáció), és kiválasztási eljárás, technológia bevezetése egy fúziós ASAS[507] jellegű adatelemző, értékelő, feldolgozó rendszer elemeként. Reflektálva az értekezés 6. hipotézisére, a fentiekre gyakorlati megoldásként egy ún. Integrált Smart LI (ISLI) koncepció, LI képesség kialakítását javaslom, amely elméleti megvalósítását, tulajdonságait a fenitek szerint definiálom. A hírközlés, majd az IKT technológiák és szolgáltatások fejlődésének hatására egyre heterogénebb adattípusokat, és párhuzamosan az LI lehetőségek funkcionális szemléletű elnevezésének evolúcióját a 26. ábra hivatott szemléltetni.



26. ábra: A hírközlő hálózatokon megjelenő egyre heterogénebb hálózati forgalom, és az LI lehetőségek funkcionális szemléletű elnevezésének evolúciója (Szerk.: A szerző)

Azonban, ha például a 6G alapú VHetNet hírközlési technológia a jövőben általánosan elterjedésre kerülne, a hálózat vertikális szegmentálása okán (a földfelszíntől elmozdul a világűr irányába), a IKT fejlődés hatására a hírközlő hálózat hagyományos állami felügyeletben lévő központi (core)rendszerét az adatfolyamok előreláthatólag elkerülhetik, a magasabb vertikális szinten lévő, a „nemzetközi térbe" kihelyezett decentralizált adatforgalmat irányító rendszerelemek irányába (UAV, HAPS, LEO műhold). Ezért elméletben szükségessé fog válni minden egyes adatforgalmat irányító elem monitoring alrendszerrel történő ellátása. Így indokolttá válhat az ilyen monitoring alrendszereken kezelt adatok aggregálása egy integrált központi monitoring LI rendszerben, melyet ISLI 2.0-ként hivatkozok. Ehhez javaslom a

[507] ASAS: All-Source. Analysis System - Minden Adatforrást Elemző Rendszer. Lásd: GYÖRGY András - KOVÁCS László (2001): Az amerikai „Minden Adatforrást Elemző Rendszer" (ASAS) és a magyar elektronikai-harc vezetési komplexumok rendszertechnikai összehasonlítása. *Hallgatói Közlemények*, 5(1), 112-128.; KOVÁCS László (2000): Az összadatforrású felderítés és a pilótanélküli felderítő repülő eszközök kapcsolata. *Repüléstudományi közlemények*, 12(1), 231-235. Online: https://epa.oszk.hu/02600/02694/00026/pdf/EPA02694_rtk_2000_01_231-238.pdf (Letöltés ideje: 2024. április 1.)

hagyományos ISLI rendszer adatforrásainak illesztését, így kiteljesítve az összadatforrású LI információgyűjtő képességet a földi, levegő és világűr infrastruktúrán üzemelő hírközlő hálózatok tekintetében, mely esetén szintén indokolt a fúziós elemzési képesség. Az ISLI 2.0 esetén azonban már minimum EU szintű együttműködési vetületen kell gondolkodni hazai viszonylatban, mind az LI technológia, mind az LI szabályozás, mind a személyes adatkezelés területén. Így akár kialakítva egy kölcsönös tagállami bizalmon alapuló „többnemzeti" jellegű LI képességet, legalább az egyes decentralizált adatforgalmat irányító rendszerelmekehez illesztett monitoring alrendszerek technológiai megvalósítása terén, az integrált központi monitoring LI rendszer tagállami felügyelete mellett, így biztosítva a nemzeti szuverenitást az ellenőrzések végrehajtása során. Tehát az ISLI 2.0 koncepció szerint amíg a légtérben, a világűrbe elhelyezett, regionális lefedettséget biztosító adatforgalmat irányító rendszerelemek (UAV, HAPS, LEO műhold) decentralizált, egyedi monitoring LI alrendszerei egymástól függetlenül, több állam LI igényeit szolgálhatnák ki, addig az ezek irányába lekérdezést, ellenőrzést, majd az adatok aggregálását, feldolgozását végrehajtó központi monitoring LI rendszerek állami hatáskörben, felügyelet mellett működnének. Így érvényesítve az IKT környezet fejlődéséből adódóan szükségessé váló nemzetközi együttműködést, azonban tiszteletben tartva a nemzeti szuverenitást a jövő LI képességei terén. Álláspontom alapján a három szupranacionális feltétel közül a személyes adatkezelés, -védelem alapjai a GDPR és az e-hírközlési irányelv alapján biztosítottak, az LI végrehajtásának szabályozása, és a technológia kialakítása még várat magára. Így célkitűzésként indokolt megfogalmazni a fentiekben levezetett LI szabályozás és technológia követő jellegét felváltó, megfelelő szcenáriókkal, tudományos kutatási eredményekkel alátámasztott, előrelátó stratégiai szemlélet[508] meghonosítását az LI képességfejlesztés területén.

Az adatvédelem/biztonság értékduál kapcsán azonosításra és bizonyításra került az alfejezetben az „IKT adatvédelmi biztonság-deficit", mely álláspontom alapján orvosolásra szorul az EU digitalizációs jog- és szakpolitikai stratégiai törekvéseinek megvalósítása érdekében. Azért, hogy az értekezés vizsgálatának elsődleges tárgyául szolgáló titkosított online kommunikációt biztosító alkalmazásszolgáltatások LI-jének elemzése teljes körű legyen, szükséges a következő fejezetben azok felhasználói, adatvédelmi trendjeinek részletes vizsgálata, az ellenőrzési lehetőségek okán a főbb alkalmazásszolgáltatások kriptográfiai jellemzőinek áttekintése, valamint a hazai alkalmazásszolgáltatókat érintő LI szabályozás értékelése.

[508] Lásd: DOBÁK – TÓTH 2023: 33-50

3.4. Részkövetkeztetések

Az értekezés érdemi tartalmi második részében, azaz a 3. fejezetben a mobil hírközlési ellenőrzést érintő IKT trendek, tendenciák komplex elemzésére került sor a meghatározott kutatási módszertan alapján, a hipotézisek alátámasztása és az új tudományos eredmények eléréséhez szükséges részkutatómunka elvégzése érdekében. A fejezeten belül vizsgálat tárgyát képezte az elektronikus digitális mobilhálózatok evolúciója, fejlődési trendjei, a mobilhálózatok felhasználói tendenciái, a mobilhálózatok kriptográfiai környezetének evolúciója, kitekintve az LI szabványosításra, a hazai hírközlési kommunikációellenőrzés normatív, szervezeti, technológiai, trendjei mellett. Az egyes al- és részfejezetekben a meghatározott kutatási módszertan alkalmazása során elvégzett cselekmények alapján az alábbi fő részkövetkeztetések vonhatók le:

3.1. alfejezet: Azonosításra kerültek az újgenerációs, rendkívül nagy kapacitású mobilhálózatokkal szemben támasztott felhasználói és fokozott adatvédelmi igények, valamint az azok által biztosítható egyes high-tech szórakoztató (VR/AR) és kommunikációs technológiák (alkalmazásszolgáltatások), továbbá a fejlett okos város digitális ökoszisztéma szolgáltatások (például e-mobilitás, okosközlekedés) várható lakossági megjelenése és elterjedése, melyeket hírközlési infrastruktúra oldalról tömegesen az 5G és 6G fog várhatóan kiszolgálni. A mobil hírközlés technológiák terén kb. 10 évente tapasztalható egy generációugrás, amely a fenti hálózati tulajdonságok érzékelhető fejlődését mutatja, a hálózati forgalom folyamatos heterogenizációja mellett, a felhasználói igények, és az új IKT szolgáltatások kiszolgálása érdekében. Ismertetésre kerültek az EU fokozódó adatvédelmi előírásai miatt az elektronikus hírközlő hálózat kiberbiztonságát garantáló kriptográfiai (C2SE) szabványok, melyek biztonsági jellemzői az 5G-nél csúcsosodnak ki, kitekintve az LI szabványosítás alakulásaira, folyamataira. A 6G bevezetése terén, akárcsak a 4G és 5G-nél szintén Dél-Korea kíván globális vezető szerephez jutni, annak 2030-ra történő általános lakossági bevezetésére irányuló kormányzati szándék alapján. Magyarország 2030-ig szóló Űrstratégiájának célrendszere alapján ki kívánja aknázni az űriparban, így az világűrinfrastruktúrával bíró hírközlésben rejlő innovatív és fenntartható gazdasági növekedést ösztönző lehetőségeket a hazai vállalatok nemzetközi szerepének erősítésével, valamint az űrszektor fejlődéséhez elengedhetetlen tudásalapú társadalmi, gazdasági feltételek, és a szükséges infrastruktúra fejlesztésével. Bemutatásra kerültek a globális űriparban, -piacon történő hazai jelenlét erősítését célzó legfrissebb intézkedések. **Így kutatási részeredmény,**

hogy a jövőben a világűr infrastruktúrára épülő elektronikus hírközlő hálózatok elterjedése várható. [H2; H4]

3.2. alfejezet: Megállapításra és tendenciaelemzési során bizonyításra került, hogy globális szinten **kb. 2030-ra az 5G lakossági mobil-előfizetések átveszik a vezető szerepet a 4G-vel szemben, szinte teljesen kiszorítva a korábbi technológiákat (2G, 3G)**. Összességében a mobil-előfizetések száma folyamatosan emelkedő tendenciát mutat globális szinten, így a hálózati modernizáció mellett megállapítható a növekvő kereslet, mely tendenciák között összefüggés azonosítható az újgenerációs hálózatok többletszolgáltatási lehetőségei okán. [H1] Az európai régiót vizsgálva **tapasztalható egy IKT piaci megosztottság a nyugat- és a közép-kelet-európai térség között, ami abban is megnyilvánul, hogy az EU-s digitalizációs törekvések a nyugat-európai országokban jobban érvényesülhetnek, mint a közép-keleti régióban**. A közép-kelet-európai adatok azért lényeges Magyarország, így a hazai LI számára, mivel **a fentiek alapján megállapítható az elektronikus hírközlési szolgáltatások állami jellegének eltolódása a régiós, globalizálódó jelleg irányába, melyet alátámaszt a 6G alapú, MI támogatott, integrált VHetNet elektronikus hírközlő koncepció**. Így a hírközlési LI tekintetében indokolt és szükséges a régiós prognosztikus előrejelzések figyelembevétele a hazai LI képesség kutatás-fejlesztése és a jogalkotás szempontjából. A tendenciák az elkövetkező 6 éves időszakban a közép-kelet-európai régióban a lakossági célú, személyközi hírközlési kommunikációt érintően **a 4G vezető szerepét vetítik előre, az 5G exponenciális erősödése, majd a 4G fokozatos kiszorítása mellett**. [H2; H4] **A fentiek alapján bizonyításra került, hogy a jövőben a légi, világűr infrastruktúrára épülő elektronikus hírközlő hálózatok elterjedése várható, amelyeken kezelt kommunikáció LI-je mind normatív, mind technológiai kihívásokat fog generálni a hagyományos infrastruktúrákhoz képest.** [H2]

A hazai mobil hírközlési trendek elemzése során megállapításra került, hogy **a mobil adatforgalom 2016-ot követően egy rendkívül dinamikus exponenciális növekedést produkál összhangban a nemzetközi trendekkel**, 2016 és 2023 második negyedéve között, mintegy 25-szörösére növelve annak mértékét, mely láthatóan összefügg a 4G szolgáltatás magyarországi bevezetésének időpontjával. **A hazai tendenciaelemzés során megállapításra került, hogy az újgenerációs mobilszolgáltatások elterjedése elsősorban a 4G és 5G azonos tendenciát mutat a globális és regionális trendekkel, azaz kiszorító hatással bír a korábbi 2G, 3G technológiákra. A regionális 5G trendeket vizsgálva azonban megállapítható, hogy**

2023-ban Magyarország jócskán túlszárnyalta a közép-kelet-európai átlagot. [H1; H2; H3; H4] Tehát előreláthatóan az újgenerációs mobilhálózatok egyfajta IKT boom-ot fognak okozni hazai viszonylatban is a kereslet kielégítése során. A mobil hívások időtartama 2021-ig növekvő tendencia mutatott, mely ezután csökkeni kezdett. **A mobil hívások időtartamának 2021-et követő visszaesését az elemzés alapján egyértelműen az online titkosítást biztosító alkalmazásszolgáltatások intenzív, tartós térnyerése okozza, melyet mind a teljes hazai mobilinternet piacra kivetített adatforgalom, mind az egy SIM kártyára jutó fajlagos mobilinternetes adatforgalom exponenciális növekedése is alátámaszt**, a vizsgált statisztikai adatok alapján. A mobilinternet térnyerésével, így a kommunikáció „internetalapúságával" kapcsolatos trendek az LI szempontjából is kiemelten lényegesek, így az értekezés vizsgálatának szempontjából is mérvadók. [H1; H2; H3; H4]

3.3. alfejezet: Az Eht. – és az azt megelőző szabályozás mellékletek szerinti vizsgálata – alapján megállapítást nyert, hogy **a hírközlési ágazati szabályozás a rendszerváltást követő időszakban együttesen valósult meg az LI törvényi szintű szabályozásával, azaz a hírközlési LI szerves részévé vált a hírközlési ágazati szabályozásnak**. Ezen továbbmenő következtést, hogy a 3.3.1. részfejezetben bemutatott hazai hírközlési tevékenység Eht.-ra épülő 21. századi normarendszerén belül **a hírközlési LI ágazati szabályozás ugyan olyan erőteljes transzparenciával valósul meg,** mint a 2.5. alfejezetben bemutatott Nbtv. és Be. szerinti általános nemzetbiztonsági és bűnüldözési célú LI szabályozása, **egyetemben a speciális rendvédelmi ágazati törvényekkel** (Ütv., Rtv., NAV tv.). [H1] A részkutatási cselekmények alapján megállapítható **a hírközlés globalizációja, valamint a határokon átívelő bűnözés erősödése, a 2015/16-tól fokozódó terrorizmus és illegális migráció magával hozta az uniós jogalkotást, jogharmonizációt a bűnüldözési célú titkos információgyűjtés tekintetében, valamint a szorosabb együttműködés szükségességét a tagállamok bűnüldöző szervei között.** [H4] A 2.5.1. részfejezetben ismertetettek alapján bűnüldözési érdekkörben, azaz bűnüldöző – igazságügyi – szerv megkeresésére ENYH esetén, az ENYH irányelv és a 2012. évi CLXXX. törvény vonatkozó rendelkezései, valamint bűnüldöző szerv – rendőrség, vámhatóság – megkeresésére, a 2006/960/IB kerethatározata és a 2002. évi LIV. törvény 8. § (2) bek. alapján **nemzetközi bűnüldözési célú titkos információgyűjtés, azon belül is az LI végrehajtására szintén igénybe vehetik az NBSZ szolgálatatásait**. Azonban az értekezés szempontjából lényeges nemzetbiztonsági érdekkörben jelentkező, nemzetbiztonsági célú együttműködésre az uniós jog hatálya nem terjed ki jelenleg. Továbbá az Eht. és a 180/2004.

(V.26.) Korm. rendelet **az NBSZ-t jelöli ki a hazai központi „LI szolgáltatói" szerepkör betöltésére**. [H1; H4]

Az alfejezetben azonosításra került az ún. „IKT adatvédelmi biztonsági-deficit", amely értelmében a fokozódó uniós adatvédelmi előírások a kriptográfia erősödése okán hátrányosan fogják érinteni az LI hatékonyságát – már az 5G-nél is – így a nemzet- és közbiztonság alkotmányos közérdek érvényesülését. Ennek oka, hogy az Unió éppen a gazdasági növekedés érdekében fogalmazza meg az IKT termékeket és szolgáltatásokat érintő fokozott adatvédelmi követelményeket a felhasználói bizalom erősítése, így végsősoron a többletfogyasztás elősegítése érdekében, azonban, ha ezáltal a nemzetbiztonsági, bűnüldözési célú LI korlátozottsága okán végsősoron közvetve sérül az egyes tagállamok, így összességében az EU biztonsághoz fűződő közérdek érvényesítését célzó eszközrendszerének hatékonysága, akkor össztársadalmi szinten csökken a komplex biztonság. Ez az IKT termékek keresletének visszaesésén keresztül hátrányosan érinti a gazdaságnövekedési törekvéseket, így az általános digitális ökoszisztéma, a digitális társadalom megteremtésének uniós szakpolitikai, stratégiai célját.

További részkutatási eredményként megállapításra és bizonyításra került, hogy a jövőben az 5G, 6G elektronikus hírközlő hálózatokon rendkívül nagy mennyiségű, és egyre heterogénebb típusú adat (kommunikációs tartalom, kísérő- és metaadat, jel) fog megjelenni, például az okos város komplex digitális ökoszisztéma egyes szolgálatásai kapcsán, melyek mind a terrorizmus, illegális migráció, transznacionális szervezett bűnözés elleni tevékenység során hozzáadott értéket képezhetnek a nemzetbiztonsági, bűnüldözési célú LI számára. **Optimális stratégiai kutatás-fejlesztési irányként a 3.3.2. részfejezetben bemutatott és alátámasztott ISLI koncepció szerinti LI képesség kialakítását javaslom. Illetve a 6G alapú VHetNet műholdas hírközlési infrastruktúra előrejelzések szerinti 2030/2040 körüli elterjedése esetén legalább Unió szintű nemzetközi együttműködés keretében, a nemzeti szuverenitást tiszteletben tartó ISLI 2.0. koncepció szerinti LI képesség lehetőségének megvizsgálását javaslom.** [H1; H2; H4] Az ISLI 2.0. képesség lehetősége kapcsán felmerül a nemzetbiztonsági tevékenység szupranacionális uniós jog alóli kivétel jellege, továbbá az egyes alkalmazásszolgáltatások kriptográfiai környezete is erőteljesen befolyásolja a koncepció hatékonyságát, így a kérdéskör további vizsgálata indokolt.

4. AZ ALKALMAZÁSSZOLGÁLTATÁSOK ELLENŐRZÉSÉT ÉRINTŐ IKT TRENDEK, TENDENCIÁK

A 3. fejezetben áttekintésre kerültek az elektronikus hírközlési szolgáltatások, azon belül is a számfüggő hírközlési szolgáltatásokat érintő LI tevékenység aspektusából lényeges trendek, tendenciák, szabályozási, kriptográfiai környezet, valamint a hírközlési LI-t értintő prognosztikus lehetőségek, javaslatok. Jelen fejezet fő tárgyköre az alkalmazásszolgáltatások LI-jét érintő IKT trendek, tendenciák komplex elemzése a meghatározott kutatási módszertan alapján, a hipotézisek alátámasztása és az új tudományos eredmények eléréséhez szükséges részkutatómunka elvégzése érdekében. A fejezeten belül vizsgálat tárgyát képezi az alkalmazásszolgáltatások felhasználói trendjei, az alkalmazásszolgáltatásokkal összefüggő adatvédelmi trendek, a biztonsági kihívási tendenciák és válaszintézkedések a nemzetközi térben, az alkalmazásszolgáltatások LI-jének hatályos hazai normatív, szervezeti evolúciója, trendjei. Valamint elvégzésre kerül az egyes alfejezetek kutatási cselekményei alapján megállapítható részkövetkeztetések levonása.

4.1. Alkalmazásszolgáltatások felhasználói trendjei, tendenciái

Az alfejezet a 3.2. alfejezetben elvégzett hírközlési trend- és tendenciaelemzését követően ezt az egyes mintavételezési céllal kiválasztott alkalmazásszolgáltatások felhasználói trendjei tekintetében is el kívánja végezni. Mint az a korábbiakban ismertetésre került az alkalmazásszolgáltatások lehetővé teszik a felhasználók számára, hogy online, titkosított csatornán, szöveges, hang alapú (VoIP) és multimédiás tartalmakat megosszanak egymással. A 2. fejezet részkövetkeztetései alapján ezen szolgáltatások nagyon népszerűek az információs társadalmak tagjai körében. Az alfejezetben a mintavételezés céljából kiválasztott Signal, WhatsApp, Messenger, iMessage, Viber, és Telegram szolgáltatások elemzésére kerül sor.

4.1.1. Alkalmazásszolgáltató felhasználókra vonatkozó trendek

A mobil alkalmazásszolgáltatások olyan népszerűek, hogy külön piacként nevesítik azt az egyes kutatóintézetek. A Business Insider 2022-es alkalmazásszolgáltatási piac jelentése alapján 2021-ben kb. 3,09 Mrd ember használt üzenetküldő alkalmazást, ami 4%-kal több az előző éves 3,21 Mrd-hoz képest. Ez 2016-tól 5 év alatt pedig 36 %-os bővülést jelent a

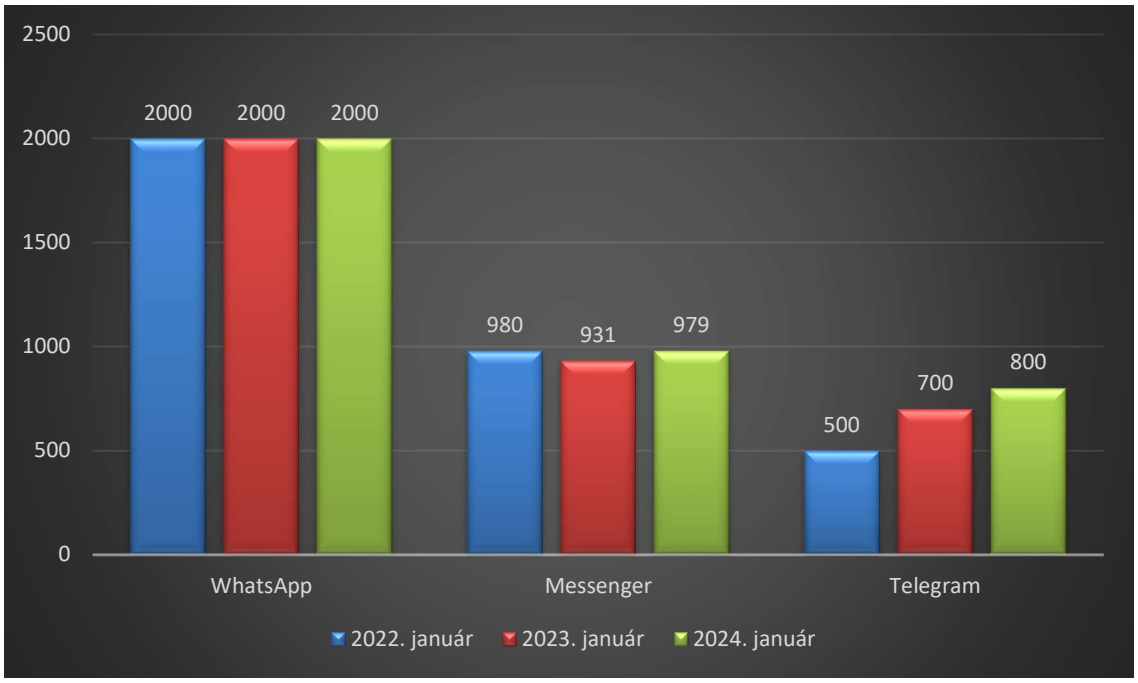
felhasználók tekintetében.[509] A 2023-as jelentés alapján az előrejelzések szerint 2022 és 2030 között is várhatóan jelentős ütemben fog növekedni a piac. A 2023-as 90.790 millió USD-ról 2029-re 274.080 millió USD-ra bővül a gazdasági volumen, az előrejelzési időszakban 20,2%-os összetett éves növekedési rátával,[510] amely a 2024-es piacjelentés alapján 2031-re eléri a 475.982 millió USD-t, szintén tartva a 20,2%-ot.[511] A jelentés szerint a piacon rendkívül gyorsan nő a kereslet, tekintettel arra, hogy a fogyasztók értékelik a költséghatékony kényelmi szolgáltatásokat. Az alkalmazásszolgáltatások piacának perzisztens növekedése a folyamatosan fejlődő IKT és egyben hírközlési technológiák miatt az egekbe fog szökni, az elkövetkező időszak tendenciáit olyan kulcsfontosság szolgáltatások fogják meghatározni, mint például a WhatsApp, Messenger, Viber és a Telegram. A mobil alkalmazásszolgáltatások piacának legszignifikánsabb mozgatórugója az okostelefonok elterjedése, gyakorlatilag „létszükségletté" válása az információs társadalom tagjainál. Továbbá a 3.1. és 3.2. részfejezetekben is vizsgált mobilinternet folyamatos sávszélességbővülése, a lefedettség növekedése és a válaszidő csökkentése is erőteljesen hozzájárul az alkalmazások terjedéséhez.[512] A 2025-ig tartó előrejelzések szerint 2024-ben 3,42 Mrd, 2025-ben pedig 3,51 Mrd felhasználót vetítenek előre.[513] A tendenciát a 27. ábra hivatott szemléltetni.

[509] ENBERG, Jasmine (2021): *Global Mobile Messaging Forecast 2021 (2021). Business Insider eMarket,* Komandotech. Online: https://www.insiderintelligence.com/content/global-mobile-messaging-forecast-2021 (Letöltés ideje: 2024. február 26.)
[510] *Mobile Messaging Services Market Size & Share | Industry Forecast – 2030*. Global Market Research. 2023. Online: https://www.linkedin.com/pulse/mobile-messaging-services-market-size-share-industry-ampfe (Letöltés ideje: 2024. február 26.)
[511] *Mobile Messaging Services Market Size & Share | Industry Forecast – 2031*. Global Market Research. 2024. Online: https://www.businessresearchinsights.com/market-reports/mobile-messaging-services-market-104760 (Letöltés ideje: 2024. február 26.)
[512] *Mobile Messaging Services Market Size & Share | Industry Forecast – 2031*. Global Market Research. 2024.
[513] ENBERG 2021

27. ábra: Alkalmazásszolgáltatás globális éves felhasználói 2019 - 2025 (Szerk.: A szerző[514])

Az alkalmazásszolgáltatásonként megoszlás tekintetében a legnépszerűbbek a Meta szolgáltatásai, azaz a WhatsApp és a Messenger voltak, összességében több mint 2,5 Mrd felhasználóval, több mint 90%-os piaci részesedést produkálva. A 2010-es évek eleje óta a Facebook első helyen áll az üzenetküldés terén, nagy felhasználói bázisával képes volt üzenetküldő platformját önálló alkalmazássá, azaz a Messengerré fejleszteni, amely minden idők egyik legtöbbet letöltött alkalmazásává vált. 2021-re már a WhatsApp lett a legnépszerűbb 2 Mrd felhasználóval, ezt követte a Messenger.[515] Ez a dominancia az alternatív üzenetküldő applikációk piaci megjelenéséhez vezetett, melyek főként a Messengert szorították vissza. A 2013-ban létrehozott Telegram és a 2014-ben bevezetett Signal alkalmazások a kriptográfiai, titkosítási – így az adatvédelmi – környezetük fejlesztésére helyezték a hangsúlyt, mely stratégia folyamatos piacszerzést jelentett számukra, szemben a Facebook és WhatsApp üzenetkezelésének üzleti érdekeiknek való alárendelésével, amely egyben a letöltések számának drasztikus csökkenését is eredményezte a 2020/2021-es évtől.

[514] ENBERG 2021
[515] CURRY, David (2023): *Messaging App Revenue and Usage Statistics (2023)*. Business of Apps. Online: https://www.businessofapps.com/data/messaging-app-market/ (Letöltés ideje: 2023. november 18.)



28. ábra: WhatsApp, Messenger és Telegram január havi felhasználó számának tendenciái 2023-2024 között (Szerk.: A szerző[516])

A fenti 28. ábra alapján 2022 januárjában a WhatsApp elérte a 2 Mrd aktív felhasználót globális szinten és meg is tartotta azokat a legfrissebb adatok alapján, az alkalmazás különösen erős az USA-n kívüli piacokon. Második helyen 2022-ben továbbra is a Messenger állt, kb. 980 millió aktív felhasználóval, mely nagyjából tartotta azt 2024. januárban is, kisebb visszaesést produkálva 2023. januárban. A Nikolai és Pavel Durov által alapított Telegram Messenger Inc. tulajdonában álló Telegram alkalmazás 2022. január havi aktív felhasználóinak száma meghaladta az 500 milliót,[517] 2024. januárra további 300 millióval felhasználóval növelve bázisát. A Telegram havi 700 millió aktív felhasználóval rendelkezett 2023. januárban, és év végére több mint 1 Mrd/hó aktív felhasználót tervezett, mely a 2024. január havi adatok alapján 800 milliót ért „csak" el, így is 100 millió felhasználóval meghaladva az előző időszakot. 2018 és 2023 között a Telegram felhasználók száma 175%-kal nőtt, azaz hozzávetőleg 350 millióval. Az alkalmazás továbbra is Oroszországban a legnépszerűbb, melyet Szingapúr és Németország

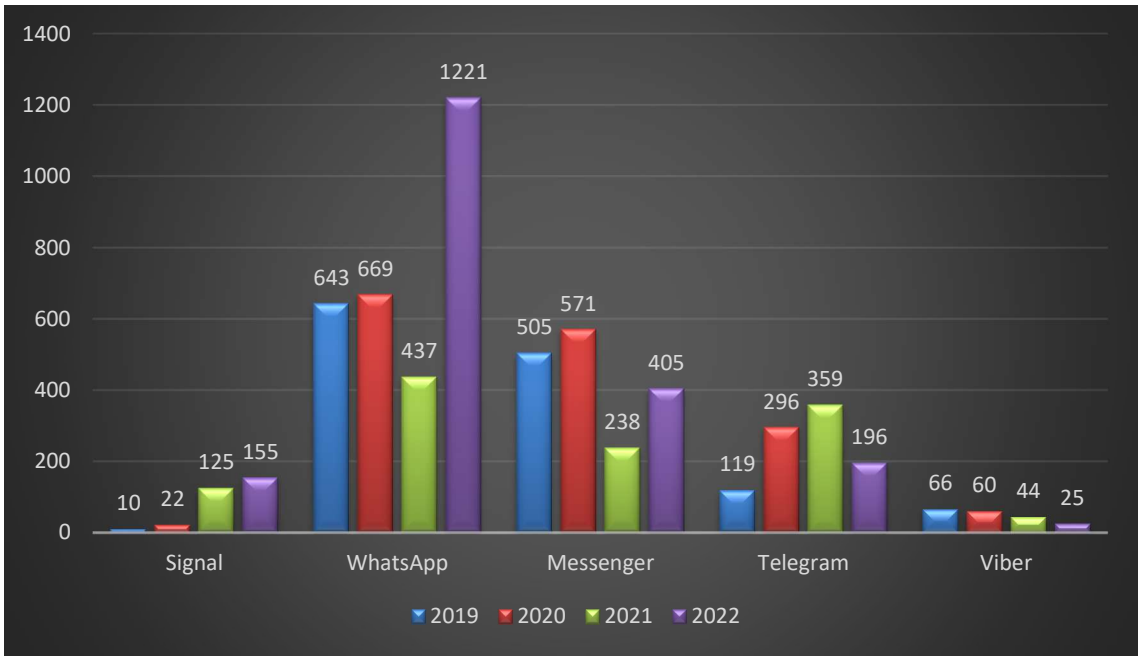
[516] DIXON, Stacy Jo (2024): M*ost popular global mobile messenger apps as of January 2024, based on number of monthly active users*. Statista. Online: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (Letöltés ideje: 2024. február 26.); CHAFFEY, Dave (2023): *Global social media statistics research summary 2023*. Smart Insights. Online: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/ (Letöltés ideje: 2023. március 24.)

[517] DIXON 2022

követ.[518] A Viber kb. 250 millió, az iMessage kb. 1 Mrd aktív felhasználóval rendelkezett a 2023-as statisztikák alapján a vizsgált időszakban.[519]

4.1.2. Alkalmazásszolgáltatások letöltésére vonatkozó tendenciák

A vizsgált alkalmazásszolgáltatások letöltésének 2019-2021 közötti éves megoszlását is indokolt elemezni a 29. ábra alapján. Ezen jól látható, hogy a WhatsApp és a Messenger letöltésinek száma 2021-re jelentősen visszaesett, bezuhant 2020-hoz képest, amely álláspontom alapján nagyban köszönhető a Metaéval kapcsolatos EU-s adatvédelmi eljárásoknak és az így megjelenő negatív, személyes adatokkal való visszaélésgyanús magatartásnak, amely ügyében az EDPB is vizsgálatot folytatott, ami a későbbiekben ismertetésre is kerül.



29. ábra: Vizsgált alkalmazásszolgáltatások letöltésének éves megoszlása 2019-2021 között (millió felhasználó/év) (Szerk.: A szerző[520])

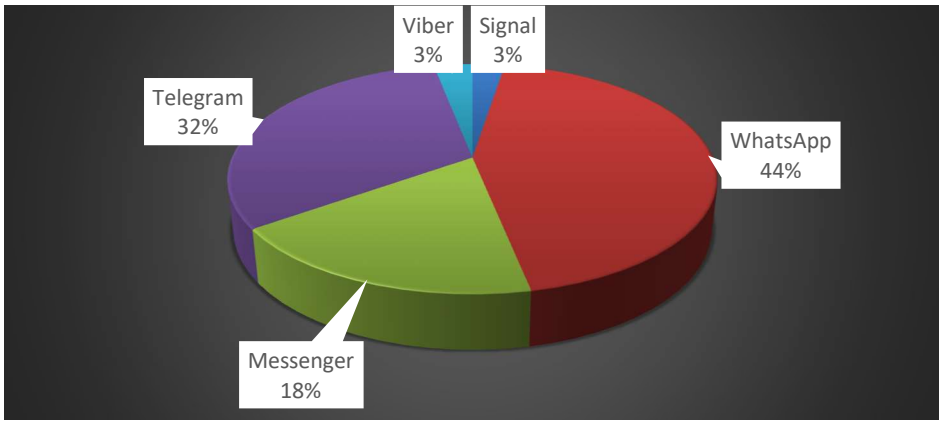
[518] RUBY, Daniel (2023): *86+ Telegram Statistics In 2023 (Usage, Revenue & Facts)*. DemandSage. Online: https://www.demandsage.com/telegram-statistics/ (Letöltés ideje: 2023. november 18.)

[519] DANIEL, Ch (2023a): *iMessage Revenue and Growth Statistics (2023).* SignHouse. Online: https://www.usesignhouse.com/blog/imessage-stats (Letöltés ideje: 2023. november 18.); DANIEL, Ch (2023b): *Viber Revenue and Growth Statistics (2023).* SignHouse. Online: https://www.usesignhouse.com/blog/viber-stats Letöltés ideje: 2023. november 18.)

[520] CURRY, David (2024a): *Messaging App Revenue and Usage Statistics (2024)*. BusinessofApps. Online: https://www.businessofapps.com/data/messaging-app-market/# (Letöltés ideje: 2024. február 26.); MARCH, Liz (2023): *Most Popular Messaging Apps Worldwide 2023*. SimilarWeb. Online:

A 29. ábra alapján látható, hogy a „sokkot” kiheverve mind a Messenger, mind pedig a WhatsApp a letöltések számában összeszedte magát, a WhatsApp drasztikus növekedést is produkált. Mind a Signal, mind pedig a Telegram a Meta szolgáltatásaival ellentétben 2021-ben is képes volt növelni letöltései számát, mint alternatíva, melyet tartott 2022-ben, a Viber letöltéseinek aránya további folyamatos csökkenése mellett. 2021-ben a Signalnál látható egy drasztikus kiugrás a letöltés számban, mely a későbbiekben részletezésre kerülő kriptográfiai környezetének is betudható a fokozódó, tudatos adatbiztonsági igény okán.

A fenti alkalmazásszolgáltatások 2023. január havi megoszlásának aránya a lenti 30. ábra alapján a második helyezett tekintetében eltérést mutat a piaci statisztikától, miszerint a piacvezető 51 millió letöltéssel, így 44%-os piaci részesedéssel a WhatsApp volt, azonban a második helyezett 36,7 millió letöltéssel, így 32%-kos piaci részesedéssel a Telegram, míg a Messenger csak a harmadik helyezett 21,3 millió letöltéssel, így 18%-os piaci részesedéssel. A Signal és a Viber 3-3%-kos részesedéssel az utolsók.



30. ábra: Vizsgált alkalmazásszolgáltatások letöltésének 2023. január havi megoszlása (Szerk.: A szerző[521])

Ország- vagy régióspecifikus vizsgálat alapján megállapítható, hogy a LINE 2023-ra a legnépszerűbb üzenetküldő platformmá vált Japánban, és a WeChat Kínában, bár ez utóbbi annak is köszönhető, hogy Kína betiltotta a Meta szolgáltatásait. Kelet-Európában és Afrikában a Viber produkálta a legtöbb letöltést, így versenyképes volt a WhatsApp-pal. Ázsiában és

https://www.similarweb.com/blog/research/market-research/worldwide-messaging-apps/ (Letöltés ideje: 2024. február 26.); CURRY, David (2024b): *Signal Revenue & Usage Statistics (2024)*. BusinessofApps. Online: https://www.businessofapps.com/data/signal-statistics/ (Letöltés ideje: 2024. február 26.)

[521] CECI, Laura (2024): *Most popular messenger apps worldwide in January 2024, by monthly downloads*. Statista. Online: https://www.statista.com/statistics/1263360/most-popular-messenger-apps-worldwide-by-monthly-downloads/ (Letöltés ideje: 2024. február 26.)

Latin-Amerikában a platformoknak egy része szuperalkalmazásokká alakult, amelyek számos funkciót kínálna az applikációkba ágyazódva. A források alapján „*A közeljövőben az üzenetküldő alkalmazások válhatnak az online vásárlás kiindulópontjává. A WeChat már bevezette az üzenetküldő alkalmazáson belül futó miniprogramok ökoszisztémáját, amelyek átirányíthatják a felhasználókat meghatározott vásárlási alkalmazásokhoz*."[522] Oroszországban 2021. Q2-ben a Telegram tovább növekedett.[523]

Az alfejezet alkalmazásszolgáltatások felhasználói trendjeire irányuló elemzése, 2030/31-ig tartó piaci tendenciáinak vizsgálata alapján bizonyítottá vált azok központi szerepének további növekedése a személyközi kommunikációs igények kiszolgálása tekintetében, a globális piac gazdasági volumenét az előrejelzések alapján 2029 és 2031 között mintegy 1,7-szeresére növelve. A statisztikák 2024-ben 3,42 Mrd, 2025-ben pedig 3,51 Mrd felhasználót vetítenek előre az alkalmazásszolgáltatások tekintetében globális szinten. Az adatok alapján Európában a piacvezetők jelenleg és a továbbiakban is a Meta szolgáltatásai (WhatsApp, Messenger), az iMessage, a Telegram, a Signal, és a Viber mellett.

4.2. Alkalmazásszolgáltatásokkal összefüggő adatvédelmi trendek, tendenciák

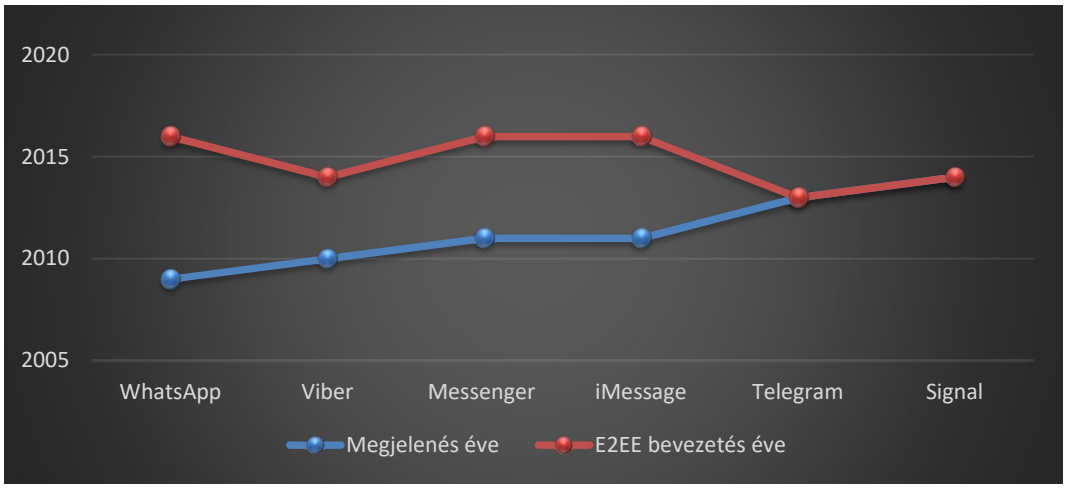
Az alfejezetben vizsgálatra kerülnek az adatvédelemmel összefüggő főbb mérföldkövek, akár az a technológia, azon belül is a kriptográfia fejlődésén, akár az a felhasználói adatbiztonsági igényeken alapul, akár jogpolitikai indíttatású. Szemléltetésre kerül, hogy azok milyen összefüggésben állnak a szolgáltatások keresletével, a biztonsági környezet változásával, illetve az LI hatékonyságával. Ennek keretében az LI hatékonysága szempontjából következtetések kerülnek levonásra a vizsgálattal érintett alkalmazásszolgáltatások kriptográfiai tulajdonságairól is.

4.2.1. Kriptográfiai trendek, tendenciák

Az elemzése során indokolt kitekintést tenni az új alkalmazásszolgáltatások megjelenési gyakoriságának és a kiberbiztonságot fokozó kriptográfiai eljárások technológiaváltásainak

[522] JACKIEWICZ, Magdalena (2023): *Chat app development trends that will shape the industry in 2023.* RST. Online: https://www.rst.software/blog/chat-app-development-trends-that-will-shape-the-industry-in-2023 (Letöltés ideje: 2023. március 25.)
[523] CURRY 2023

evolúciójára is. Néhány éve egyre több titkosított csevegőalkalmazás jelent meg, amelyek biztonságos kommunikációt ígértek, valamint 2016 óta az E2EE egyre elterjedtebb, így reagáltak a szolgáltatók a fokozott adatvédelemi igényekre. Az E2EE azt jelenti, hogy a kommunikáció *„tartalmát még a csevegőalkalmazást működtető vállalat sem látja.”*[524]

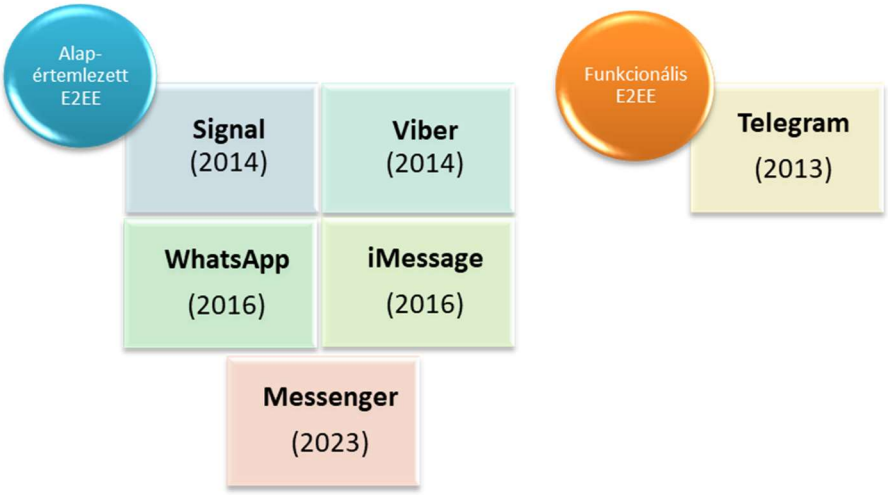


31. ábra: Vizsgált alkalmazásszolgáltatások és az E2EE bevezetésének összehasonlítása (Szerk.: A szerző.[525])

Az értekezés során vizsgált alkalmazásszolgáltatások és azok E2EE bevezetésének összehasonlítását a fenti 31. ábra hivatott szemléltetni. Folyamatosan jelennek meg új alkalmazások, amelyek a személyes adatvédelmet és a biztonságos kommunikációt helyezik előtérbe, de a piaci verseny és a fogyasztói igények e tekintetben is folyamatosan változnak. Egyes nagyobb platformok, mint például a Meta szolgáltatásai is folyamatosan javítják a kriptográfiai tulajdonságaikat, a felhasználók kommunikációjának biztonságosabbá tétele céljából, amely egyrészről a protokollok, algoritmusok fejlesztéséhez, másrészről az E2EE alkalmazásának általános elterjedéséhez vezetett. A Telegram, Signal, és a Viber is rendszeresen frissíti alkalmazásait és javítja a biztonsági szolgáltatásokat. Ugyanakkor más kisebb alkalmazásfejlesztők is kínálnak titkosított csevegőalkalmazásokat, amelyek megjelenése és frissítése változó ütemű. Az új titkosított alkalmazásszolgáltatások megjelenése és elfogadottsága számos tényezőtől függ, például az innovációs lehetőségektől, a keresleti igényektől, és az alkalmazásfejlesztők által felismert biztonsági kockázatoktól.[526] A 32. ábra szemléltetni hivatott, hogy mely alkalmazásszolgáltatások és mikortól biztosítják

[524] BÁNYÁSZ at al. 2022: 26.
[525] 4. számú melléklet: *A 4.lfejezet ábráinak forrásadattáblái*
[526] *The Most Secure Messaging Apps in 2023*. Avast. 2023. Online: https://www.avast.com/c-most-secure-messaging-apps (Letöltés ideje: 2024. február 27.)

alapértelmezetten az E2EE-t két végponti IKT eszköz közötti kommunikáció során, és melyek csak funkcionálisan.



32. ábra: Vizsgált alkalmazásszolgáltatások megoszlása alapértelmezett és funkcionális E2EE alapján (Szerk.: A szerző[527])

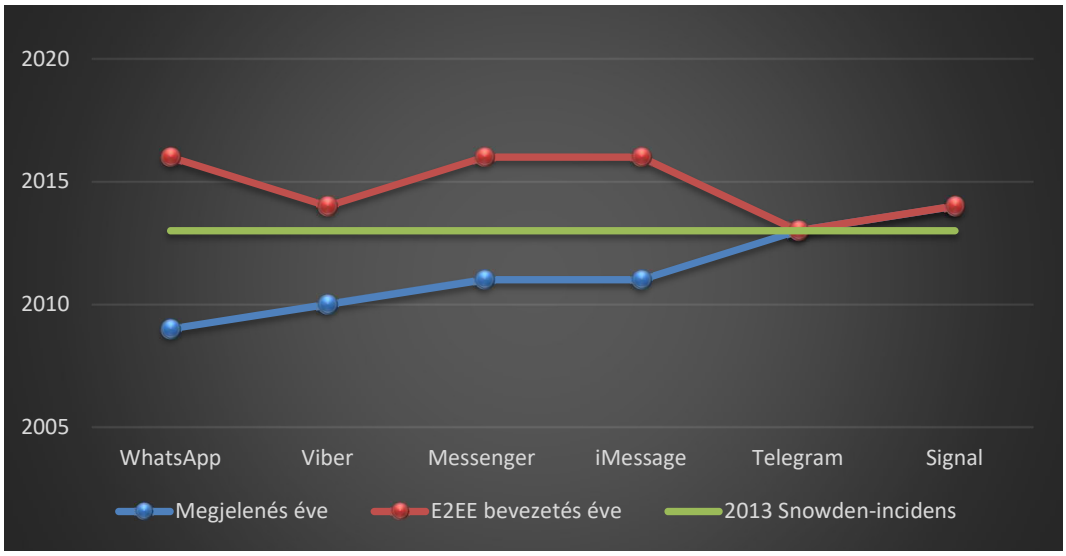
A fenti 32. ábra alapján megállapítható, hogy a vizsgált hat alkalmazásszolgáltatás közül öt mára alapértelmezetten biztosítja az E2EE-t a lakossági felhasználók kétoldalú kommunikációja során. A legutóbb a Meta aktiválta a funkciót a Messenger tekintetében 2023 decemberében,[528] melynek egyik oka a másik Meta szolgáltatás, a WhatsApp-pal való azonos szintű technológiai adatvédelmi környezet biztosítása, azonban álláspontom alapján piacszerző indíttatása is volt a kriptográfia fejlesztő intézkedésnek, hiszen annak keresletnövelő hatása is van egyben, melyet a következőkben kívánok bemutatni, bizonyítani. Az E2EE tényét marketing jelleggel a szolgáltatók például a VoIP hanghívások képernyőjén meg is jelenítik. Az iMessage bejelentette, hogy az iOS 17.4-es Apple szoftververziójával 2024 márciustól egy új kriptográfiai funkciót integrál az iMessage-be PQ3 néven. Az Apple szerint ez az innovatív és piacvezető kriptográfiai protokoll kiterjedt védelmet nyújt még a rendkívül kifinomult kvantumszámítások ellen is, olyan védelmet biztosítva, amely meghaladja az összes többi széles körben elterjedt üzenetküldő alkalmazást. Az Apple szerint a PQ3 bevezetése új mércét állít fel az üzenetküldő alkalmazások biztonsága terén, és tükrözi a vállalat határozott elkötelezettségét az adatvédelem és a biztonság iránt a kvantumszámítástechnika korszakában

[527] Lásd: 2. számú melléklet: *Az értekezés során vizsgált alkalmazásszolgáltatások kriptográfiai jellemzői*
[528] CRISAN, Loredana (2023): *Launching Default End-to-End Encryption on Messenger*. Meta. Online: https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/ (Letöltés ideje: 2024. február 26.)

is.[529] Tehát a Messenger 2023 decemberi alapértelmezett E2EE bevezetése, és az iMessage 2024-es „anti-kvantumszámítás” képességgel bíró E2EE PQ3 kriptográfiai protokollja alapján megállapítható, hogy a 2014/2016-os időszakot követően napjainkra ismét egy „titkosítási verseny” kezd kialakulni az alkalmazásszolgáltatások piacán, már előre reagálva az IKT környezet fejlődésének kvantumszámítás alapú innovációjára.

4.2.2. Felhasználói adatvédelmi trendek

Indokolt kitekinteni Edward Snowden, volt NSA[530] munkatárs által 2013-tól az USA Nemzetbiztonsági Közösségének jogellenes és tömeges „lehallgatási” ügyeinek kiszivárogtatása[531] (a továbbiakban: Snowden-incidens) és az E2EE általános bevezetésének összefüggéseire, amely idővonalát az alábbi 33. ábrára szemlélteti.



33. ábra: Vizsgált alkalmazásszolgáltatások és az E2EE bevezetésének és a Snowden-incidens időpontjának összehasonlítása (Szerk.: A szerző[532])

A 33. ábra szerinti idővonalak összevetése során megállapítható, hogy a Snowden-incidenst követően felgyorsult az E2EE alapértelmezett bevezetése az alkalmazásszolgáltatók

[529] HARDWICK, Tim (2024): *iOS 17.4 to Add This 'Groundbreaking' New Messaging Feature*. MacRumors. Online: https://www.macrumors.com/2024/02/23/ios-17-4-adds-groundbreaking-imessage-feature/ (Letöltés ideje: 2024. február 28.)
[530] NSA: National Security Agency – Nemzet Biztonsági Ügynökség
[531] Lásd: GREENWALD, Glenn (2014): *A Snowden-ügy - Korunk legnagyobb nemzetbiztonsági botránya.* Budapest: HVG Könyvek.
[532] 4. számú melléklet: *A 4.fejezet ábráinak forrásadattáblái*

tekintetében, kezdve a Viber és a Signal által. Álláspontom alapján ez egyfajta keresletfokozó üzletstratégiai döntésként is értelmezhető, így növelve a felhasználók bizalmát a szolgáltatások adatbiztonságossága iránt, egyben mérsékelve az esetleges keresletcsökkentést, amely a 4.2. alfejezetben ismertetésre került például a Meta szolgáltatásai tekintetében. Nem sokkal a 2013-as Snowden-incidenst követően 2014-ben megjelent az eleve E2EE-t integráló alternatív Signal egyfajta „keresleti-rést" kihasználva, amely felhasználói száma 2022 januárjában meghaladta a 40 milliót.[533] Időrendben megállapítható, hogy a Snowden-incidens követően a vizsgált alkalmazásszolgáltatások E2EE integrálási tendenciát kezdtek el produkálni.

A felhasználók által preferált adatvédelmi trendek között ki kell térni az Ekertv. szerinti alkalmazásszolgáltatások igénybevételének „számfüggetlenségére", azaz az anonimitás jóval nagyobb potenciáljára, mint a hírközlési szolgáltatások esetében. Az elektronikus hírközlési szolgáltatási jogviszony polgári jogi értelemben, olyan a Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.) által szabályozott szerződéses magánjogi jogviszony, amely a szolgálató és a szolgáltatást igénybe vevő magánszemély (a továbbiakban: előfizető), üzleti partner között létrejött szerződéses kereskedelmi jogügylet. Az Eht. szerinti rendkívül átfogóan szabályozott keretben a hírközlési szolgáltató az Eht. 154. § (2) bek. szerint „*az előfizetői szolgáltatás nyújtása körében kezeli az előfizető azonosításához szükséges*" taxatíve felsorol adatokat, többek között hatósági, bűnüldözési és az Nbtv. szerinti adatszolgáltatási célból. A kezelendő és átadandó adatok megléte azonban NI-ICS igénybevétele esetén igencsak korlátozott, már csak az előfizetői szerződés megkötése tekintetében is. Ezen kívül, mint az a fentiekben ismertetésre került, az Eht. 157. – 159. § szabályozza a kezelt forgalmi és számlázási adatok, továbbá a 159/A. § bűnüldözési, nemzetbiztonsági és honvédelmi célú adatmegőrzési kötelezettség ír elő implementálva a vonatkozó EU-s irányelvet. Az Ekertv. adatkezelésre vonatkozó fejezete jóval korlátozottabb az Eht.-nál, azonban a 13/B. § taxatíve felsorolja a külső engedélyhez kötött titkos információgyűjtésre jogosult szerv megkeresése esetén átadandó adatköröket az alkalmazásszolgáltatás igénybe vevője és az igénybevétel körülményei tekintetében. Ugyanis az alkalmazásszolgáltatások igénybe vevői, felhasználói[534] nem egyedileg megtárgyalt előfizetői szerződést kötnek a szolgáltatóval, hanem ráutaló magatartással, vagy kinyilatkoztatással elfogadják a Ptk. szerinti általános szerződési feltételeket (a továbbiakban: ÁSZF). Ezen szolgáltatásoknál magas az anonimitás lehetősége.

[533] MOXIE, Marlinspike (2016): *Signal on the outside, Signal on the inside*. Signal Online: https://signal.org/blog/signal-inside-and-out/ (Letöltés ideje: 2023. április 10.); CURRY 2024b
[534] Általános díjmentességük okán nem beszélhetünk előfizetőről.

Gondoljunk csak arra, hogy például a Messengernél hívószám, vagy más kontrollálható módon megadott személyes adat alapján adott felhasználó végtelen számú felhasználói, ún. hamis, vagy „fake" profilt hozhat létre, melyek egyben kihívást is jelentenek a nemzetbiztonsági, bűnüldöző szervek számára,[535] hiszen ezeket előszeretettel alkalmazzák például social engineering[536] során. A fentiek okán az anonimizálással szemben van egyfajta rendvédelmi nyomás például a vagyonelleni és a későbbiekben részletesebben áttekintésre kerülő EU-s jogalkotói szinten is vitákat gerjesztő gyermek- és ifjúságvédelem tekintetében. Ennek okán az alkalmazásszolgáltatók elkezdték a profilokat az e-mail cím mellett telefonszámhoz kötni, mely már áttételes módon alkalmasabb az egyedi felhasználó beazonosíthatóságára.

A részfejezet következtetéseként álláspontom alapján globális, de legalább is EU szinten követelményként kellene támasztani az alkalmazásszolgáltatók számára a felhasználó természetes személy regisztrációja során a mobil hívószám megadásának kötelezettségét azonosíthatósági célból. Ennek megőrzésére és szolgáltatására az alkalmazásszolgáltató kötelezett lenne, így a rendvédelmi szervek közvetetten ugyan, de hazai viszonylatban az Eht. mögöttes szabályai alapján már jóval hatékonyabban be tudnák azonosítani a tevékenységgel érintett természetes személyt, és például LI során egyértelműen köthető lenne hozzá a kommunikációja. Megállapítható, hogy a 2013-as Snowden-incidenst követően a vizsgált alkalmazásszolgáltatások E2EE integrálási tendenciát kezdtek el produkálni, egyben új „titkosított" alkalmazások piaci megjelenésével, a potenciális felhasználói bizalomvesztésre adott piaci válaszként a kereslet fenntartása, helyreállítása érdekében.

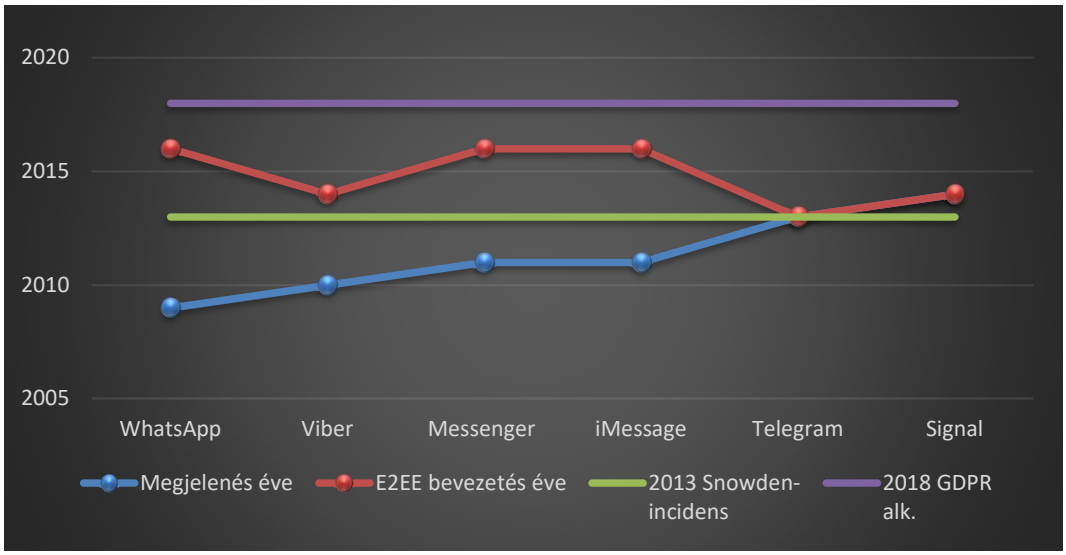
4.2.3. Normatív adatvédelmi tendenciák

A részfejezet vizsgálatának indokoltsága álláspontom alapján a GDPR alábbi preambulumbekezdéseinek idézésével a leghitelesebb „*(6) A gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét. A személyes adatok gyűjtése és megosztása jelentős mértékben megnőtt. […] (7) E fejlemények egy olyan szilárd és az*

[535] BÁNYÁSZ Péter (2017): Kiberbűnözés és közösségi média. *Nemzetbiztonsági Szemle*, 5(4), 69. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1634/946 (Letöltés ideje: 2024. február 27.); BÁNYÁSZ Péter (2018): Social engineering and social media. *Nemzetbiztonsági Szemle*, 6(1), 60-74. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1511/829 (Letöltés ideje: 2024. február 27.)

[536] Lásd: TÓTH, Tamás (2019): General description of social engineering and its place in information warfare. *National Security Review*, 5(1), 42-55. Online: https://doi.org/10.38146/BSZ.SPEC.2020.2.9 (Letöltés ideje: 2024. február 27.); TÓTH Tamás (2020): Az egyes social engeneering módszerek elhatárolása és rendszerezése. *Szakmai Szemle*, 18(1), 87-110. Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2020_1_szam.pdf#page=87 (Letöltés ideje: 2024. február 27.); DOBÁK – TÓTH 2021

eddiginél következetesebb uniós adatvédelmi keretet igényelnek, amelyet erős kikényszeríthetőség támogat, hiszen a bizalom megteremtése fontos a digitális gazdaság belső piaci fejlődéséhez. […] A természetes személyek, a gazdasági szereplők és a közhatalmi szervek számára a jogbiztonságot és a gyakorlati biztonságot fokozni kell." A GDPR alkalmazandóságának összefüggéseit a vizsgált alkalmazásszolgáltatások és az E2EE bevezetésével, a Snowden-incidens időpontjával a 34. ábra szemlélteti.



34. ábra: Vizsgált alkalmazásszolgáltatások és az E2EE bevezetésének, a Snowden-incidens időpontjának és a GDPR alkalmazandóságának összehasonlítása (Szerk.: A szerző[537])

A GDPR-on alapuló adatkezelési szabályok alapján az EDPB a norvég adatvédelmi szabályozó hatóság, azaz a GDPR szerinti érintett felügyeleti hatóság kezdeményezésére meghozott 2023. október 27-ei kötelező erejű döntése[538], valamint annak 2023. november 10-ei végrehajtási határozata[539] megállapította, hogy a Meta a Facebook és Instagram vonatkozásában az európai felhasználók személyes adatait a GDPR-ral ellentétes módon, viselkedésalapú célzott hirdetések érdekében kezelte és továbbította az EU kívülre, az USA-ba. Ezért a Metát 390 millió eurós pénzbírsággal sújtotta a GDPR ellenes adatkezelése okán. Az eljárások Maximilian

[537] 4. számú melléklet: *A 4. fejezet ábráinak forrásadattáblái*

[538] Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR) Adopted on 27 October 2023. EDPB. 2023. Online: https://edpb.europa.eu/system/files/2023-12/edpb_urgentbindingdecision_202301_no_metaplatformsireland_en_0.pdf (Letöltés ideje: 2024. február 27.)

[539] Végrehajtási utasítás a Meta Platforms Ireland Limited ügyében az ír adatvédelmi törvény (Data Protection Act) 133. cikk (9) bek. és 133. cikk (10) bek., valamint a GDPR 60. és 66. cikkei alapján. EDPB. 2023. Online: https://edpb.europa.eu/system/files/2023-12/nationalenforcementnotice202311_ie_metaplatformsireland_en_0.pdf (Letöltés ideje: 2024. február 27.)

Schrems osztrák állampolgár által 2013-ban benyújtott kereset nyomán indultak, amely szerint a Facebooknak nem volt jogalapja az ő és más európai polgár adatainak jogellenes kezelésére.[540] Schrems kezdeményezte, hogy az Ír adatvédelmi hatóság tiltsa meg a Facebook Írországban letelepedett leányvállalata számára a személyes adatainak az USA-beli illetőségű Facebook Inc-nek történő továbbítását, arra hivatkozva, hogy az USA-ban hatályban lévő adatvédelmi normák és gyakorlat nem biztosít a személyes adatok számára elégséges védelmet a hatóságok által folytatott - nemzetbiztonsági és bűnüldözési célú - megfigyelési tevékenységekkel szemben.[541] Az ügy kapcsán a Európai Parlament LIBE[542] Bizottsága által lefolytatott vizsgálat alapján „*még inkább hangsúlyossá vált az adatbiztonság és a személyes adatok védelme, mind a szabályzás szükségességének, mind a biztonság fokozására szolgáló technikai képességek megteremtése terén*."[543] Az ügy rávilágított a Meta adatvédelmi hiányosságaira, amely felhasználói számának csökkenését is eredményezte.

Az aktuális Európai trendek a személyes adatvédelem fokozására helyezik a hangsúlyt, akár ha a GDPR rendelkezéseit érvényre juttató a fent említett EDPB döntésre gondolunk a Schrems-ügyben. A döntés jogalapjául az EUB C-311/18. számú ügyben előzetes döntéshozatal iránti kérelem tárgyában 2020. július 16-án hozott ítélete[544] (a továbbiakban: Ítélet) szolgált, amely egyben érvénytelenítette az USA tekintetében a Bizottság az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló, 2016. július 12-i (EU) 2016/1250 bizottsági végrehajtási határozatot (a továbbiakban: „adatvédelmi pajzs határozat"). Azonban az Ítélet a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló 2010. február 5-i 2010/87/EU bizottsági határozatot (a továbbiakban: ÁSZF határozat) továbbra is érvényesnek minősítette. Az adatvédelmi pajzs határozat értelmében az USA az EU–USA adatvédelmi pajzs (Privacy Shield) az Unióból az öntanúsított USA-beli szervezetekhez továbbított személyes adatok tekintetében biztosított megfelelő szintű védelmet. Vagyis, ha olyan USA-beli szervezet felé történt az adattovábbítás, amely csatlakozott az adatvédelmi pajzshoz, a megfelelő védelmi szint biztosítottnak volt

[540] NEMES Tamás (2022): *Rekordösszegű bírságot kell fizetnie a Facebook anyacégének*. Világgazdaság. Online: https://www.vg.hu/nemzetkozi-gazdasag/2022/12/rekordosszegu-birsagot-kell-fizetnie-a-facebook-anyacegenek (Letöltés ideje: 2023. november 24.)
[541] C-311/18. sz. EUB
[542] LIBE: Civil Liberties, Justice and Home Affairs - Állampolgári Jogi, Bel-és Igazságügyi Bizottság
[543] DOBÁK Imre (2022): Társadalom – technológiai környezet – nemzetbiztonság. In DOBÁK Imre (szerk.): *Nemzetbiztonság a 21. század elején*. Budapest: Ludovika Kiadó. 56.
[544] C-311/18. számú, Data Protection Commissioner kontra Facebook Ireland és Maximillian Schrems ügyben az Európai Unió Bírósága 2020. július 16-án hozott ítélete [ECLI:EU:C:2020:559] Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:62018CJ0311&from=EN (Letöltés ideje: 2024. február 27.)

tekintendő a vonatkozó Bizottsági határozat alapján. Azonban a Bíróság fenti Ítéletében, annak 199-201. pontjai szerint megállapította, hogy a határozat megsértette a Charta összefüggésben értelmezett GDPR 45. cikkének (1) bekezdéséből eredő követelményeket, tekintettel arra, hogy a GDPR által megkövetelt védelmi szint az USA vonatkozásában az adatvédelmi pajzs által nem volt biztosított, így az adatvédelmi pajzs határozat érvénytelen. Schrems az Ítélet 55. pontja alapján arra hivatkozott, hogy „*az amerikai jog arra kötelezi a Facebook Inc-t, hogy a neki továbbított személyes adatokat az amerikai hatóságok, így a National Security Agency (NSA) és a Federal Bureau of Investigation (FBI) rendelkezésére bocsássa. Azt állította, hogy mivel ezeket az adatokat különböző megfigyelési programok keretében a Charta 7., 8. és 47. cikkével összeegyeztethetetlen módon használták fel, az ÁSZF határozat nem igazolhatja az említett adatoknak az Egyesült Államokba történő továbbítását*”.

Azonban Joe Biden amerikai elnök 2022. október 7-én aláírta az USA hírszerzési tevékenységére vonatkozó garanciák megerősítéséről szóló 14086 számú elnöki végrehajtási rendeletet[545] (a továbbiakban: Végrehajtási Rendelet), mely előírja azokat az intézkedéseket, amelyeket a 2022 márciusában bejelentett EU-USA adatvédelmi és adattovábbítási keretrendszerhez szükséges amerikai kötelezettségvállalások végrehajtása érdekében tesz. A transzatlanti adatforgalom kulcsfontosságú az EU-USA közötti gazdasági kapcsolatok szempontjából.[546] A végrehajtási rendelet elősegítheti, hogy a Bizottság a GDPR 45. cikke szerinti megfelelőségi határozat elfogadásával helyreállítsa az EU és az USA között a megfelelő védelmet biztosító transzatlanti adatáramlás korábban definiált kiemelt keretrendszerét. Azonban fontos kihangsúlyozni, hogy a Végrehajtási Rendelet nem állította helyre az EU-USA adatvédelmi pajzsot, így a szervezeteknek továbbra is olyan alternatív megoldásokat kell alkalmazniuk, mint a harmadik országba irányuló adattovábbításokra vonatkozó általános ÁSZF határozat, vagy a GDPR 47. cikke szerinti kötelező erejű vállalati szabályok.[547]A Bizottság az adatvédelmi pajzs kiváltására 2023. július 10-én elfogadta az EU-USA

[545] 14086 of October 7, 2022, on Enhancing Safeguards for United States Signals Intelligence Activities.

[546] DE at al. (2022): *President Biden Signs Executive Order on U.S. Intelligence Activities to Implement EU-U.S. Data Privacy Framework*. MayerBrown. Online: https://www.mayerbrown.com/en/perspectives-events/publications/2022/10/president-biden-signs-executive-order-on-us-intelligence-activities-to-implement-eu-us-data-privacy-framework (Letöltés ideje: 2024. február 27.)

[547] DR. DOMOKOS Márton - DR. HORVÁTH Anna Zsófia (2022): *Érkezik a Privacy Shield 2.0? – Nagyító alatt az USA hírszerzési tevékenységek fokozottabb védelméről szóló elnöki rendelete*. Jogi Fórum. Online: https://www.jogiforum.hu/blog-adatvedelem-10/2022/10/21/privacy-shield-2-0-nagyito-alatt-az-usa-hirszerzesi-tevekenysegek-fokozottabb-vedelmerol-szolo-elnoki-rendelete/ (Letöltés ideje: 2024. február 27.)

adatvédelmi keretre (a továbbiakban: DPF[548]) vonatkozó megfelelőségi határozatot,[549] mely megállapítja, hogy a DPF alapján az USA az EU-hoz a GDPR alapján mérhető megfelelő védelmi szintet biztosít az EU-ból amerikai vállalatoknak, kormányzati szerveknek továbbított személyes adatok tekintetében anélkül, hogy további adatvédelmi intézkedéseket kellene bevezetni. Ursula von der Leyen, a Bizottság elnökének nyilatkozta alapján: *„Az új EU-USA adatvédelmi keret biztonságos adatáramlást biztosít az európaiak részére, és jogbiztonságot teremt az Atlanti-óceán mindkét partján működő vállalatok számára."*[550] Azonban az EDPB a 2023. február 28-ai 5/2023. számú véleménye[551] alapján „*üdvösnek tartaná, ha a határozatnak nem csak a hatálybalépése, de már az elfogadása is attól függene, hogy minden amerikai hírszerző ügynökség elfogad-e aktualizált szabályzatokat és eljárásokat a 14086. sz. elnöki rendelet végrehajtására*."[552] Azonban az feltételezhető, hogy az NSA európai megfelelői szívesek elfogadnák a terrorizmus elleni küzdelemmel kapcsolatos releváns információkat, amennyiben olyan lehetőség adódna, hogy az illegálisan megszerzett adatok megakadályozhatnának egy újabb európai terrortámadást, minden európai kormány kétségtelenül a biztonságot választaná a magánélet védelmével szemben.[553]

A részfejezet következtetéseként megállapítható, hogy az EU jogpolitikai törekvései fokozzák az adatvédelmi intézkedések, az adatbiztonság szintjére irányuló elvárásokat. Ez az EU és USA kapcsolatokban az EU-ból az USA-ba irányuló adatkezelés terén is megnyilvánul, melynek aktuálisan a DPF szab megfelelési keretszabályokat. Azonban az értekezés vizsgálatához kapcsolódó releváns következtetés, hogy az EU-ból az USA-ba irányuló személyes adatkezelés GDPR ellenességét és annak újraszabályozását egyfeleől az USA nemzetbiztonsági célú titkos információgyűjtő tevékenységével kapcsolatosan feltárt adatvédelmi incidens jellegű tényezők

[548] DPF: Data Privacy Framework – adatvédelmi keret

[549] Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (notified under document C(2023)4745), OJ L 231, 20.9.2023, 118–229.

[550] *Protección de datos: la Comisión Europea adopta una nueva decisión de adecuación para la circulación de datos UE-EE.UU. con seguridad y confianza.* Comisión Europea. 2023. Online: https://ec.europa.eu/commission/presscorner/detail/es/ip_23_3721 (Letöltés ideje: 2024. február 27.)

[551] 5/2023.sz. vélemény a személyes adatoknak az EU–USA adatvédelmi keret szerinti megfelelő védelméről szóló európai bizottsági végrehajtási határozat tervezetéről. EDPB. 2023. Online: https://edpb.europa.eu/system/files/2023-09/edpb_opinion52023_eu-us_dpf_hu.pdf (Letöltés ideje: 2024. február 27.)

[552] *Az Európai Adatvédelmi Testület üdvözli az EU–USA adatvédelmi keret módosításait, de aggályait továbbra is fenntartja*. EDPB. 2023. Online: https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_hu (Letöltés ideje: 2024. február 27.)

[553] SABJANICS, István (2022): Rebooting US-EU Data Transfers in the Pipeline - The Resurrection of the Acclaimed Privacy Shield. *Hungarian Yearbook of International Law And European Law*, 10(1), 215. Online: https://www.elevenjournals.com/tijdschrift/HYIEL/2022/1/HYIEL_2666-2701_2022_010_001_012.pdf (Letöltés ideje: 2024. július 7.)

indukálták. A kapcsolódó kutatási eredményekkel egyetértve „*Anélkül, hogy túl pesszimistának akarnánk tűnni, a legjobbat kell remélnünk az újonnan frissített adatvédelmi pajzstól, de a bizalom kétirányú út. Az amerikai hatóságok korábbi magatartásának fényében jobb, ha kezdettől fogva éberek maradunk, és hosszú távon is éberen figyeljük a folyamatokat*."[554]

4.3. Alkalmazásszolgáltatásokkal összefüggő biztonsági kihívások, tendenciák és válaszintézkedések a nemzetközi térben

Mint, ahogy az értekezés témaválasztásának indoklása és az elvégzett kutatási cselekmények során is felmerült az alkalmazásszolgáltatások dinamikusan bővülő felhasználói köre nem minden esetben jogkövető magatartás során él a szolgáltatások adta lehetőségekkel és élvezi a személyes adatok, magánélet és magántitok védelméhez fűződő alapvető jogok biztosítására hivatott normatív és technológiai adatvédelmi intézkedéseket. A határokon átnyúló nemzetbiztonsági és bűnüldözési célú titkos információgyűjtés személyes adatvédelmi aspektusai a DPF előzményei során is felmerültek. A titkosított kommunikációt biztosító alkalmazásszolgáltatások jogellenes célú felhasználására számos nemzetközi esettanulmány is szolgál, akár az uniós jogalkotás szintjét elérő online gyermekvédelem kapcsán, melyek bemutatására jelen alfejezetben kerül sor, a nemzetköz LI együttműködések, és az alkalmazásszolgáltatók hatósági adatszolgáltatási attitűdjének vizsgálatával egyetemben.

4.3.1. Az alkalmazásszolgáltatások jogellenes felhasználásra vonatkozó nemzetközi esettanulmányok

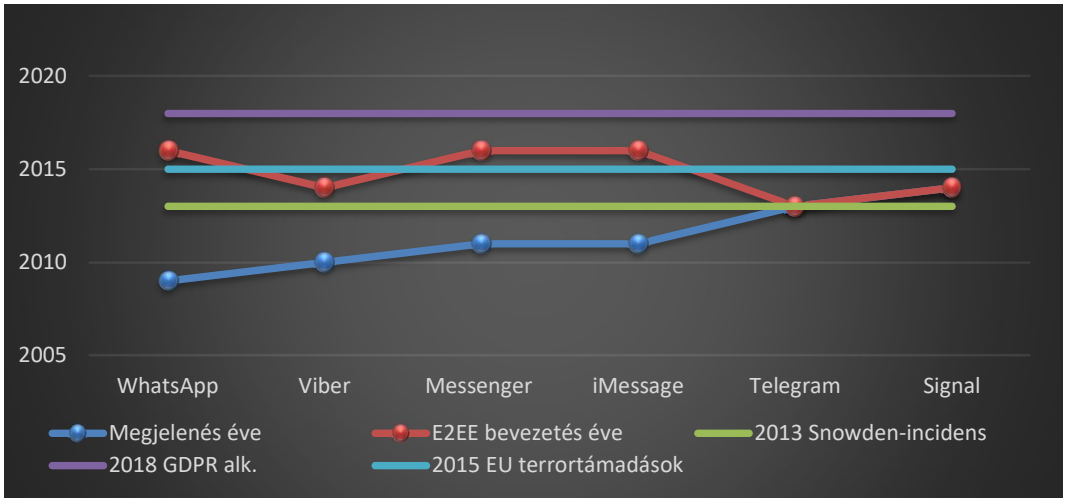
A szakirodalom alapján megállapítható a nemzetközi terrorizmus 2015 utáni diverzifikációja, azaz hálózatalapúsága az ISIS felett aratott katonai győzelmet követően.[555] Gilles de Kerchove, az Unió egykori terrorellenes koordinátora már 2016 végén felhívta a figyelmet arra, hogy az EU-ból az ISIS-hez csatlakozó, majd Európába visszatérő idegen harcosok egy része hamis személyazonossággal az Amniyattól[556] kapott terrorveszélyt megvalósító feladattal tért haza, irányító tisztjeikkel pedig titkosított kommunikációt biztosító alkalmazásokon keresztül

[554] SABJANICS 2022: 215

[555] HANKISS Ágnes (2019): Az Iszlám Állam titkosszolgálata - Diverzifikációs Folyamatok. *Arc És Álarc*, 3(1), 121. Online: http://real.mtak.hu/112356/1/HAMVAS_2019_1.pdf (Letöltés ideje: 2023. december 8.)

[556] Az ISIS titkosszolgálatától, arabul az Emni.

tartották a kapcsolatot.[557] Vélhetően az alkalmazásszolgáltatások a 21. század legelterjedtebb infokommunikációs szolgáltatásaivá váltak, amelyeket jogsértő cselekmények megvalósítása során például a terror-, bűnszervezetek is alkalmaznak kommunikációs csatornaként. Ezt támasztja alá a francia terrorelhárítás vizsgálata is, miszerint 2016 augusztusában az ISIS terrorszervezet két terroristája a 19 éves Adel Kermiche és Abdel-Malik Petitjeanaz meggyilkolták a 86 éves Jacques Hamelt, az Észak-franciaországi Saint-Étienne-du-Rouvray-i plébánia tiszteletesét. A terroristák az E2EE-t integráló Telegram alkalmazásszolgáltatáson keresztül kommunikáltak, illetve koordinálta tevékenységüket az ISIS.[558] A Nemzetközi Terrorelhárítási Intézet egy 2018-as beszámolója alapján az ISIS tekintetében a toborzás, a logisztika, a finanszírozás, maga a műveleti tevékenység is konspirált hálózatalapú szervezeti modellen alapult.[559] Tekintettel a decentralizált, hálózatalapú, zárt terrorista sejtekre és a konspirált, alacsony késleltetési idővel bíró utasítási, jelentési lánc széles földrajzi kiterjedésére, azaz globalizáltságára, a kapcsolattartás elsődlegesen személytelen módon kell/ kellett, hogy megvalósuljon, mely legköltséghatékonyabb megoldásai közé tartoznak az titkosított online kommunikációt biztosító alkalmazásszolgáltatások, egyéb platformok.



35. ábra: Vizsgált alkalmazásszolgáltatások és az E2EE bevezetésének, a Snowden-incidens időpontjának, a GDPR alkalmazandóságával és a 2015-től kezdődő Európai terrortámadások kezdőidőpontjának összehasonlítása (Szerk.: A szerző[560])

[557] BLANCHE, Ed (2017): *The Arab Weekly*. UPI. Online: https://www.upi.com/Top_News/Voices/2017/03/20/Islamic-States-killing-machine-focused-on-sleeper-cells/6291490033456/ (Letöltés ideje: 2023. december 8.)
[558] HADDAD, Margot - HUME, Tim (2016): *Killers of French priest met 4 days before attack*. CNN. Online: http://edition.cnn.com/2016/08/01/europe/france-church-attack-telegram/index.html (Letöltés ideje: 2023. december 8.)
[559] DR. AZANI, Eitan (2018). *Global Jihad – The Shift from Hierarchal Terrorist Organizations to Decentra-lized Systems*. Herzlia: International Institute for Counter-Terrorism. 12-15. Online: https://www.ict.org.il/images/Global%20Jihad%20%E2%80%93%20The%20Shift%20from%20Hierarchal.pdf (Letöltés ideje: 2024. január 9.)
[560] 4. számú melléklet: *A 4. fejezet ábráinak forrásadattáblái*

A 2015-től kezdődő európai terrortámadások kezdőidőpontjának összehasonlítását a vizsgált alkalmazásszolgáltatások, az E2EE bevezetésével, a Snowden-incidens időpontjával és a GDPR alkalmazandóságával a 35. ábra szemlélteti. Ez alapján a 2015-ös európai terrorhullám idején az alkalmazásszolgáltatások már E2EE integráltak, így korlátozva az LI-t. A szakirodalom alapján „*Élhetünk bárhol a Földön, legyen az egy világi nagyhatalom vagy egy kis nemzetállam területe, a globalizáció árnyoldalának köszönhetően olyan veszélyforrásokkal kell szembenéznünk, amely a bolygón élő összes ember életét, testi épségét és joggyakorlását sérti vagy veszélyezteti.*”[561] Ezt a megállapítást a hálózat alapú transznacionális terrorizmuson túl erősíti a szervezett bűnözés globalizációja, gondoljunk akár csak a kiberbűnözésre, illetve az elektronikus információs rendszer felhasználásával elkövetett bűncselekményekre, amelyek megvalósítását elősegíti az infokommunikáció globalizációja. Ennek elektronikus hírközlési értelemben vett infrastrukturális „kiszolgálója” a globális konvergenciát és konnektivitást biztosító internetszolgáltatás, mely egyben az EU stratégiai célkitűzése is – nyilván a jogkövető felhasználók számára, de látható a visszaélés szerű felhasználás. Az Europol 2021 évi SOCTA jelentése alapján a kiberbűnözés (elsősorban az online csalások) az egyik legelterjedtebb bűnelkövetési formává vált. „*Gyakorlatilag minden bűncselekmény megvalósítása tartalmaz néhány online komponenst, például olyan digitális megoldásokat, amelyek megkönnyítik a bűncselekmények során végbement kommunikációt*.”[562] A Telegramot az USA-beli Proud Boys nevű szélsőjobboldali erőszakszervezet is felhasználta antiszemita események koordinációjára.[563] Írország Stratégiai Párbeszéd Intézetének egy vizsgált 2021-es jelentése szerint az ír szélsőjobboldali csoportok Telegramon keresztül továbbított üzeneteinek száma a 2019-es 801-ről 2020-ra mintegy 60.377-re nőtt.[564] Egy aktuális 2023. március 13-ai ENSZ szakértői beszámoló szerint „*A mianmari katonai junta online terrorkampányt szervez, és a közösségi média platformjait fegyverezi fel a demokratikus ellenzék leverésére*.”[565]

---

[561] KOVÁCS István (2023): A nemzetközi szervezett bűnözés statisztika elemzése a SOCTA és Eurostat rendszerekben. *Belügyi Szemle*, 71(5), 851. Online: https://doi.org/10.38146/BSZ.2023.5.6 (Letöltés ideje: 2023.december 8.)

[562] *European Union Serious and Organised Crime Threat Assessment* (SOCTA) 2021. Europol, 2021. 32. Online: https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf (Letöltés ideje: 2023. december 8.)

[563] *Proud Boys celebrate Trump's 'stand by' remark about them at the debate* New York Times. 2020. Online: https://www.nytimes.com/2020/09/29/us/trump-proud-boys-biden.html (Letöltés ideje: 2023. december 25.)

[564] GALLAGHER, Aoife - O'CONNOR, Ciarán (2021): *Layers of Lies: A First Look at Irish Far-Right Activity on Telegram.* London: Institute for Strategic Dialogue. 7-8. Online: https://www.isdglobal.org/wp-content/uploads/2021/04/Layers-of-Lies.pdf (Letöltés ideje: 2023. december 25.)

[565] ANDREWS, Thomas at al. (2023): *Myanmar: Social media companies must stand up to junta's online terror campaign say UN experts*. Genewa: The Office of the High Commissioner for Human Rights, United Nations Online: https://www.ohchr.org/en/press-releases/2023/03/myanmar-social-media-companies-must-stand-juntas-online-terror-campaign-say (Letöltés ideje: 2023. december 26.)

A 2021-es Mianmari katonai államcsínyt követő emberi jogi visszaélések során betöltött szerepe okán az ENSZ Emberi Jogi Főbiztosának Hivatala továbbá felszólította a Telegramot, hogy tegyen lépéseket az emberi jogi visszaélések azonosítására, megelőzésére és enyhítésére a platformján, mely legalább 13 szélsőséges „katonabarát" fiókot blokkolt.[566] A Telegram kapcsán a médiában fellelhető gyermekpornográf tartalmak Új-Delhiben történő terjesztése.[567] Az alkalmazásszolgáltatások konspiratív kommunikációs csatornát biztosíthatnak továbbá az illegális áruk és szolgáltatások kereskedelmének, így az illegális fegyverkereskedelem, a proliferáció számára is. Bács Zoltán György kutatási alapján „*Ugyanakkor van egy rendkívül sajátos terület, a nemzetközi szervezett bűnözés egyik különösen veszélyes ága, ahol az ágazati, stratégiai konvergencia megfigyelhető. Ez pedig a nemzetközi kábítószer-bűnözés és a terrorfinanszírozás*."[568] A fenti kihívásokra természetesen mind jogpolitikai, mind technológiai intézkedésekkel próbálnak reagálni az egyes államok nemzetbiztonsági, bűnüldözési célú LI szervei, akár állami, akár nemzetközi együttműködési szinten. Dobák Imre következtetései alapján „*a biztonság területén látható egymásrautaltság felvetette a nemzeteken túlmutató közös gondolkodás, az együttműködés és az információk megosztásának szükségességét. Gondolhatunk itt a már évtizedek óta meglévő, eltérő tagságot felölelő titkosszolgálati együttműködési formákra (például a Five Eyes[569] együttműködés, Berni Klub[570]), de idesorolhatóak az elmúlt évtizedekben létrejött intézményesített együttműködési formák [például Interpol, Europol]. Ezek egy része a terrorizmushoz kapcsolódó információmegosztást szolgálja, elfogadva azt, hogy az együttműködésekben érintett nemzetek egyéb hírszerzési területei a tagállami szuverenitás, a nemzeti érdekek érvényesítése és védelme érdekében működnek.*"[571] A fentiek alapján indokolt kitekintést tenni a nemzetközi LI együttműködések vertikumára a következőkben.

---

[566] ANDREWS 2023

[567] MIHINDUKULASURIYA, Regina (2019): *Rape videos, child porn, terror — Telegram anonymity is giving criminals a free run - The end-to-end encryption provided by social media app Telegram has paved the way for a host of illegal activities*. The Print. Online: https://theprint.in/tech/rape-videos-child-porn-terror-telegram-anonymity-is-giving-criminals-a-free-run/307959/ (Letöltés ideje: 2023. december 26.)

[568] BÁCS Zoltán György (2022): Viribus Unitis, avagy civil professzionális konvergencia a 21. században. In DOBÁK Imre (szerk.): *Nemzetbiztonság a 21. század elején*. Budapest: Ludovika Kiadó. 49.

[569] Az Amerikai Egyesült Államok, az Egyesült Királyság, Ausztrália, Kanada és Új-Zéland részvételével megvalósuló technikai jellegű hírszerzési együttműködés. Hivatalos nevén ez nem más, mint az UKUSA (United Kingdom, United States of America) együttműködés LI specifikus kerete, amely második világháború alatt az Egyesült Királyság és az Amerikai Egyesül Államok között létrejött hírszerzési együttműködés, amelynek napjainkban már Ausztrália, Kanada és Új-Zéland is tagja.

[570] 1971-ben létrehozott, az Európai Unió, Norvégia és Svájc biztonsági és hírszerző szolgálatai vezetőinek részvételével megvalósuló informális titkosszolgálati fórum.

[571] DOBÁK Imre (2022): A nemzetbiztonság 21. századi értelmezése és jellemzői. In DOBÁK Imre (szerk.): *Nemzetbiztonság a 21. század elején*. Budapest: Ludovika Kiadó. 21.

A részfejezet következtetéseként megállapítható, hogy a fokozódó személyes adatvédelmi előírások következtében megjelenő technológiai válaszlépések, azaz az alkalmazásszolgáltatások kriptográfiai tulajdonságainak fejlődése egyben a jogellenes tevékenységek számára is konspiratív lehetőségeket biztosít, melyek a feldolgozott szakirodalom, esettanulmányok alapján a terrorizmus, szervezett bűnözés, extrémizmus, emberiesség elleni bűncselekmények, proliferáció, és végsősoron a gyermekpornográfia során online terjesztés, kapcsolattartás céljából is számos esetben igénybevételre kerültek. A titkosított kommunikációt biztosító alkalmazásszolgáltatások jogellenes tevékenységben történő kommunikációs célú felhasználásának kiemelt társadalmi jelentőségét az ENSZ Emberi Jogi Főbiztosának fellépése is jelzi. Azonosítható a köz- és nemzetbiztonsági érdeksérelem, azaz az elvégezett esettanulmányfeldolgozás alapján bizonyítást nyert, hogy az alkalmazásszolgáltatásokkal kapcsolatos nemzetközi normatív adatvédelmi és elektronikus információbiztonsági környezet fejlődése hátrányosan érinti az azokon végbement kommunikáció LI-jének technológiai hatékonyságát, tehát a gyakorlat altámasztja az Ekertv. szerinti alkalmazásszolgáltatások LI képességének létjogosultságát, indokoltáság.

4.3.2. Az alkalmazásszolgáltatási LI nemzetközi együttműködési vetületei

Az alkalmazásszolgáltatási LI nem katonai (polgári) jellegű nemzetközi együttműködési formáinak vizsgálatát érdemes a tradicionálisan globális szinten is számottevő technikai információgyűjtő kapacitással bíró államokkal kezdeni, így elsősorban az USA-val. Az NSA a FISA[572] módosításairól szóló törvény (a továbbiakban: FAA[573]) 702. szakasza alapján 2008

[572] The Foreign Intelligence Surveillance Act (FISA) of 1978. Public law 95-511, 92 Stat. 1783. Online: https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf (Letöltés ideje: 2024. február 28.); Lásd: MCADAM, James G. (2026): *Foreign Intelligence Surveillance Act (FISA): An Overview.* Glynco: Federal Law Enforcement Training Centers. Online: https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf (Letöltés ideje: 2024. február 28.)

[573] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008. Public law 110-261, 122 Stat. 2436. Online: https://www.govinfo.gov/content/pkg/STATUTE-122/pdf/STATUTE-122-Pg2436.pdf (Letöltés ideje: 2024. február 28.); Lásd: LIU, Edward C. (2021): Foreign Intelligence Surveillance Act (FISA): An Overview. Congressional Research Service. Online: https://sgp.fas.org/crs/intel/IF11451.pdf (Letöltés ideje: 2024. február 28.)

után kialakította és működteti a „PRISM" fedőnevű downstream[574] jellegű LI rendszerét,[575] amely a közösségi média-, alkalmazásszolgáltatókkal (például Meta, Apple) együttműködve magas LI potenciállal bír a szolgáltatásaik keretében végbement kommunikáció ellenőrzése terén.[576] Azonban a PRISM hatékonysága kapcsán felvetődik az E2EE LI-t korlátozó, ellehetetlenítő szerepe. Természetesen az USA finanszírozási oldalról jóval jelentősebb kapacitással bír a rendkívül erőforrásigényes rejtjelfejtő eljárások kidolgozása terén is. A Snowden által kiszivárogtatott iratok megmutatták, „*hogy az amerikai kormány az Európai Unió számos hivatalát megzavarta, és legalább harmincnyolc külföldi nagykövetség után kémkedett*"[577], továbbá „*akár hétmilliárd embert is megfigyelnek, rögzítik az adataikat*"[578]. A PRISM által gyűjtött adatokhoz az információk szerint angolszász nemzetbiztonsági célú bilaterális nemzetközi együttműködés keretében hozzáfér az Egyesült Királyság GCHQ[579] LI szerve is. Az angolszász vonalon tovább haladva azonosítható egy nagykapacitású LI eljárás, mégpedig a nemzetközi internetforgalom globális optikai hálózatairól kicsatolt kommunikáció totális ellenőrzése, azaz a GCHQ által a multilaterális Five Eyes angolszász nemzetközi LI

[574] „*A hírközlő rendszereken folytatott kommunikáció ellenőrzésének – az amerikai külföldi irányú hírszerzési szakterminológia alapján – két típusa különböztethető meg: a „downstream" és az „upstream" jellegű információgyűjtés elhatárolásával. A „downstream" információgyűjtés a hírközlési szolgáltatókkal történő együttműködésen alapuló eljárás, amely a rendszereikben megjelenő adatokra fókuszál. A folyamatban az érintett információgyűjtő szerv küldi meg a szükséges azonosítót az elektronikus kommunikációs szolgáltatónak, majd ezt követően egyfajta szolgáltatói közreműködéssel, adatigénylés során történhet az információgyűjtés*". TÓTH 2020: 50

[575] A PRISM-t megelőzően az USA első olyan programja, amely az addig csak piaci-kereskedelmi oldalon használt adatfúziós megoldásokat ültette át az állami (nemzetbiztonsági-bűnüldözési) környezetbe a 2003. október 20-tól elindult M.A.T.R.I.X. (Multistate AntiTerrorism Infomation Exchange – Többállami Terrorizmusellenes Információcsere) program volt. Lásd: SABJANICS István (2013): Adatvédelem és terrorellenes intézkedések az Egyesült Államokban: A MATRIX modellkísérlet története és visszhangjai. In GERENCSÉR Balázs Szabolcs (szerk.): *Modellkísérletek a közigazgatás fejlesztésében: Az ún. „pilot projektek" határai elméletben és gyakorlatban.* Budapest: Pázmány Press. 79-88. Online: https://jak.ppke.hu/uploads/articles/227518/file/modellkiserletek_kotet.%20_0515pdf.FINAL.pdf (Letöltés ideje: 2024. július 13.)

[576] BRAUN, Stephen - FLAHERTY, Anne – GILLUM, Jack – APUZZO, Matt (2013): *Secret To Prism Program: Even Bigger Data Seizure.* AP. Online: https://web.archive.org/web/20130910083307/http://bigstory.ap.org/article/secret-prism-success-even-bigger-data-seizure (Letöltés ideje: 2024. február 28.); *NSA slides explain the PRISM data-collection program.* Washington Post. 2013. Online: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (Letöltés ideje: 2024. február 28.)

[577] DR. IFJ. LOMNICI Zoltán (2024): Kormányzati szivárogtatások és következményeik az Egyesült Államokban. AlaptörvényBlog. Online: https://alaptorvenyblog.hu/kormanyzati_szivarogtatasok_es_kovetkezmenyeik_az_egyesult_allamokban.html Letöltés ideje: 2024. július 7.)

[578] ALMÁSI Miklós (2016): A láthatatlan hatalmak. *Magyar Tudomány*, 177(6), 686. Online: https://epa.oszk.hu/00600/00691/00153/pdf/EPA00691_mtud_2016_06_681-689.pdf (Letöltés ideje: 2024. július 7.)

[579] GCHQ: Government Communications Headquarters – Kormányzati Kommunikációs Központ

együttműködés keretében üzemeltett „TEMPORA" fedőnevű upstream[580] DPI képesség,[581] melynek szintén korlátja az E2EE, amennyiben az nem kerül rejtjelfejtésre. „*Itt – a kiszivárgott adatok szerint – 200 darab, egyenként 10 Gb/s adatátviteli sebességű optikai kábelen (ezek közül egy időben legalább 46-on) átfolyó összes információt kicsatolják és feldolgozzák.*"[582] Az Egyesült Királyságban 2023-ban ismét felvetődött az IPA[583] módosítása a fenti E2EE kriptográfiával kapcsolatos biztonsági kihívások okán, mely értelmében többek között „*a szolgáltatóknak azonnali hatállyal intézkedniük kell, ha a biztonsági funkciók letiltására irányuló kérést kapnak a minisztériumtól […]"* A javaslast a szolgáltatók oldaláról ellenreakciókat váltott ki, hivatkozva arra, hogy a titkosítási funkciók további korlátozhatóság okán az Egyesült Királyság digitális politikája nem nyújtaná a nemzetközileg elvárt személyes adatbiztonsági szintet.[584] Ennek a 4.3.3. részfejezet alapján az elektronikus hírközlési, vagy az alkalmazásszolgáltatók által EU-n kívüli adatkezelés tekintetében komoly relevanciája van, már ha csak a DPF előzményeire tekintünk.

Az USA-nál maradva szükséges megvizsgálni az USA bilaterális LI célú együttműködési lehetőségeinek keretrendszerét is. USA Kongresszusa az FAA-hoz köthetően 2018. március 23-án fogadta el a CLOUD[585] Act-et azzal a céllal, hogy javítsa az USA-beli és a külföldi hatóságok bűnüldözési célú végrehajtási együttműködését. A CLOUD Act egyrészről kötelezi például az USA székhelyű alkalmazásszolgáltatókat az Eht.-hoz hasonló adatmegőrzésre. Másfelől viszont feljogosítja az USA Igazságügyi Minisztériumát olyan más partnerországok kormányzati, igazságügyi szervével való bilaterális végrehajtási megállapodások megkötésére, amelyek alapján a partnerország jogosult LI szervével közvetlen együttműködési kötelezettség terheli az USA székhelyű szolgáltatót (például Meta, Apple). Így szolgáltatói együttműködés keretében az LI-vel érintett felhasználóval és annak kommunikációjával kapcsolatban kezelt

[580] Az „upstream" típus, angolszász terminológia szerinti technikai információgyűjtés pedig – nemzeti és nemzetközi szinten – a jelentősebb gerinchálózati csomópontokon, létesítményeken áthaladó kommunikáció ellenőrzésére irányul, amely már felöleli a hang, az írás és a multimédia (kép, videó, élőstream stb.) típusú közlemények ellenőrzését is. DOBÁK Imre (2017): Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében. *Hadmérnök,* 12(2), 240. Online: http://hadmernok.hu/172_19_dobak.pdf (Letöltés ideje: 2024. február 28.)

[581] *Why we're taking the UK government to court over mass spying*. Amensty International. 2020. Online: https://www.amnesty.org.uk/why-taking-government-court-mass-spying-gchq-nsa-tempora-prism-edward-snowden (Letöltés ideje: 2024. február 28.)

[582] KOVÁCS 2021: 125

[583] Investigatory Powers Act 2016. Online: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted (Letöltés ideje: 2024. február 28.)

[584] DÖMÖS 2023

[585] Clarifying Lawful Overseas Use of Data Act (CLOUD Act) March 23, 2018. Public law 115–141, Stat. 1213-25. Online: https://www.govinfo.gov/content/pkg/PLAW-115publ141/pdf/PLAW-115publ141.pdf (Letöltés ideje: 2024. február 28.)

adatokat az USA székhelyű szolgáltatónak át kell adni a külföldi állam LI szervének, annak megkeresése esetén. A CLOUD végrehajtási megállapodás hatálya alá tartozó szolgáltatók olyan magánjogi jogalanyok, amelyek lehetővé teszik a felhasználók számára, hogy hírközlő hálózaton, vagy egyéb elektronikus információs rendszeren keresztül kommunikáljanak és feldolgozzák vagy tárolják az elektronikus adatokat.[586] Egy CLOUD végrehajtási megállapodás megkötéséhez azonban egy inverz GDPR-DPF szabályozási megfelelőségi vizsgálat lefolytatása szükséges, mely értelmében a partnerország LI-re vonatkozó szabályozásának meg kell felelnie az USA nemzeti jogszabályaiban is érvényesülő elvárásoknak például az engedélyezés, adatkezelés stb. terén. Jelenleg csak két állammal van ilyen megállapodása az USA-nak, mégpedig Ausztráliával, és a Brexitet követően az Egyesült Királysággal, így itt is érvényesül a tradicionális, bizalmi alapú angolszász multilaterális tengely.[587] Egy a CLOUD Act alkalmazásnak tapasztalatait vizsgáló EU-s tanulmány ezt kritikaként értékeli.[588] A tanulmány szerint a CLOUD Act és a GDPR szabályozása okán fellépő mélyebb aszimmetriák orvosolása a DPF előkészítése során megtörtént, mely során közeledni kezdett egymáshoz az USA-beli és az EU-s adatkezelési szabályozás, melyet szintén gazdasági okok indukáltak a személyes adatok transznacionális kezelhetősége érdekében.

Globális szintű multilaterális bűnüldözési célú tradicionális együttműködést valósít meg az 1923. szeptember 07-én alapított Interpol[589], mely fő profilja az információ-megosztás és koordináció egyfajta nemzetközi információfúziós központként működve, elsődlegesen a terrorizmus, a kiberbűnözés, valamint a szervezett bűnözés területeire összpontosítva[590], az emberkereskedelem, csempészet és korrupciós bűncselekmények mellett. Az EU-t vizsgálva újgenerációs hírközlési hálózatok tekintetében a 3.1.3. részfejezet alapján megállapítható, hogy az EU már szabvány szintjén fokozta a technológiai biztonság, azaz a kiberbiztonság követelményeit, elsősorban a titkosság, az anonimizálás tekintetében. Azonban a fentiekben rejlő kockázatot, azaz az adatvédelem/biztonság értékduálja egyensúlyának kibillenési veszélyét az Europol bűnüldözési célú LI aspektusából már 2019-ben felismerte. „*Az 5G*

[586] *Regarding CLOUD Act Executive Agreements*. U.S. Department of Justice Criminal Division. Online: https://www.justice.gov/criminal/criminal-oia/regarding-cloud-act-executive-agreements (Letöltés ideje: 2024. február 28.)
[587] *The CLOUD Act*. European Union Agency for Criminal Justice Cooperation. 2022. Online: https://www.eurojust.europa.eu/publication/cloud-act (Letöltés ideje: 2024. február 28.)
[588] *The CLOUD Act*. Eurojust. 2022. Online: https://www.eurojust.europa.eu/sites/default/files/assets/the-cloud-act.pdf (Letöltés ideje: 2024. február 28.)
[589] Interpol: International Criminal Police Organization - Nemzetközi Bűnügyi Rendőrség Szervezete
[590] *Connecting Police For a Safer World*. Interpol. Online: https://www.interpol.int/content/download/624/file/GI-01_2020-01_EN_LR.pdf (Letöltés ideje: 2024. február 28.)

bevezetése jelentős hatással lesz a rendfenntartó szervek munkájára [...], és jelentősen rontja a jogszerű lehallgatás (LI) alkalmazási képességeit. A törvényes lehallgatás a bűnüldöző hatóságok (terrorizmus, szervezett bűnözés, számítógépes bűnözés) központi nyomozati és keresési eszköze [...]. Ezért a bűnüldöző hatóságok számára rendkívül fontos, hogy ezt az eszközt a mobilkommunikáció további technikai fejlődése ellenére megőrizzék."[591] Az Európai Rendőrfőnökök 2019. márciusi informális találkozójának eredményeként az 5G Szakértői Csoport 2021 októberében a Törvényes Lehallgatási Egységek Európai Vezetőinek[592] állandó csoportjává alakult, mely célja az LI képességek összehangolása és a szabványosítás támogatása, valamint egységes módszerek és technikai elemzési eljárások kidolgozása, amelyek biztosítják az LI fenntarthatóságát a tagállamokban, párhuzamosan biztosítva az uniós adatvédelmi törekvések érvényesülését, például a megfelelő kriptográfiai eljárások alkalmazása, fejlesztése mellett.[593] Az EU „*a közös bel- és igazságügyi területén a tagállamok bűnüldöző szerveinek hírszerzési együttműködése önálló EU-s intézményen, az Europolon*[594] *belül valósul meg, és nem EU-, hanem tagállami szintű erőfeszítéseket támogat.*"[595] Az Europol alapfeladatait tekintve[596] mind műveleti, mind szakértői támogatást, mind információcserét biztosít az uniós tagállamok bűnüldöző szervei számára, hazai viszonylatban a nemzetközi bűnügyi információséért folytató Nemzetközi Bűnügyi Együttműködési Központon (SIRENE Iroda, Nemzetközi Információs Osztály) keresztül. Az EU „titkos információgyűjtő" képességének szupranacionális szervezete még az EU INTCEN[597] és az EU SATCEN[598], a katonai EUMS INT DIR[599] mellett, azonban ezen formációk elemzése nem tárgya az értekezésnek, ahogy a NATO komponenseké sem.[600] Ebben a körben szükséges még jelölni a Terrorelhárítási Csoport, a TREVI Csoport, a Belügyminiszterek Nyugat-mediterrán Konferenciája, illetve a Visegrádi országok bűnüldözési célú multilaterális együttműködését.[601]

---

[591] Lawful Interception – Strengthening EU cooperation. 11517/1/20 (1) 1-2. Brüsszel 2020. Online: https://data.consilium.europa.eu/doc/document/ST-11517-2020-REV-1/en/pdf (Letöltés ideje: 2024. február 28.)

[592] European Heads of Lawful Interception Units - Törvényes Lehallgatási Egységek Európai Vezetői

[593] Lawful Interception – Strengthening EU cooperation (Brussels, 5 November 2020), 11517/1/20 REV 1. 3.

[594] Europol: European Union Agency for Law Enforcement Cooperation – Bűnüldözési Együttműködés Európai Uniós Ügynöksége

[595] BENEDEK 2014. p. 95.

[596] Lásd: Az Európai Parlament és a Tanács (EU) 2016/794 rendelete (2016. május 11.) a Bűnüldözési Együttműködés Európai Uniós Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről, OJ L 135, 24.5.2016, 53–114.

[597] EU INTCEN: European Union Intelligence and Situation Centrer – EU Helyzetelemző Központ

[598] EU SATCEN: European Union Satellite Ceneter – EU Műhold Központ

[599] EUMS INT DIR: EU Military Staff, Intelligence Directorate – EU Katonai Törzs, Hírszerző Igazgatóság

[600] BODA 2016:161-170; BÉRES 2018: 251-290

[601] KISS-BENEDEK József (2013): A nemzetbiztonsági szolgálatok nemzetközi együttműködése. In DR. KOBOLKA István (szerk.): *Nemzetbiztonsági alapismeretek*. Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó. 346-347.

A 2.5.1. részfejezetben ismertetettek alapján az uniós tagállamok között, az SZBJT keretében megvalósuló másodlagos uniós jogforrások szerinti bűnüldözési célú együttműködésen belüli igazságügyi együttműködésre az ENYH irányelv ad jogi keretet, melyet a 2012. évi CLXXX. törvényben ültetett át Magyarország. A rendőrségi és a vámhatósági uniós együttműködésre és információcserére ad jogi keretet a Tanács 2006/960/IB kerethatározata, amely a 2002. évi LIV. törvénnyel vált a hazai jogrendszer részévé. Ezen normák alapján a magyarországi LI alkalmazására és végrehajtására jogosult szerveknek lehetősége van a más EU tagállam joghatósága alá tartozó kommunikáció tartalmához, kísérő- és metaadataihoz hozzáférni a joghatósággal rendelkező tagállam által lefolytatott eljárási cselekmények során megkeletkező információk megkeresés alapú átvételével, mely természetesen kölcsönösségen alapul. A fenti jogszabályok, valamint az Nbtv., Be., Ütv., Rtv. és NAV tv. vonatkozó rendelkezései alapján nemzetközi együttműködésben megvalósuló bűnüldözési célú LI során a jogosult megrendelő szerv a végrehajtásra az NBSZ-t is igénybe veheti. Blaskó Béla megállapítása alapján megjegyzendő, hogy a kommunikáció tartalmára irányuló LI esetében a külső engedély meglétén túl a „*megkeresés […] akkor teljesíthető, ha a titkos lehallgatás célszemélye Magyarország területén tartózkodik, továbbá, ha a célszemély harmadik állam területén tartózkodik, azonban a titkos lehallgatás Magyarország területén működő távközlési szolgáltató közreműködését igényli, vagy a titkos lehallgatást lehetővé tevő technikai eszköz Magyarország területén található*.”[602] Tehát az eljárásrend követi az Eht., és az Ekertv. hatáselv alapján érvényesülő területi hatályát. Azonban, mint minden nemzetközi együttműködésnek, így a fenti uniós jogi aktusok általiaknak is, akkora a hatásuk, amekkorákat a tagállamok döntésük alapján rájuk ruháznak, nem még, ha abból kimaradnak releváns államok. Az igazságügyi ENYH irányelvet a tagállamoknak 2017. május 22-ig kellett átültetniük nemzeti jogrendszerükbe, azonban Dánia és Írország élt az „opt out”, azaz a kimaradási klauzula lehetőségével – akár csak az SZBJT esetében –, így az irányelv rájuk nem hatályos,[603] akár csak az Egyesült Királyságra sem volt az még a Brexitet megelőzően[604]. Tehát megállapítható, hogy az uniós bűnüldözési célú LI-t is érintő multilaterális jogsegélyi keretben éppen az az Írország

[602] BLASKÓ Béla - BUDAHÁZI Árpád (2019): *A nemzetközi bűnügyi együttműködés joga*. Budapest: Dialóg Campus Kiadó. 37. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/13041/web_PDF_Nemzetkozi_bunugyi_egyuttmukodes_joga.pdf?sequence=1 (Letöltés ideje: 2024. február 28.)

[603] NAGY Anita (2017): Európai nyomozási határozat a kölcsönös elismerés elve tükrében. *Kúria Lapja*, 65(6), 5. Online: https://real.mtak.hu/86782/1/NagyanitaEur%c3%b3painyomoz%c3%a1si.pdf (Letöltés ideje: 2024. február 28.)

[604] MOHAY Ágoston (2014): Opt-out/opt-in megoldások az uniós bel- és igazságügyi együttműködés terén: sokféleség az egységben? *Közjogi Szemle*, 8(1), 33. Online: https://szakcikkadatbazis.hu/doc/3328139 (Letöltés ideje: 2024. február 28.)

opt out, amely területén a Meta és az Apple európai disztribútorainak, adatkezelőinek, szolgáltatás nyújtásának székhelye található.

Az EU-n belül maradva Franciaország és Németország tagállamközi bilaterális együttműködése keretében szintén 2016-ban arra a következtetésre jutott, hogy „*az európai hatóságokat komoly kihívás elé állítja a titkosított kommunikáció ellenőrzése, így megoldásokat kellett találni arra, hogy miként lehet hozzáférni a titkosított adatokhoz, ugyanakkor egyúttal hogyan lehet biztosítani a polgárok digitális magánszférájának védelmét.*”[605] A fentiek alapján a két tagállam az EUB-nél kezdeményezte a szolgáltatók által biztosított „titkosítások” részleges feloldásának normatív lehetőségét a terrorellenes célú LI hatékonyságának biztosítása érdekében. Továbbá adatcsere megállapodást kötöttek, amely értelmében kölcsönösen biztosítják egymás bűnüldöző szervei számára a közvetlen adatkérés lehetőségét a területükön működő szolgáltatóktól az állampolgárok védelme érdekében.[606] A fenti jogi aktussal kapcsolatban Békési Nikoletta és Sabjanics István kutatásai eredményei alapján megállapítható, hogy: „*A német parlament által elfogadott új törvény lehetővé teszi azt, hogy a nyomozó hatóságok még a titkosítás előtt – állami engedéllyel – trójai programot telepítsenek a célszemély eszközeire, és ezáltal hozzáférjenek az elküldés előtti, még a titkosításon át nem esett tartalmakhoz*.”[607] Ez nem a DPI szerinti LI, hanem az aktív kémprogram módszer körét érinti.

A részfejezet során a nemzetközi multilaterális együttműködések keretében vizsgálatra kerültek az angolszász nemzetbiztonsági célú LI formációk (UKUSA) és eljárások (downstream: PRISM; upstream: TEMPORA), valamint a bűnüldözés nemzetközi együttműködésének szervezete (Interpol). Az angolszász vonalon maradva kitekintés történt az Egyesült Királyság E2EE-vel kapcsolatos aktuális LI kihívásaira, szabályozási törekvéseire. Bemutatásra került az USA bilaterális LI célú együttműködési lehetőségének jogilag is szabályozott formája a CLOUD Act megállapodás, amely értelmében az USA igazságügyi szerve 2018-at követően végrehajtási passzív jogsegélymegállapodást köthet adott partnerország kormányzati szervével, amely alapján a partnerország jogosult kormányzati szerve közvetlenül fordulhat szolgáltatói

[605] BERTA Sándor (2016): *Német-francia javaslat az üzenetküldő programok lehallgatására*. Sg.hu. Online: https://sg.hu/cikkek/it-tech/120885/nemet-francia-javaslat-az-uzenetkuldo-programoklehallgatasara (Letöltés ideje: 2024. február 28.)

[606] BERTA 2016

[607] BÉKÉSI Nikolett – SABJANICS István (2017): A terrorizmus elleni fellépés magánszférát érintő kérdései. In CSINK Lóránt (szerk.): *A nemzetbiztonság kihívásainak hatása a magánszférára*. Budapest: Pázmány Press. 245-246. Online: https://jak.ppke.hu/uploads/articles/1185528/file/Csink_maganszfera_TAN40.pdf (Letöltés ideje: 2024. február 28.)

együttműködés alapú LI során az USA székhelyű alkalmazásszolgáltatóhoz (például Meta, Apple) a szolgáltató által az LI-vel érintett felhasználóval és kommunikációjával kapcsolatban kezelt adatok átadása érdekében. Eddig ilyen megállapodást az USA csak az Egyesült Királysággal és Ausztráliával kötött. Az EU-t vizsgálva bűnüldözési célú LI multilaterális együttműködés kapcsán megállapításra került, hogy annak egyfajta szervezeti keretet ad az Europol például a szabályozás előkészítés és információcsere formájában. Továbbá tényleges műveleti célú aktív/ passzív jogsegély alapú támogatást biztosítanak az SZBJT keretén belüli másodlagos uniós jogi aktusok (ENYH irányelv, Tanács 2006/960/IB kerethatározata), amelyek implementálásra kerültek a hazai jogban, viszont a Meta és Apple európai disztribútorainak székhelyet adó Írország opt out a jogforrások hatálya alól. Az EU-s LI célú bilaterális együttműködés keretében a francia-német tengely E2EE-t korlátozó EUB igénye került vizsgálatra, Németország aktuális E2EE-t áthidaló aktív kémprogram LI módszerének szabályozásával egyetemben. Az EU szupranacionális joghatósága alól kilépve és vizsgálva az európai országok nemzetbiztonsági célú multilaterális formációit, azonosításra került a Berni Klub, melynek az EU tagországokon kívül tagja Norvégia és Svájc kijelölt nemzetbiztonsági szolgálata, valamint a visegrádi országok hírszerző szolgálatainak informális együttműködése is. Azonban ezen informális szervezetközi nemzetközi együttműködéseknek olyan joghatást kiváltó kötőerővel bíró jogalkotási mandátumuk, mint az EU-nak nincsen.

4.3.3. Az alkalmazásszolgáltatások kriptográfiai környezetének kihívásaival összefüggő uniós jogpolitikai aktualitások, elemzések

Az előző részfejezetben az esettanulmányok feldolgozása során látókörbe került a „*Telegram kapcsán a médiában fellelhető gyermekpornográf tartalmak Új-Delhiben történő terjesztése.*[608]" Ezen bűncselekményi tényállási körnek az online tér, az internet, a közösségi média és az egyéb globális hozzáférésű IKT szolgáltatások általi egyre fokozódó terjedése az EU-ban már a jogalkotók, az a Tanács, a Parlament és a Bizottság szintjét elérő, a gyermekek szexuális bántalmazásának megelőzésére és az ellene folytatott küzdelemre irányuló fokozott jog- és szakpolitikai törekvéseket, jogalkotási folyamatokat indítottak el. Ez a tagállamok között az uniós szintű döntéshozatali mechanizmusokban vitákat és megosztottságot generál az E2EE engedélyezése, korlátozása vagy eltörlése kapcsán. Ezen kiélezendő tagállami

[608] MIHINDUKULASURIYA 2019

megosztottság a CSA rendelet javaslat tervezetet[609] (a továbbiakban: CSAM[610]) megvitató 2023. májusi Tanácsi Rendészeti Munkacsoport értekezletet követően került nyilvánosságra. A vita központi kérdése az, hogy a gyermekek szexuális bántalmazásának megelőzésére és az ellene folytatott küzdelemre való hivatkozással milyen mértékben korlátozható a titkosítás a digitális platformok ellenőrzése – így az alkalmazásszolgáltatások LI-je – céljából, figyelembe véve a Chartában és az alapító szerződésekben lefektetett alapvető jogok és szabadságok jogszerű korlátozását, azaz a 2.3.1. részfejezetben átfogóan ismertetett alapjogi garanciális szabályokat. A Stanford Egyetemen zajló kutatása[611] alapján 20 tagállamnak az E2EE biztonsági célú határozott ellenzését, a problémáról való nem tudomásvételt, a szabályozás korlátozásának elutasítását, az E2EE-t eltűrők, inkább megkerülők, a pragmatikus nem cselekvést tanúsítók, és az E2EE-t támogatók szerinti megoszlása az alábbi 36. ábrán látható.

E2EE kriptográfia határozott elutasítói	E2EE problémáról nem vesznek tudomást	E2EE-t korlátozó szabályozás elutasítói	E2EE-t megtűrők, inkább megkerülők	Pragmatikus nem cselekvést tanúsítók	E2EE határozott támogatói
Spanyolország	Belgium	Dánia	Hollandia	Csehország	Finnország
Magyarország	Lengyelország	Románia	Bulgária	Olaszország	Észtország
Szlovénia		Szlovákia		Málta	Németország
Litvánia		Írország			
Horvátország					
Ciprus					

36. ábra: Vizsgált EU tagállamok E2EE kriptográfia korlátozásának/ támogatásának megoszlása a CSAM tükrében (Szerk.: A szerző[612])

A kutatása alapján megállapítható, hogy Spanyolország álláspontja a legdrasztikusabb, mivel a tagállam „*egyenesen kijelentette, hogy a végpontok közötti titkosítást a törvénynek teljes mértékben meg kell tiltania*”[613], míg például Észtország és Finnország, Németországgal egyetemben nem támogatja az E2EE korlátozhatóságát a magánélethez fűződő alapvető jog védelme érdekében az internet alapú kommunikáció során. Magyarország a nemzetközi

[609] Javaslat az Európai Parlament és a Tanács rendelete a gyermekek szexuális bántalmazásának megelőzésére és az ellene folytatott küzdelemre vonatkozó szabályok megállapításáról, COM/2022/209 final. Brüsszel. 2022.5.11. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52022PC0209 (Letöltés ideje: 2024. február 27.)

[610] CSAM: Child Sex Abuse Regulation material – gyermek szexuális abuzálása elleni rendelet tervezet

[611] PFEFFERKORN, Riana (2023): *EU member states still cannot agree about end-to-end encryption*. Stanford: The Center for Internet and Society, Stanford Law School. Online: https://cyberlaw.stanford.edu/blog/2023/06/eu-member-states-still-cannot-agree-about-end-end-encryption (Letöltés ideje: 2024. február 27.)

[612] PFEFFERKORN 2023

[613] PFEFFERKORN 2023

politikai és szövetségesi téren is biztonságcentrikusan lép fel, így ebben az esetben is az E2EE biztonságra gyakorolt negatív hatásait alapul véve határozottan, a spanyol álláspontot követően kategorikusan támogatja annak korlátozását, úgy ahogy azt a vizsgált EU tagállamok többsége, ellentétben az Észak- és Nyugat-európai tagállamokkal (Franciaország álláspontja nem ismert). A kutatás alapján Magyarország egyértelmű és következetesen képviselt álláspontja, hogy „*a bűnüldözés problémája az online platformok által használt teljes körű, végpontok közötti titkosítás következménye, amely lehetetlenné teszi az elektronikus hírközlési szolgáltatókon keresztüli klasszikus adatlehallgatási tevékenységet*", például az alkalmazásszolgáltatások LI-jét. Azonban a magyar álláspont alapján az LI-nek „*arányosnak kell lennie a magánélet és az adatvédelem alapvető elveivel*". Magyarország „*az adatlehallgatás és -hozzáférés új módszereit szeretné […] a bűnüldözési képességek fenntartása érdekében, amely a nagy nemzetközi online platformokkal és okoseszköz-gyártókkal való együttműködésen alapul*". E célból a nemzeti joghatóság megállapítása elengedhetetlen lenne az LI, és az online platformszolgáltatók, valamint az okoseszköz-gyártók tekintetében. *„A CSA-rendelet pedig ne kerüljön a magyar rendvédelem útjába azzal, hogy olyan rendelkezéseket tartalmaz, amelyek megakadályozzák az E2EE [biztonsági szempontú] korlátozását."*[614] Tehát a fentiek alapján jól érzékelhető az egyes tagállamok külpolitikai álláspontja az adatvédelem/biztonság értékduáljának kiegyensúlyozatlansága kapcsán. Továbbá megállapítható Magyarország következetes, stabil és feltétlen álláspontja az össztársadalmi szintű biztonság, azon belül is kiemelten a gyermekvédelem iránti elköteleződés terén, amelyet az „IKT boom" és az EU digitalizációs stratégiai célkitűzéseinek keretében is érvényesíteni törekszik az online térben.

Az Európai Parlament Kutatási Szolgálatának az E2EE és a gyermekek védelméről szóló vizsgálatáról készült összefoglalótanulmánya alapján az Europol szerint „*A magánélet tiszteletben tartásának és annak védelemének biztosítása mellett az E2EE támogatja a bűnelkövetőket és a kiberbűnözőket is egyaránt*."[615] Az Europol szerint a gyermekek elleni szexuális bűnözők technikai intézkedéseket alkalmaznak (pl. illegális online tevékenységeik anonimizálása és titkosítása), hogy kijátsszák a bűnüldöző hatóságokat, ezzel akadályozva a megelőzést, felderítést. Ezen megállapítás alátámasztja a 4.3.2. részfejezet következtetéseit az

[614] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - comments from delegations on Articles 12 to 15 (9068/22, 14143/22). Council Law Enforcement Working Party (Police). 2022. 31-40. Online: https://s3.documentcloud.org/documents/23819681/law-enforcement-working-party-document-encryption.pdf (Letöltés ideje: 2024. február 27.)

[615] NEGREIRO, Mar (2023): A*t a Glance - Digital issues in focus - E2E encryption and protection of children online*. European Parliament ResearchService. 1. Online: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/751473/EPRS_ATA(2023)751473_EN.pdf (Letöltés ideje: 2024. február 27.)

anonimizálással kapcsolatban. Az ilyen jellegű szervezett bűnözői hálózatok mérete óriási. Egy az Europol által a közelmúltban támogatott németországi művelet során 400.000 tagot számláló elkövetői kört, a „Boystownt" pedofilhálózatot lepleztek le.[616] 2023-ban bűnüldöző szervek nemzetközi csoportja, köztük az Interpol, az FBI és az Ausztrál Szövetségi Rendőrség – a többnemzeti nyomozócsoport tagjai ugyanazok, mint a 2.5.3. részfejezetből ismert „Trójai Pajzs" akció magja – 2023-ban arra hívta fel a Meta figyelmét, hogy 2024-ben ne vezesse be az E2EE-t a Messengeren és az Instagram Chaten, mint azt korábban tervezett. Ennek a Meta „eleget is téve" azt nem 2024-ben, hanem már 2023. decemberében be is vezette a 4.3.1. részfejezet elemzése alapján. A Meta csak 2023 januárjában 490.000 fiókot törölt a gyermekbiztonsági irányelveinek megsértése miatt.[617]

A részfejezet következtetésként megállapításra került, hogy az alkalmazásszolgáltatások LI-jét érintően a CSAM vitájában képviselt hazai külpolitikai álláspont alátámasztja az értekezés során eddig levont következtetéseket, miszerint az IKT környezet változásaiból adódó LI jellegű kihívásokra válaszul nemzetközi szintű együttműködésre van szükség a nemzetbiztonsági, bűnüldözési célú LI tevékenység perzisztens, hatékony fenntartása érdekében. A CSAM vita nem szól másról, mint az alkalmazásszolgáltatások felhasználóinak fokozott személyes adatvédelmét biztosító E2EE kriptográfia és az általa ellehetetlenülő gyermekek sérelmére elkövetett bűncselekmények megelőzésére, felderítésére irányuló bűnüldözési célú LI közötti konfliktus, azaz az adatvédelem/biztonság kiegyensúlyozott értékduáljának elmozdulásáról a biztonság hátrányára, mely alapján az „IKT adatvédelmi biztonsági-deficit" teória szintén igazolást nyert a gyakorlatban. A részfejezetben elvégzett kutatási cselekmények alapján tapasztalható egyfajta politikai szintű elköteleződés az uniós tagországok nagyobb hányadánál az E2EE korlátozásának uniós szintű szabályzási keret közé ültetésére a gyermekek szexuális kizsákmányolásának IKT szolgáltatások terén történő visszaszorítása érdekében. A CSAM úgy néz ki, hogy az Európát ért terrortámadásoknál, az illegális migrációs és a következményeként jelentkező bűnözési hullámnál is nagyobb egységet tud kovácsolni az EU politikai vezetésében, egyben eddig nem látott lendülettel, ami az E2EE közbiztonsági, bűnüldözési célú korlátozását jelenti, így megnyitva a lehetőséget az „IKT adatvédelmi biztonság-deficit" visszabillentésére a biztonság javára. Akkor, ha a

[616] *4 arrested in takedown of dark web child abuse platform with some half a million users*. Europol. Online: https://www.europol.europa.eu/media-press/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users (Letöltés ideje: 2024. február 27.)
[617] NEGREIRO 2023: 2

gyermekvédelem kapcsán áttörhető az „E2EE jég” az EU szintjén, akár jogalkotási, akár technológiai oldalról is megnyílik a lehetőség a nemzetbiztonsági érdekek ezen irányú érvényesítésére is a titkosított kommunikációt biztosító alkalmazásszolgáltatások LI-je terén. Álláspontom alapján amennyiben az E2EE korlátozása terén jogalkotás várható, az szabályzás jelleggel fog történni az E2EE alkalmazhatóságának korlátozásával, tekintettel arra, hogy az E2EE kriptográfia jelenlegi ismeretink alapján gyakorlati titkosságot biztosít. [618]

4.3.4. Alkalmazásszolgáltatók hatósági adatszolgáltatási együttműködési attitűdje

Az esettanulmányok, valamint az uniós jog- és szakpolitika terrénumát követően a komplex vizsgálat érdekében szükséges elemezni az alkalmazásszolgáltatók által közzétett nemzetbiztonsági, bűnüldözési célú együttműködésekre vonatkozó adatokat is. Igen kiterjedt forráskutatás alapján azonban ilyen célirányos, valóban objektívnek tekinthető transzparens adatok nem állnak a rendelkezésre, azonban a hatósági adatszolgáltatások gyűjtőfogalma alatt az európai piacvezető Meta nyilvános statisztikát vezet 2013 óta, mely adatok mintavételezési céllal iránymutatók az alkalmazásszolgáltatók fentiekben levezetett biztonsági célú együttműködési hajlandósága terén, hiszen a hatósági adatszolgáltatások körébe beletartozik mind a bűnüldözési, nemzetbiztonsági, adatvédelmi hatósági, felügyelő hatósági. stb. tevékenységi kör „*A kormányok és állami hatóságok bűnügyi nyomozásokkal, eltűnt személyekkel, terrorelhárítási tevékenységekkel, bírósági eljárásokkal és kiberbiztonsági fenyegetések kezelésével kapcsolatban nyújthatnak be adatkéréseket a Metához.*”[619] A Meta hatósági adatszolgáltatási megkereséseinek és azok teljesítésének globális megoszlását az alábbi 37. ábra mutatja.

[618] SZÁDECZKY 2016: 179

[619] FEKŐ Ádám (2024): *Rekordszámú személyes adatot kért ki a magyar kormány a Facebook felhasználóiról*. Media1. Online: https://media1.hu/2024/01/09/rekordszamu-szemelyes-adatot-kert-ki-a-magyar-kormany-a-facebook-felhasznaloirol/ (Letöltés ideje: 2024. február 27.)

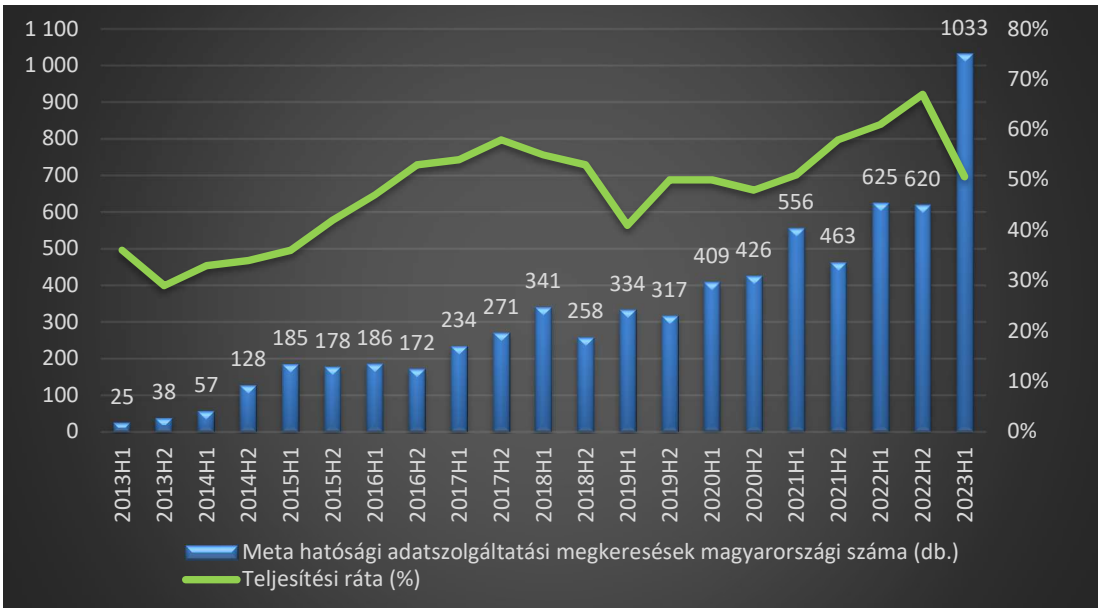
37. ábra: Meta hatósági megkereséseinek és azok teljesítésének globális megoszlása (Szerk.: A szerző[620])

A 37. ábra alapján megállapítható, hogy 2023 első félévében összesen 271.692 darab kérvényt nyújtottak be a jogosult hatóságok a Metához, amelyek összesen 496.372 darab fiók esetében kértek adatokat. Soha ennyi kérelem nem érkezett még be a Metához fél év alatt, a Meta a megkeresések 76,9 százalékában teljesítette az adatszolgáltatást, a maradékot elutasította. Ennek az az oka, hogy „*az egyes szervezeteknek általában jogi eljárásokat kell követniük, például házkutatási parancsot vagy bírósági végzést kell beszerezniük, amikor felhasználói adatokat kérnek az olyan vállalatoktól, mint a Facebook. Azonban egyes hatóságok, titkosszolgálatok sokszor ezen dokumentumok nélkül próbálnak meg adatokat kérni a közösségi platformtól, amit a Meta jogi csapata vizsgálhat meg, és dönthet úgy, hogy nem teljesíti ezeket a kérvényeket.*”[621] A 37. ábra alapján látható trend a Metához érkező hatósági megkeresések számának exponenciális növekedése, mely 2013-2023 között 10,8-szorosára nőtt, míg a teljesítési statisztika 66%-ról 77%-ra nőtt 2023 első félévére. A 37. ábra és a 3.2.1. részfejezet 28. ábrájának összehasonlítása esetén megállapítható, hogy a megkeresések azonosan növekvő tendenciát mutatnak a globális mobil előfizetések számával, ha a 3.2.2. részfejezet 20. ábrájával hasonlítjuk össze, megállapítható, hogy a hazai mobil előfizetések számával is azonos tendenciát mutat. Továbbá, ha a 37. ábrát a 3.2.2. részfejezet 24. ábrájával hasonlítjuk össze, akkor megállapítható ugyanaz az exponenciális jellegű növekedés a hatósági megkeresések,

[620] *Global Overview.* Meta. 2024. Online: https://transparency.fb.com/reports/government-data-requests/ (Letöltés ideje: 2024. február 27.)

[621] JELINEK Anna (2024): *Rekordszámú személyes adatot kért ki a magyar kormány a Facebooktól*. 444. Online: https://444.hu/2024/01/09/rekordszamu-szemelyes-adatot-kert-ki-a-magyar-kormany-a-facebooktol (Letöltés ideje: 2024. február 27.)

valamint az internetforgalmat bonyolított hazai okostelefonos SIM-kártyák számának és fajlagos adatforgalmának alakulása terén. Az európai iszlám fundamentalista terrortámadások, valamint az ISIS elleni nemzetközi koalíciós műveletek időszakával kapcsolatos releváns következtetésként levonható, hogy 2015-2017 között megduplázódott a Metához érkező hatósági adatszolgáltatási megkeresések száma és ebben az időszakban 69%-ról 75%-ra nőtt azok teljesítési hajlandósága. A GDPR 2018-as hatálybalépését követően, így az európai adatvédelmi hatósági hálózat és a tagállami hatóságok közötti jogsegély jellegű együttműködés kezdetét követően a globális megkeresési ráta 2,6-szorosára nőtt 2023-ra. Tehát a fenti statisztikai- és tendenciaelemzések alapján megállapítható részkövetkeztetés, hogy a mobilinternet forgalom bővülésével azonos tendenciát mutat a Metához érkező hatósági adatszolgáltatási megkeresések száma, így közvetetten bizonyítható az internet alapú titkosított kommunikációt biztosító alkalmazásszolgáltatások, egyéb közösségi média platformok hatósági – azon belül bűnüldözési, nemzetbiztonsági – célú tevékenységgel való fokozódó érintettsége, tehát a jogsértő cselekmények során történő logisztikai, kommunikációs célú alkalmazása, és az igénybevétel bővülése a mobilinternet szolgáltatások keresletének növekedésével azonosan. A fenti globális kitekintést követően indokolt megvizsgálni a Meta hazai hatósági adatszolgáltatási megkereséseinek és azok teljesítésének megoszlását az alábbi 38. ábra alapján.



38. ábra: Meta hatósági megkereséseinek és teljesítésének hazai megoszlása (Szerk.: A szerző[622])

[622] *Global Overview - Hungary.* Meta. 2024. Online: https://transparency.fb.com/reports/government-data-requests/country/HU/ (Letöltés ideje: 2024. február 27.)

A magyar hatóságok 2023 első félévében rekordszámú, 1033 adatkérést küldtek a Metának amely 1,7-szerese az előző időszaknak. Azonban a nemzetközi trendtől eltérően hazai adatok nem exponenciális emelkedést, hanem egyfajta polinomiálisan emelkedő rátát mutatnak, amely 2023 első félévében drasztikusan megugrott. Ennek az okai vizsgálhatóak, azonban a hosszútávú trendek tekintetében ezen mintavételezési pont nem bír elmélyült kutatást igénylő relevanciával, annyi azonban megjegyzendő, hogy 2022 második felére rendeződött át a hazai polgári nemzetbiztonsági struktúra kormányzati irányítása.[623] A nemzetközi trendtől szintén eltérő adatot mutat a hazai teljesítési ráta, amely szintén igen ingadozó, 2022 második félévére 67%-os mutatóval majdnem elérte a globális átlagot, azonban 2023 első félévében bezuhant 51%-ra.

A közép-kelet-európai térséget elemezve, először Szlovákiát vizsgálva látható, hogy néhány 10 darab körül alakult a megkeresések félévenkénti száma, mely teljesítési hajlandósága szintén igen változó, Szlovákia teljesítési rátája 33,3%.[624] Csehországban 2022/2023-ra szintén berobbant az adatkérési megkeresések száma, míg 2021 második félévében 151 darabot jegyeztek, addig 2023 első félévére ez felduzzadt 839-ra, 77,2%-os teljesítési rátával.[625] Lengyelországnál 2018 után egyfajta erőteljesebb emelkedés figyelhető meg a megkeresések terén, 2023 első félévére elérte a 6.910 megkeresést, 68,26%-os teljesítési rátával.[626] Romániában is emelkedik a tendencia, azonban ez a megkeresések száma és az állam területének, lakosságának arányában nem számottevő, 2023. első félévében 431 volt, 62,8%-os teljesítési rátával.[627] Tehát a közép-kelet-európai térséget elemezve megállapítható, hogy 2023 első félévében a Metához legtöbb hatósági adatkérést benyújtó állam számosságába Lengyelország volt, melyet Magyarország követ, lakosságához viszonyítva Magyarország vezet, a teljesítési rátát pedig Csehország vezeti.

Nyugat-európai mintavételezés tekintetében Németország Metához benyújtott hatósági adatszolgáltatási megkereséseinek tendenciája azonos ütemben nő a nemzetközi trenddel, 2023

[623] Lásd: Tóth 2022: 69-71
[624] *Global Overview - Slovakia.* Meta. 2024. Online: https://transparency.fb.com/reports/government-data-requests/country/SK/ (Letöltés ideje: 2024. február 27.)
[625] *Global Overview – Czech Republic.* Meta. 2024. Online https://transparency.fb.com/reports/government-data-requests/country/CZ/ (Letöltés ideje: 2024. február 27.)
[626] *Global Overview - Poland.* Meta. 2024. Online: https://transparency.fb.com/reports/government-data-requests/country/PL/ (Letöltés ideje: 2024. február 27.)
[627] *Global Overview - Romania.* Meta. 2024. Online: https://transparency.fb.com/reports/government-data-requests/country/RO/ (Letöltés ideje: 2024. február 27.)

első félévében 20.741 megkeresést nyújtott be, 71,8%-os teljesítési rátával.[628] Franciaország 2019-től csökkenő, stagnáló szintet mutat, 2023 első félévében 12.022 megkeresést realizálva, 85%-os teljesítési mutatóval.[629] A hasonló területtel és lakossággal bíró Spanyolország 2023 első félévében mindösszesen 2.935 megkeresést nyújtott be a Metához, 64,1%-os teljesítési rátával.[630] A fenti adatokat összevetve a 3.2.1. részfejezet 25. ábrájával, azonos trend állapítható meg a Nyugat- és Közép-Kelet-Európa közötti megosztottság kapcsán a Metahoz benyújtott hatósági adatszolgáltatási megkeresések mennyisége, nagyságrendje, valamint a 4G/5G jelenlegi és várható általános elterjedése között. Az EU-n kívüli Euro-atlanti térségben érdekességként az Egyesült Királyság 9.787 kérelemmel bírt 2023 első felében, 87%-os teljesítési ráta mellett[631], az USA 73.956 megkereséssel vezeti a 2023 első félévi ranglistát, közel 88%-os teljesítési mutatója mellett.[632]

A részfejezetben az európai piacvezető Meta hatósági adatszolgáltatási attitűdjét mintavételezési céllal bemutató tendenciaelemzés során megállapításra kerül a szolgáltatóhoz beérkező hatósági megkeresések globális számának exponenciális növekedése. A trend- és tendenciaelemzések alapján megállapítható részkövetkeztetés, hogy a mobilinternet fogalom bővülésével azonos tendenciát mutat a Metához érkező hatósági adatszolgáltatási megkeresések száma, így bizonyítható az internet alapú titkosított kommunikációt biztosító alkalmazásszolgáltatások, egyéb közösségi média platformok hatósági – azon belüli bűnüldözési, nemzetbiztonsági – érdeket sértő tevékenységgel való fokozódó érintettsége, tehát a jogsértő cselekmények során történő logisztikai, kommunikációs célú alkalmazása, és az igénybevétel bővülése a mobilinternet szolgáltatások keresletének növekedésével azonos módon. Nyugat- és Közép-Kelet-Európa közötti megosztottság tapasztalható a Metahoz benyújtott hatósági adatszolgáltatási megkeresések mennyisége, nagyságrendje között. Közép-kelet-európai térséget elemezve megállapítható, hogy a 2023 első félévében a Metához legtöbb hatósági adatszolgáltatási megkeresést benyújtó állam lakosságához viszonyítva Magyarország volt, azonban csak 51%-os teljesítésii rátával. A vizsgálat alapján globális szinten a Metához

[628] *Global Overview - Germany.* Meta. 2024. Online: https://transparency.fb.com/reports/government-data-requests/country/DE/ (Letöltés ideje: 2024. február 27.)
[629] *Global Overview - France.* Meta. 2024. Online: https://transparency.fb.com/reports/government-data-requests/country/FR/ (Letöltés ideje: 2024. február 27.)
[630] *Global Overview - Spanis.* Meta. 2024. Online: https://transparency.fb.com/reports/government-data-requests/country/ES/ (Letöltés ideje: 2024. február 27.)
[631] *Global Overview – United Kingdom*. 2024. Online: https://transparency.fb.com/reports/government-data-requests/country/GB/ (Letöltés ideje: 2024. február 27.)
[632] *Global Overview – United States*. 2024. Online: https://transparency.fb.com/reports/government-data-requests/country/US/ (Letöltés ideje: 2024. február 27.)

2023 első félévében benyújtott hatósági adatszolgáltatási megkeresések 76,9 százalékát teljesítette, míg Szlovákia tekintetében 33%-ot, az USA tekintetében 88%-ot, a maradékot elutasította. Tehát megállapítható, hogy az alkalmazásszolgáltató a hatósági együttműködések keretében az egyes tagállamok hatóságai, azon belül értelmezve a jogosult LI szervezetei által közvetlenül megküldött megkeresések jelentős hányadát átlagosan megválaszolja, míg kb. az ¼-ének teljesítését megtagadja a kb. 10 éves gyakorlat alapján.

A közvetlen szolgáltatói megkeresés okán felvetődik az előzőekben ismertetett ENYH, és bűnügyi jogsegély intézmények ilyen téren meglévő létjogosultságának kérdése. Ennek kapcsán felmerül az értekezés szempontjából is vizsgálandó kérdés, mégpedig hogy a szolgáltatói együttműködésen alapuló LI során a fentiek alapján az alkalmazásszolgáltatónak jogilag lehetősége van-e az adatszolgáltatás megtagadására, hivatkozva a szolgáltató belső „törvényességi kontrolljára" például egy alkotmányos jogállami keretek között, demokratikusan működő, garanciális szabályoknak megfelelő, törvényileg szabályozott LI tevékenységet végző nemzetbiztonsági, vagy bűnüldöző szerv megkeresése esetén? Ráadásul elég nagy eltérés tapasztalható mondjuk az USA 88%-os, Magyarország 51%-os és Szlovákia 33%-os teljesítési rátája között. Ennek körülményei, jogszerűségének kérdése az alkalmazásszolgáltatási LI szempontjából vizsgálandó kérdés az Ekertv. vonatkozásában, melyre az értekezés következő alfejezetében kerül sor a hazai szabályozás szempontjából részletesen, azt összevetve a nemzetközi trendekkel, kihívásokkal. Továbbá a 2.7., valamint a 4. fejezet előző alfejezeti alapján megállapítható, hogy a Meta WhastApp és Messenger szolgáltatásai E2EE-vel ellátottak, így azokból tartalmi adat a szolgáltató oldalán a gyakorlati titkosság okán nem kinyerhető, melyet a Meta is megerősíti a Messenger alkalmazás súgóközpontjában, miszerint az E2EE „*azt jelenti, hogy senki más nem láthatja, vagy hallhatja a leírtakat vagy elhangzottakat – még a Meta sem. Akkor sem tehetnénk meg, ha szándékunkban állna.*" Tehát felmerül a kérdés, hogy akkor milyen adatok tekintetében képes a Meta teljesíteni az adatszolgáltatásokat. Ilyenek például a nem végpont titkosított csoportos chat funkciók, az egyes metaadatok stb.[633]

[633] *Messenger Súgóközpont.* Meta. 2024. Online: https://www.facebook.com/help/messenger-app/1084673321594605 (Letöltés ideje: 2024. február 27.)

4.4. A hazai alkalmazásszolgáltatási LI normatív, szervezeti evolúciója, trendjei

Az alkalmazásszolgáltatások LI tevékenységére vonatkozó speciális ágazati szabályozás áttekintése érdekében szükséges az Ekertv., valamint az LI-vel kapcsolatos végrehajtási részletszabályokat meghatározó 185/2016. (VII.13.) Korm. rendelet áttekintése. Az értekezés további érdemi tudományos következtetéseinek levonása érdekében szükséges az „IKT boom" várható hatásainak vizsgálata az alkalmazásszolgáltatási LI tekintetében is, mely az alfejezetben elvégzésre kerül.

4.4.1. Az Ekertv. szerinti szabályozás hátterének összefüggései az Eht. szerinti LI szabályozás egyes vetületeivel

Az Ekertv. szerinti alkalmazásszolgáltatási LI szabályozás tételes elemzésének előkészítése érdekében szükséges kitérni a 2.6.3. részfejezetben azonosított problémakörre a 3.3.1. részfejezetben taglalt Eht. 92. § (5) bek. szerinti elektronikus hírközlési szolgáltató által kiépítendő központi monitoring LI alrendszer és az NI-ICS – azaz az e fejezet és az Ekertv. szerinti titkosított online kommunikációt biztosító alkalmazásszolgáltató – viszonya tekintetében. Elsősorban az értekezés korábbi részkövetkeztetésinek elemzésére, és az Ekertv. vonatkozó módosításának indokolására építve.

Az első megállapítás, hogy az Eht. 2003-ban az LI kapcsán még az akkori technológiai fejlettségnek megfelelő technológiasemlegességi szabályok szellemiségét tükrözte, azaz akkoriban még a fizikai hírközlő infrastruktúra üzemeltetője és a tényleges elektronikus hírközlési szolgáltatást nyújtó (például személyközi hírközlési, internet-hozzáférési szolgáltatás) integrált módon, kvázi heterogén szolgáltatási modellben adott szolgáltatónál összpontosult, nem különült el. A második megállapítás, hogy ezen hírközlési szolgáltatók szabványosított hálózati topológiája adott nemzet-, tagállam területén központi (core)rendszerrel rendelkezett a szolgáltatás nyújtásához szükséges további hálózati rendszerelemekkel, például a RAN hálózattal egyetemben. Roaming esetén, melyet az EU 2022/612 rendelete,[634] hazai viszonylatban pedig az Eht. szabályoz, a tagállami hálózati topológiákból adódóan a forgalomnak át kellett haladnia a tagállami központi (core)rendszeren. A harmadik megállapítás, hogy a fentiek alapján az Eht. 1. § (1) bek. a) pontja szerinti tárgyi

[634] Az Európai Parlament és a Tanács (EU) 2022/612 rendelete (2022. április 6.) az Unión belüli nyilvános mobilhírközlő hálózatok közötti barangolásról (roaming), OJ L 115, 13.4.2022, 1–37.

hatálya, egyfelől kvázi területi jelleggel bírt a hagyományos szolgáltatók infrastruktúrájának oldaláról (a szakirodalom helyesen fogalmi szinten is elhatárolja az infrastruktúra szolgáltató fogalmát[635]), hiszen azok általánosan tagállami szinten kerültek kialakításra – Magyarország területén biztos – központi (core)rendszerrel ellátva. Ez a modell érvényesül általánosságban a napjainkban is. Az LI szempontjából ez azért lényeges, mert adott tagállam elektronikus hírközlő hálózatán kezelt adatok az ország területén, joghatóságának felügyelete alatt kerültek/ kerülnek kezelésre – összhangban az uniós és hazai adatvédelmi előírásokkal – azok alól a roaming esete kivétel, hiszen az adat (hang hívás, üzenet, multimédiás adat) elhagyja az ország területét, de itt a határokon átnyúló adatkezelés jogszerű. A fentiek alapján a tagállami joghatóság szerint, a tagállami nemzetbiztonsági és bűnüldöző szervek a működési területükkel érintett hírközlési szolgáltatás keretében kezelt adatokhoz LI során így hozzáférhetnek, például hazai viszonylatban az Eht. 92. § szerinti módon, az Nbtv., Be. törvényi felhatalmazása alapján. Abban az esetben, ha a tagállami jogosult LI szerv például titkos információgyűjtés keretében a tagállami hírközlő hálózattól független, más állam joghatósága alá tartozó elektronikus hírközlő hálózaton kezelt adatokhoz kíván jogszerűen hozzáférni, akkor a 2.5.2. és 3.3.1. részfejezetekben ismertetettek alapján a másik tagállam bűnüldöző szerveit jogsegély, ENYH formájában felkérheti ezen adatok beszerzésére és átadására, mely Írország opt out státuszára tekintettel korlátozottnak tekinthető.

Azonban az NI-ICS esetében felmerül a személyközi hírközlési szolgáltatás és a fizikai hírközlő infrastruktúra üzemeltetésének elkülönülése, heterogenizációja, hiszen az NI-ICS-t, azaz a titkosított online kommunikációt biztosító globális, regionális területi lefedettséggel rendelkező Ekertv. szerinti alkalmazásszolgáltatót (például az USA-beli anyavállalati hátterű, európai disztribútorral rendelkező Meta, Apple), a tagállami elektronikus hírközlő szolgáltatók (például a nemzetköz hátterű, tagállami, így magyarországi tagvállalattal rendelkező Telekom, Vodafone, Yettel) által üzemeltetett hírközlő hálózaton, fizikai infrastruktúrán biztosított mobilinternet-hozzáférési szolgáltatás igénybevétele útján nyújtják a felhasználóknak. Tehát az NI-ICS a hálózati topológia alapján a szolgáltatást adott földrajzi ponton elhelyezett központi (core)rendszer, ebben az esetben kiszolgálószerver által, az internet globalitását kihasználva nemzetközi jelleggel nyújtja, a nemzetközi szinten összekapcsolt, konvergens hírközlő hálózatok igénybevételével. Az előző alfejezetek alapján az EU szintű szolgáltatásnyújtásnak

[635] Lásd: KOVÁCS 2015: 184-186

technológiai okokon túl, igen szigorú adatkezelési okai is vannak, a technológiasemlegesség elvét is figyelembe véve.

Az USA-beli anyavállalatú Meta (WhatsApp és Messenger szolgáltatások) tekintetében, a Meta Platforms Ireland Limited európai disztribútorának székhelye, az EU tagállamokat kiszolgáló szervereinek – illetve a számítási felhő (tárhely)infrastruktúrájának – fizikai elhelyezése, letelepítési helye, így az EU szintű adatkezelés székhely szerinti állama Írország.[636] Az USA-beli anyavállalatú Apple (iMessge, FaceTime szolgáltatások) tekintetében, a Apple Operations Europe Ltd. az európai disztribútor, ami a Metához hasonlóan szintén írországi székhellyel rendelkezik. Ezen NI-ICS-ek, alkalmazásszolgáltatók által nyújtott szolgáltatások elérhetők Magyarországon is, így a hatáselv alapján számfüggetlen hírközlési szolgáltatási tevékenységük az Eht. 1. § (1) bek. a) pontja alapján az Eht. hatálya alá tartozik (másfelől pedig az Ekertv. 1. § (1) bek. a) pont alapján az Ekertv. hatály alá tartozik). Ez alapján azonban rájuk is kötelezőek az Eht. 92. § rendelkezési, így a monitoring LI alrendszer kialakítás is, a hazai központi LI szerv ilyen igényű megkeresése esetén. Tehát, ha az NI-ICS-esek tekintetében vizsgáljuk az elektronikus hírközlés hazai szabályozását, már itt is felmerül a nemzetköziség kérdése a hatáselv alapján kiterjesztett kvázi területi hatály tekintetében, hiszen a fentiek alapján az Eht. szerint kijelölt hazai központi LI szerv – csak az EU térségben maradva, abból nem kilépve – monitoring funkcióval bírna a Meta és az Apple Írországban letelepített kiszolgáló szerverein. Ennek álláspontom alapján mind technológiailag, mind adatvédelmi, mind a kriptográfia fejlődésének szempontjából az előzményeket figyelembe véve igencsak korlátozott lehetőségei voltak, melyeket a hazai jogpolitika és az értekezés során feldolgozott szakirodalom is alátámaszt. Ezt álláspontom alapján a hazai jogalkotó is értékelte és megalkotta a Eht. szerinti passzív DPI módszer alternatíváját, azonban már nem az Eht., hanem az Ekertv. hatálya alatt az NI-ICS tevékenységet, mint titkosított kommunikációt biztosító alkalmazásszolgáltatást szabályozva a hazai központi LI szerv és az alkalmazásszolgáltató együttműködésének keretében (előzmény 2.5.1.). Ez jelen fejezet vizsgálatának fő tárgyát képezi, fókusszálva arra, hogy például az írországi székhelyű Meta disztribútor vajon milyen jogelv, jogértelmezés alapján folytatja legalább 10 éve azon gyakorlatát, hogy felülbírálja az egyes EU tagállamok – és a harmadik országok – hatósági adatszolgáltatási megkereséseit, belső kontrollmechanizmust gyakorolva dönt azok jogszerűségről, a kiszolgálás elutasításáról

[636] 2/2022. számú a Meta Platforms Ireland Limited (Instagram) ügyében az ír felügyeleti hatóság döntéstervezetéről kialakult vitában az általános adatvédelmi rendelet 65. cikke (1) bek. a) pontja értelmében elfogadott kötelező erejű határozat. EDPB. 2022. 6

érdemi szankció nélkül. Előre láthatólag a nemzeti joghatóságok, az alkalmazott jogok kollíziója lehet a háttérben.

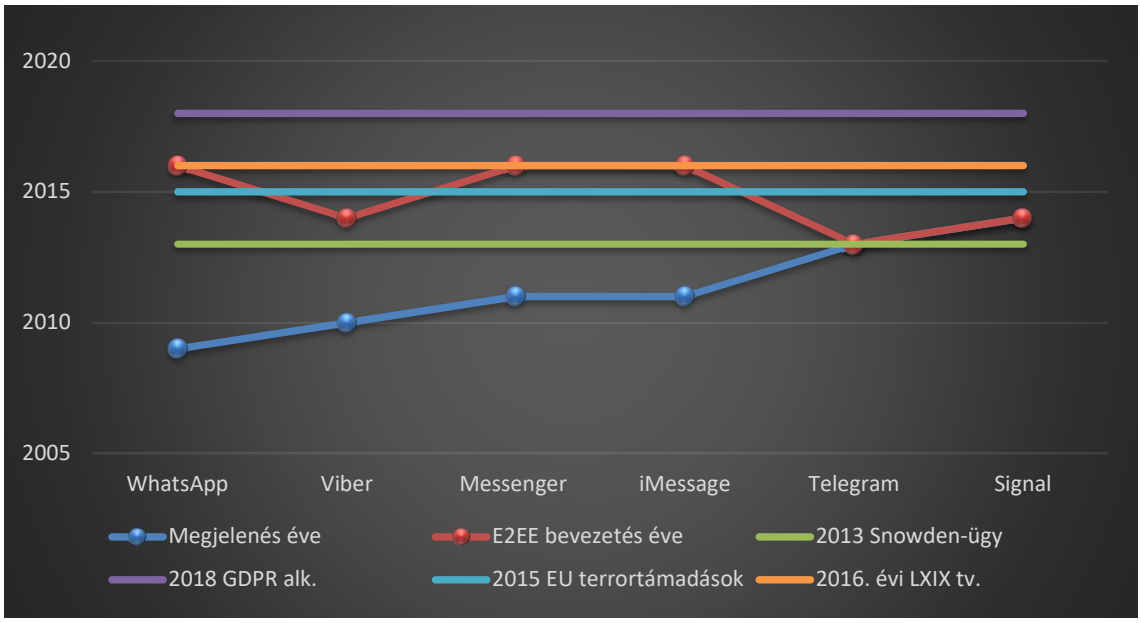
4.4.2. Az Ekertv. 2016-os terrorellenes módosításától napjainkig

Az internet alapú titkosított kommunikációt biztosító alkalmazásszolgáltatás 2016 magasságában jelent meg a hazai jogforrásokban, azaz az Ekertv.-ben bűnüldözési, nemzetbiztonsági tevékenység kapcsán, mégpedig a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló 2016. évi LXIX. törvény alapján. Indokolása szerint a „*II. Kódolt telefonos szolgáltatások korlátozása*" című fejezetének akkori általános helyzetképe megállapította, hogy „*A technikai fejlődés következtében az internet alapú globális kommunikációs rendszerek, valamint ezen szolgáltatások egyre szélesebb körben terjednek el és megfizethető áron vehetők igénybe, így reális veszélyt jelent, hogy az általános kommunikációs szokások megváltoznak, és a hagyományos hírközlési szolgáltatók helyett ezen szolgáltatásokat veszik igénybe a bűnözői körök. Tekintettel arra, hogy a mobiltelefonok kommunikációjának védelmét ellátó rendszernek egyik elemét képező mobiltelefonos alkalmazás az egyes alkalmazásszolgáltatók interneten elérhető, kereskedelmi céllal létrehozott felületén megtalálható, onnan telepíthető, így kivédhető, hogy az egyes országok szolgálatai a kommunikációt, vagy az ahhoz kapcsolódó információkat megszerezhessék, valamint dekódolhassák.*" Az indokolás a „bűnözői körök" elleni bűnüldözési célú LI-t nevesíti, mely érthető, hiszen a nemzetbiztonsági tevékenység nem tartozik az uniós jog hatálya alá. A további indokolás alapján az Ekertv.-ben megjelenő új rendelkezések megoldást jelentettek a törvény hatálya alá tartozó alkalmazásszolgáltatók adatmegőrzési, adatszolgáltatási és együttműködési kötelezettségének megteremtésére, mivel ezen szolgáltatók a rendvédelmi – így polgári nemzetbiztonsági – és igazságügyi szervek irányába akkoriban nem tartoztak adatszolgáltatási és együttműködési kötelezettséggel, tehát a hazai jogértelmezésben a rendvédelmi szerven belül értelmezve megjelenik a polgári nemzetbiztonsági célú LI esetköre is.

Az indokolás szerint az Ekertv.-t érintő módosítás egyrészt megteremtette annak a lehetőségét, hogy a szolgáltató köteles legyen hozzáférést biztosítani mindazon adatokhoz és információkhoz, amelyek a titkos információgyűjtés eszközeinek, módszereinek alkalmazásához nélkülözhetetlenek, másrészről pedig a módosítás a szolgáltató részére kötelező jelleggel írja elő a NBSZ-szel történő, a titkos információgyűjtés feltételeit érintő megállapodások megkötését. Tehát az Eht. szerinti hazai központi hírközlési LI szerv az Ekertv.

szerint is kijelölésre került az alkalmazásszolgáltatói LI szerepkör betöltésére, a hazai koncentrált LI képesség új vertikumát megteremtve egyben. A fenti 2016-os jogalkotói következtetések már csak a 3.2.2. részfejezet azon következtetései szerint is érdekesek, miszerint a mobil adatforgalom 2016-ot követően egy rendkívül dinamikus exponenciális növekedést produkál összhangban a nemzetközi trendekkel, 2016 és 2023.Q2 között, mintegy 25-szörösére növelve mértékét, mely láthatóan összefügg a 4G szolgáltatás magyarországi bevezetésének időpontjával. Tehát az elvégzett hírközlési trendelemzés alapján az LI-vel kapcsolatosa jogpolitikai szemlélet időtállónak bizonyult az internetes alkalmazás alapú kommunikáció hazai tendenciáit illetően.

A vizsgált alkalmazásszolgáltatások és az E2EE bevezetésének, a Snowden-incidens időpontjának, a GDPR alkalmazandóságának, a 2015-től kezdődő Európai terrortámadások kezdőidőpontjának és a 2016. évi LXIX. törvény hatálybalépésének időrendi összehasonlítását a 39. ábra szemlélteti.



39. ábra: A vizsgált alkalmazásszolgáltatások és az E2EE bevezetésének, a Snowden-incidens időpontjának, a GDPR alkalmazandóságának, a 2015-től kezdődő Európai terrortámadások kezdőidőpontjának és a 2016. évi LXIX. törvény hatálybalépésének összehasonlítása (Szerk.: A szerző[637])

[637] 4. számú melléklet: *A 4. fejezet ábráinak forrásadattáblái*

A 2.6.4. részfejezetben kimutatásra került, hogy az Ekertv és a 185/2016. (VII.13.) Korm. rendelet értelmezése alapján alkalmazásszolgáltatás esetén a kommunikáció egyedi felhasználók, vagy azok csoportja számára információcserét, vagy egyoldalú megosztást lehetővé tevő szolgáltatás igénybevétele során végbemenő közlés, amely elektronikus hírközlő (például mobilinternet) hálózat igénybevétele útján valósul meg. A kommunikáció tartalmának rejtjelezése, megváltoztatása vagy tömörítése esetén taralomnak csak a közlés eredeti formájára visszaállított adat minősül[638] (amit a felhasználó begépelt küldés előtt, vagy amit a fogadást követően a címzett elolvas), összhangban az Eht.-val. Ennek az LI eredményesége szempontjából van kiemelt jelenősége, hiszen például a rejtjelezett tartalomhoz technikailag hiába fér hozzá a jogosult LI szerv, ha az nem megfejthető nem valósul meg a jogszabályi előírás. Az Ekertv. 2016. július 17-től hatályos 3/B. §-a kimondja, hogy „*Az az alkalmazásszolgáltató, aki az információs társadalommal összefüggő olyan szolgáltatást nyújt, amely a szolgáltatást igénybe vevők között titkosított kommunikációt biztosít olyan módon, hogy a kommunikáció tartalma vagy a kommunikációs csatorna felépítésével kapcsolatos funkciók nem kizárólag a felhasználó végberendezésén valósulnak meg (végpont-végpont közötti titkosítás), köteles - az e törvényben meghatározott feltételek szerint - a titkosított kommunikációt biztosító alkalmazás igénybevételével továbbított küldemények, közlések tartalmát a külső engedélyhez kötött titkos információgyűjtésre jogosult szerv megkeresése esetén átadni […]*.” A végrehajtás rendjét a 185/2016. (VII. 13.) Korm. rendelet 2. § részletezi, a 2. § (3) bek. alapján „*Az alkalmazásszolgáltatótól a titkosított kommunikáció tartalma - törvényben meghatározott feltételeknek megfelelően - kizárólag az NBSZ útján igényelhető, illetve az alkalmazásszolgáltató ezeket az adatokat kizárólag az NBSZ részére adhatja át.*” Tehát nemzetbiztonsági vagy bűnüldözési célú LI tevékenység körében az EE2E-t nem alkalmazó alkalmazásszolgáltatások tekintetében a szolgáltató köteles a titkos információgyűjtéssel érintett rejtjelezetlen kommunikáció tartalmát az NBSZ megkeresése esetén annak átadni, a törvényi garanciális és szabályozási, engedélyezési feltételek fennállása esetén, így biztosítva a technológiasemlegesség elvének érvényesülését az E2EE gyakorlati titkosság okán. A jogszabály az alkalmazásszolgáltatókat érintő LI tevékenység során megvalósuló tartalomellenőrzés végrehajtására kizárólagosságot biztosít az Eht. szerinti hírközlő hálózaton folytatott kommunikáció LI-jének végrehajtására kijelölt hazai központi LI szerve, azaz az NBSZ számára.

[638] 185/2016. (VII.13.) Korm. rendelet 1. § b) – c) pont

Szintén a 2.6.4. részfejezet alapján alkalmazásszolgáltató esetében nem kísérő, hanem metaadatot szabályoz az Ekertv. és a 185/2016. (VII.13.) Korm. rendelet. Az Ekertv. hatálya alá tartozó alkalmazásszolgáltatáshoz kapcsolódóan a 185/2016. (VII.13.) Korm. rendelet 1. § d) pontja szerint a metaadat az Ekertv. 13/B. § (2) bekezdésében meghatározott adat, tehát az LI-vel érintett szolgáltatás típusa, az előfizetőnek vagy felhasználónak a szolgáltatás igénybevételéhez szükséges azonosító adatai, az igénybevétel dátumát, kezdő és záró időpontja, valamint a regisztrációhoz és az igénybevételhez használt IP-cím és portszám, továbbá a felhasználói azonosító adatai. Azaz a metaadat a titkosított alkalmazásszolgáltatás igénybevételével végbemenő kommunikáció vonatkozásában elsősorban a felhasználóra utaló azonosítóadat, a kommunikáció időpontja, valamint a kommunikáció során felhasznált végponti eszköz (például okostelefon) elektronikus hírközlő hálózat igénybevétele során kibocsájtott azonosító adata, azaz IP-címe és portszáma. Az Ekertv. 3/B. § kimondja, hogy a nem E2EE titkosított kommunikációt biztosító alkalmazásszolgáltató „*[…] a titkosított kommunikációt biztosító alkalmazás igénybevételével kapcsolatosan keletkező, vagy kezelt, a 13/B. § (2) bekezdése szerinti metaadatokat a 13/B. § szerint megőrizni és külső engedélyhez kötött titkos információgyűjtésre jogosult szerv megkeresése esetén átadni*.” A végrehajtás rendjét a 185/2016. (VII. 13.) Korm. rendelet 2. § részletezi, a 2. § (1) bek. alapján „*A titkos információgyűjtésre felhatalmazott szervezetek a titkos információgyűjtés során a metaadatokat a Nemzetbiztonsági Szakszolgálaton (a továbbiakban: NBSZ) keresztül vagy az e rendeletben meghatározottak szerint az alkalmazásszolgáltatótól közvetlenül kérelmezik.*” Tehát nemzetbiztonsági vagy bűnüldözési célú LI tevékenység körében az EE2E-t nem alkalmazó alkalmazásszolgáltatások tekintetében a szolgáltató köteles a titkos információgyűjtéssel érintett rejtjelezetlen kommunikáció metaadatait a jogosult LI szerv közvetlen, vagy az NBSZ megkeresése esetén annak átadni, a törvényi garanciális és engedélyezési feltételek fennállása esetén. Ezen a ponton lényeges megállapítani, hogy az Ekertv. 3/B. § szerinti metaadatszolgálatásra irányuló rendelkezés nemzetbiztonsági célú LI esetén a technológiasemlegesség elvét biztosítani hivatott lex specialis-a a nemzetbiztonsági szolgálatok 2.3.2. részfejezetben kifejtett Nbtv. 39. – 40. § szerinti általános adatkérési felhatalmazásának, valamint az NBSZ Nbtv. 8. § (1) bek. h) pontja szerinti általános adatigénylés-közreműködői felhatalmazásnak. A jogszabály az alkalmazásszolgáltatókat érintő LI tevékenység során megvalósuló metaadatszolgáltatás végrehajtására nem biztosít kizárólagosságot a hazai központi LI szerv számára, a tartalomellenőrzés végrehajtásával ellentétben.

Tehát részkövetkeztetésként az Ekertv. 3/B. § szerinti alkalmazásszolgáltatói LI 2016-tól hatályos E2EE-t érintő kivételszabályának értékelése kapcsán megállapítható, hogy az megfelel a technológiasemlegesség elvének, tekintettel az E2EE gyakorlati titkosságára, azaz a kommunikáció tartalmához való rejtjelezetlen hozzáférés kvázi lehetetlenségére, rejtjelfejtő eljárás alkalmazása nélkül. A szabályozás időtállósága kapcsán levonható következtetés, hogy az a 2.4.1. részfejezetben ismertetettek szerint már a hatálybalépésének időpontjában is csak korlátozottan volt hatékony, tekintettel arra, hogy a vizsgált alkalmazásszolgáltatások ¾-e addigra már E2EE kriptográfiát alkalmazott, mely aktualitását nézve megállapítható, hogy az E2EE alapértelmezettségének, azaz kizárólagosságának folyamatos terjedésével (például Messenger 2023. december), valamint a legújabb poszt-kvantumszámításnak is ellenálló kriptográfiai algoritmusok megjelenésével (iMessage 2024. március) tovább korlátozódik. Tehát a fenti bizonyítás alapján megállapítható, hogy az alkalmazásszolgáltatások LI-jének hazai jogszabályi környezete a hatékonyság szempontjából 2023-hoz képest, kb. 8-10 éve fokozódóan korlátozott azok kriptográfiai tulajdonságainak fejlődéséhez képest. Így az alkalmazásszolgáltatások globalizációjának, valamint azok kriptográfiai környezeti fejlődésének hatására az elektronikus hírközlési szolgáltatások LI-jét szabályozó hatályos hazai normarendszer hatékonysága erodálódik, e téren az LI képesség rezilienciája korlátozott. Ezen hazai szabályozási kihívások nemzetközi szintű értékelése érdekében volt szükség előzetesen a 4.3. alfejezetben az átfogó nemzetközi kitekintésre, mely alapján megállapítható, hogy a vizsgált országok (USA, Egyesült Királyság, Franciaország, Németország) hasonló szabályozási kihívásokkal küzdenek a monitoring alapú DPI LI módszer tekintetében. Erre egyfelől megoldást a rendkívül nagy pénzügyi erőforrásigényes rejtjelfejtés nyújthat, azonban csak időlegesen a kriptográfiai eljárások folyamatos fejlődése okán a 2.7. alfejezetben és a 4.2.1. részfejezetben ismertetettek alapján, illetve az aktuális német jogalkotási példánál maradva az aktív kémprogram szerinti LI módszer is alternatíva az E2EE kezelésére, azonban ez csak rendkívül korlátozott mennyiségben biztosíthatja az LI-t, valamint licencigénye okán ez jóval költségesebb, mint a szolgáltatói költségviselés lehetőségét magában hordozó központi DPI monitoring alrendszer alapú ellenőrzés. Tehát a fentiek alapján is bizonyítást nyert, hogy az alkalmazásszolgáltatásokkal kapcsolatos nemzetközi normatív adatvédelmi és elektronikus információbiztonsági környezet fejlődése hátrányosan érinti az azokon végbement kommunikáció LI-jének technológiai hatékonyságát.

A részfejezet alapján szükséges megvizsgálni és következtetéseket levonni az alkalmazásszolgáltatók – a 4.3.4. részfejezet mintavételezése alapján a Meta – hatósági, így a

nemzetbiztonsági, bűnüldözési LI célú adatszolgáltatási megkereséseinek – eddig még doktori (PhD) értekezésben nem vizsgált – kiszolgálását megtagadó gyakorlatáról. Az Ekertv. területi hatálya az 1. § (1) bek. a) pontja alapján kiterjed arra az információs társadalommal összefüggő szolgáltatást nyújtóra is, amely nem csak Magyarország területéről, hanem az ország területére irányuló szolgáltatást is nyújt, például külföldön helyezkedik el a fizikai infrastruktúrája (például szerver, számítási felhő), és a szolgáltatást Magyarország területén igénybe vevők ahhoz az Eht. szerinti mobilinternet-hozzáférési szolgáltatáson keresztül kapcsolódnak. Tehát az Ekertv.-ben territoriális elvvel szemben a hatáselv érvényesül (tárgyi,) területi hatálya terén. Az Ekertv. 2. § 16) pont szerint Magyarország területére irányuló szolgáltatás többek között az „*alkalmazásszolgáltató valamennyi olyan információs társadalommal összefüggő szolgáltatása, amely Magyarországon elérhető, függetlenül attól, hogy az alkalmazásszolgáltató Magyarországon letelepedett […]*". Azonban az Ekertv. 1. § (1) bek. a) pontjának indokolása a letelepedési, származási ország elvének alkalmazását rendeli érvényesíteni miszerint „*A törvény, összhangban a 2000/31/EK irányelv („e-kereskedelem irányelv") 3. Cikkében foglalt rendelkezésekkel érvényesíteni kívánja az ún. „származási ország" elvet, amelynek lényege, hogy az Európai Unión belül az információs társadalommal összefüggő szolgáltatást annak a tagállamnak a joga szerint kell elbírálni, amelynek területéről azt ténylegesen, azaz a technológiai feltételek biztosításán túlmenő tartalommal nyújtják. Annak megállapítása, hogy ebből a szempontból mi minősül „tényleges" tevékenységnek tehát elsősorban technikai kérdés.*"[639]

Tehát hazai viszonylatba nézve az Ekertv.-ben érvényesülő területi elv és az azt kiterjesztő hatáselv, valamint az uniós szabályozáspolitikával összhangban implementálásra kerülő származási ország elvének érvényesítése összeütközést, azaz kollíziót idézhet elő a magyar nemzeti joghatóság szerinti LI tevékenység végrehajtása, és az ír nemzeti joghatóság szerinti szabályozást magára hatályosnak tekintő alkalmazásszolgáltató hatósági adatszolgáltatási megkeresések kiszolgálására irányuló magatartása terén. Hiszen nem mindegy, hogy az alkalmazásszolgáltató a megkeresések jogalap-, jogszerűségi vizsgálatát az ír, vagy a magyar nemzeti jog szerint végzi el, már ha erre egyáltalán van jogalapja, amely erősen megkérdőjelezhető, mivel a törvényességi kritériumok meglétéért az Nbtv. 61. § (1) bek. alapján az LI-t alkalmazó szerv a felelős, a megkeresett alkalmazásszolgáltatónak pedig

[639] T/5141. számú törvényjavaslat az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről. Részletes indokolás az 1. §-hoz. Magyarország Kormánya. 2001. szeptember.

adatszolgáltatási kötelezettsége áll fenn, nincsen jogalapja külső törvényességi kontrolt gyakorolni ilyen esetekben. Gyakorlatilag, hogy ha a Magyarországon igénybe vehető WhatsApp, Messenger szolgáltatást nyújtó írországi székhelyű Meta (aki egyben adatkezelő) titkosított kommunikációt biztosító alkalmazásszolgáltató európai szerverei Írországban találhatók, és ha a magyar nemzeti szabályozás az LI végrehajtása, engedélyezése kapcsán eltér a letelepedési, származási országban érvényes szabályozástól, és erre való hivatkozással az Ekertv. alapján együttműködésre kötelezett szolgáltató megtagadja azt, azaz az adatszolgáltatási megkeresés teljesítését az eljárás során, akkor fennáll a magyar titkos információgyűjtésre jogosult szerv és a külföldi székhelyű alkalmazásszolgáltató közötti nemzetközi jogvita, amelynek a nemzetközi, az uniós jog szerinti feloldása (például rendezése, szankcionálása, kikényszeríthetősége) jelenleg nem kidolgozott. Azonban annak megállapítása szükséges, hogy 2023 decemberétől a Messenger E2EE bevezetésével sem a WhatsApp, és már sem a Messenger tekintetében nem hatályos az Ekertv. 3/B. § a Metára a kommunikációs tartalom tekintetében, azonban a nem E2EE-vel ellátott adatok, mint például a metaadatok tekintetében az. Azonban fontos kiemelni, hogy az Ekertv. 3/B. § és 13. § rendelkezéseink 2016-os megjelenésével a jogalkotó egy az IKT környezet fejlődéséből adódó joghézagot volt hivatott a technológiasemlegesség elvét figyelembe véve kitölteni az alkalmazásszolgáltatói együttműködés titkos információgyűjtés során megvalósuló törvényi szintű rendezésével.

Részkövetkeztetésként az alkalmazásszolgáltatók írországi székhelyű disztribútorainak (Meta) hatósági, így a nemzetbiztonsági, bűnüldözési LI célú adatszolgáltatási megkereséseinek kiszolgálását megtagadó gyakorlatával kapcsolatban a fentiek alapján megállapítható, hogy azt a letelepedési, származási ország elvén alapuló ír nemzeti joghatósági szabályok alapján alkalmazott joggyakorlat szerint teszik, amely esetenként kollízióban állhat a magyar nemzeti joghatóság szerinti LI szabályozással, mely gyakorlat így a hazai törvények alapján jogellenes lehet. Ez feltételezhető a többi tagállam vonatkozásában is. Megoldásként jogi kötőerővel rendelkező szankció, kényszer az együttműködést megtagadó magatartások okán álláspontom alapján jelenleg nincsen biztosítva tekintettel a Meta 10 éves gyakorlatára.[640] Hazai viszonylatban mind az Eht. (NI-ICS), mind az Ekertv. (alkalmazásszolgáltató) tartalmaz szankcionálási rendelkezéseket a felügyeleti hatóság, azaz az NMHH számára, azonban ismert szankcionálási joggyakorlat ezen a téren nem áll rendelkezésre, akár csak a nemzetközi térben

[640] Az NMHH az Ekertv. 16/H. § (1) bek. alapján a 3/B. §-ban vagy a 13/B. §-ban meghatározott együttműködési kötelezettségét megszegő alkalmazásszolgáltatót 100.000 forinttól 10.000.000. forintig terjedő bírsággal sújthatja, mely álláspontom alapján nem alkalmas a visszatartó hatás kiváltására például egy Meta, Apple esetén.

sem. Tekintettel Írország opt out státuszára sem az EUMSz. SZBJT, sem az ENYH irányelv, sem a Tanács 2006/960/IB kerethatározat szupranacionális uniós jog szerinti rendelkezései nem nyújtanak a Bizottság, vagy az EUB szintenjén kikényszeríthető megoldást. Tehát a fentiek alapján a jövőben is hatékony alkalmazásszolgáltatási LI képesség biztosítása érdekében nélkülözhetetlen lesz a kölcsönös bizalmon alapuló nemzetközi együttműködés fokozása az információcserén túl a jövő LI képességei kialakításának lehetőségét is figyelembe véve, a nemzeti szuverenitás tiszteletben tartása mellett.

Az Unión belüli tagállamközi együttműködésre jó gyakorlatként hozható a GDPR (5) preambulumbekezdése és a 60. cikk szerinti együttműködés a fő felügyeleti hatóság és a többi érintett felügyeleti hatóság között, valamint a GDPR 61. cikke szerinti eljárás az ún. kölcsönös segítségnyújtás egykapus nemzeti adatvédelmi hatósági együttműködési rendszere.[641] Ez a személyes adatok határokon átnyúló kezelése esetén megvalósuló eljárások során biztosít a tagállamok hatóságai számára jogsegélyt, egyben a nem együttműködő magatartás szankcionálásával, akár a fellebbviteli szerv, az EDBP által, melyre példa a 4.2.3. részfejezetben ismertet C-311/18. számú Meta adatkezelését érintő EUB ügy kapcsán az EDPB-nek a norvég adatvédelmi szabályozó, fő felügyeleti hatóság kezdeményezésére meghozott 2023. október 27-ei kötelező erejű döntése,[642] valamint annak a 2023. november 10-ei végrehajtási határozata.[643] Továbbá az értekezés vizsgálatának nem képezi szorosan tárgyát, de indokolt megemlíteni az Ekertv. aktuális, 2024. február 17-ei hatályos módosítását, az internetes közvetítő szolgáltatások egyes szabályairól szóló 2023. évi CIV. törvény 27. - 32. §-ai alapján, amelyek azonban nem érintették az Ekertv. 3/B. § és 13/B. rendelkezéseit.[644]

---

[641] Lásd: Dr. Balogh Gyöngyi - Dr. Hackspacher Andrea - Dr. Bíró János - Dr. Szabó Endre Győző - Dr. Számadó Tamás (2020): *A Nemzeti Adatvédelmi és Információszabadság Hatóság eljárásai*. Budapest: NKE. 37-45. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/15005/A%20Nemzeti%20Adatvedelmi%20%C3%A9s%20Informacioszabadsag%20Hatosag%20eljarasai.pdf?sequence=3&isAllowed=y (Letöltés ideje: 2024. február 29.)

[642] Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR) Adopted on 27 October 2023. EDPB. Online: https://edpb.europa.eu/system/files/2023-12/edpb_urgentbindingdecision_202301_no_metaplatformsireland_en_0.pdf (Letöltés ideje: 2024. február 29.)

[643] Végrehajtási utasítás a Meta Platforms Ireland Limited ügyében az ír adatvédelmi törvény (Data Protection Act) 133. cikk (9) bek. és 133. cikk (10) bek., valamint a GDPR 60. és 66. cikkei alapján. EDPB. Online: https://edpb.europa.eu/system/files/2023-12/nationalenforcementnotice202311_ie_metaplatformsireland_en_0.pdf (Letöltés ideje: 2024. február 29.)

[644] A T/6064. sz. törvényjavaslat általános indokolása szerint a törvény célja a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról szóló, 2022. október 19-i (EU) 2022/2065 európai parlamenti és tanácsi rendelet (digitális szolgáltatásokról szóló rendelet) adaptációja. A törvény garanciális rendelkezéseket állapít meg, így biztosítva, hogy a közvetítő szolgáltatók határon átnyúló tevékenységére vonatkozó egységes uniós előírások hazánkban az uniós jogintézményekkel összhangban érvényesüljenek, mely okán rögzíti például a digitális szolgáltatási koordinátor hatósági eljárásainak és nemzetközi együttműködésének szabályait is.

4.4.3. Az „IKT boom” várható hatásai az alkalmazásszolgáltatási LI-re

Az értekezés korábbi kutatási cselekményei alapján megállapításra került az alkalmazásszolgáltatások központi szerepének további növekedése a lakossági célú kommunikációs igények kiszolgálásában. A statisztikák 2024-ben 3,42 Mrd, 2025-ben pedig 3,51 Mrd alkalmazásszolgáltatás felhasználót vetítenek előre globális szinten, a Meta szolgáltatásainak (WhatsApp, Messenger) európai piacvezetésével, az iMessage, a Telegram, a Signal, és a Viber mellett. Trend az alkalmazásszolgáltatások kriptográfiai környezetének folyamatos fejlődése, amely vonatkozásában a Messenger 2023 decemberi alapértelmezett E2EE bevezetése, és az iMessage 2024. márciusi „anti-kvantumszámítási” képességgel bíró PQ3 kriptográfiai protokollja alapján megállapítható, hogy a 2014/2016-os időszakot követően napjainkra ismét egy „titkosítási verseny” kezd kialakulni az alkalmazásszolgáltatások piacán, melynek része a 4.2.2. részfejezetben vizsgált felhasználói anonimizálás elterjedésének nemzetbiztonsági, bűnüldözési szempontú fokozott problémaköre. A fokozódó személyes adatvédelmi előírások következtében megjelenő technológiai, kriptográfiai válaszlépések, az alkalmazásszolgáltatások esetében a jogellenes tevékenységek számára is konspiratív lehetőségeket biztosítanak, melyek a feldolgozott esettanulmányok alapján a terrorizmus, szervezett bűnözés, extrémizmus, emberiesség elleni bűncselekmények, proliferáció, és végsősoron a gyermekpornográfia során online terjesztés, kapcsolattartás céljából is számos esetben igénybevételre kerültek. Ez korlátozza, végsősoron ellehetetleníti a DPI jellegű monitoring LI képességet, így sértve az egyes államok nemzetbiztonsági, bűnüldözési érdekeit. Nemzetközi szinten vizsgálatra kerültek az egyes államok, informális és formális nemzetközi együttműködéseinek normatív és technológiai LI válaszintézkedései. Továbbá áttekintésre került a hazai alkalmazásszolgáltatási LI szabályozás, amely kapcsán megállapítható, hogy hasonlóan a többi vizsgált állam jogszabályaihoz, az technológiai okokból fokozottan korlátozottan hatékony az E2EE-vel védett online kommunikáció LI-je tekintetében. Azonosításra került a letelepedési/származási ország elvének és a hatáselv normatív kollíziója a hatósági, így nemzetbiztonsági, bűnüldözési célú adatszolgáltatási megkeresések teljesítésének megtagadása tekintetébe, egyben a gyakorlatban megvalósuló igencsak vitathatóan legitim, jogszerű alkalmazásszolgáltatói kvázi „törvényességi kontroll” intézményesülésével. Összefoglalva álláspontom alapján a 21. század IKT boom-jának, az IKT környezet alkalmazásszolgáltatásokkal kapcsolatos fejlődésének kiemelt nemzetbiztonsági, bűnüldözési érdekeket sértő várható negatív hatásai, kihívásai az alábbiak:

- az infokommunikációs felhasználói anonimitás lehetőségének fokozódása;
- az állami, az uniós és a nemzetközi jog „felett állás” státuszát gyakorló globális szolgáltatók hatósági együttműködése korlátozódásának veszélye;
- az E2EE-t integráló online kommunikációt biztosító alkalmazásszolgáltatások igénybevételének további terjedése a titkos információgyűjtéssel érintettek körében;
- az infokommunikációs szolgáltatásoknál az E2EE általánossá válása, és a további innovatív kriptográfiai eljárások fejlődése.

A fenti LI jellegű kihívásokra az alkalmazásszolgáltatási trendek, a biztonsági környezet negatív változása, és a nemzetközi kitekintés során azonosított pozitív gyakorlat, válaszok alapján indokolt hazai alternatívát is javasolni az értekezés keretében kiteljesítve annak tudományos kutatási módszertanát, a gyakorlat számára is hasznosítható, alkalmazott jellegű tudományos eredmény biztosítása érdekében. Azonban a javaslattételt megelőzően indokolt figyelembe venni az LI-vel kapcsolatos nemzetközi gazdasági trendeket az erőforrásigény meghatározása érdekében. Az aktuális statisztikai adatok alapján a globális LI piac teljesítménye 2022-ben 3,00 Mrd USD volt, az iparági előrejelzések szerint a 2023-as 3,79 Mrd USD-ről 2032-re 24,53 Mrd USD-ra fog növekedni, mintegy 26,30%-os összetett éves növekedési rátát produkálva a 2023-2032 időszakban.[645] A valós idejű elemzések iránti igény növekedése és az internetes nyomon követés a törvény által a piac növekedését elősegítő kulcsfontosságú tényezők. Ezt érdemes összevetni az alkalmazásszolgáltatások 4.1.1. alfejezetben vizsgált piacának volumenével, mely az előrejelzések szerint a 2023-as 90,790 Mrd USD-ról 2029-re 274,080 Mrd USD-ra bővül, 20,2%-os összetett éves növekedési rátával, amely a 2024-es piacjelentés alapján 2031-re eléri a 475,982 Mrd USD-t, szintén tartva a 20,2%-os növekedést.[646] Tehát megállapítható, hogy míg az alkalmazásszolgáltatások globális piacának teljesítménye 2023-ban 90,8 Mrd USD volt, addig az LI piacé 3,8 Mrd USD, ami az alkalmazásszolgáltatói piac 4,2%-a. 2031-ben az előrejelzések szerint az arány valamit javulni fog az LI piac viszonyított 5,2%-os mutatójával. Az észak-amerikai LI piac erősödő dominanciája várható a digitális átállás széles körű elterjedése, a csúcstechnológiák használata,

[645] DHAPTE, Aarti (2024): Lawful Interception Market Overview. Market Research Report. Online: https://www.marketresearchfuture.com/reports/lawful-interception-market-9596?utm_term=&utm_campaign=&utm_source=adwords&utm_medium=ppc&hsa_acc=2893753364&hsa_cam=20298941735&hsa_grp=151951244833&hsa_ad=663291708226&hsa_src=g&hsa_tgt=dsa-2088470533900&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gad_source=1 (Letöltés ideje: 2024. február 29.)

[646] *Mobile Messaging Services Market Size & Share | Industry Forecast – 2031*. Global Market Research. 2024. Online: https://www.businessresearchinsights.com/market-reports/mobile-messaging-services-market-104760 (Letöltés ideje: 2024. február 26.)

az általános 5G lefedettség, a bővülő IKT eszközök szegmense, így ezek alapján a kormányzati szervek szignifikánsabban fokozódó LI igénye okán. Az USA globális LI piaci vezető részesedését az európai régió követi, melynek oka a várhatóan fokozódó terrorizmus, az EU digitalizációs stratégiai törekvései keretében megvalósuló széles körű internet-hozzáférés, az elektronikus hírközlő hálózati technológiába való jelentős beruházások, így a digitális infrastruktúra bővülése következtében a megnövekedő fogyasztás. Azonban az európai LI piac volumenéhez hozzátartozik az is, hogy abból a legnagyobb részesedést magáénak tudható nemzeti piac az Egyesült Királyságé lesz, mely a legdinamikusabban növekszik.[647] A fenti statisztikaiadatok, gazdaságnövekedési trendek alapján látható, hogy a piaci szereplők az alkalmazásszolgáltatások piacán érdekeltek inkább beruházni, szemben az LI piaccal, mely volumene töredéke az előbbinek. Ennek alapján előrevetíthető az alkalmazásszolgáltatási piacon jelenetősebben érvényesülő szabályozási lobbitevékenység, a jóval nagyobb előforrásokon alapuló technológiai innovációval, kutatás-fejlesztéssel egyetemben.

A fenti jellemzők és a nemzetközi LI piac növekedési trendelemzését követően álláspontom alapján a globális alkalmazásszolgáltatók hatósági adatszolgáltatási megkereséseinek kiszolgálását korlátozó gyakorlata szerinti uniós, nemzeti „jog felett állását” kezdő lépésként a bűnüldözési célú LI terén egy összetett, több lépcsős nemzetközi szolgáltatói együttműködés alapú LI szabályozási keret tudná feloldani tartósan és hatékonyan, amelyre az EU és tagállamai tekintetében a következő javaslatokat teszem:

- **Kriptográfia (E2EE) korlátozása az alkalmazásszolgáltatások tekintetében:** Egyfajta előfeltételként nélkülözhetetlen az E2EE jogi kötőerővel bíró korlátozása az alkalmazásszolgáltatások teljes körű LI képességének biztosítása érdekében a nemzetközi, uniós jog terrénumán azok globális jellegéből adódóan. Természetesen e mellett szükséges olyan alternatív kriptográfiai technológia alkalmazásának elősegítése, amely biztosítja az EU által elvárt személyes adatvédelmi, -biztonsági szintet, így a bűnüldözési érdek tekintetében egyensúlyban tartva az adatvédelem/biztonság értékduálját, és felszámolva a bűnüldözési érdek terén az „IKT adatvédelmi biztonság-deficitet”. Amennyiben az E2EE korlátozása nem valósul meg, álláspontom alapján akkor is indokolt az E2EE-től mentes adatok részleges LI képességének jelen koncepció szerinti nemzetközi szabályozása, és a javasolt koncepció alkalmazása.

[647] DHAPTE 2024

- **USA – EU CLOUD Act ernyő jogsegélyegyezmény**: Az E2EE korlátozására irányuló előfeltétel biztosítását követően első lépésként tekintettel az USA CLOUD Act végrehajtási megállapodásán alapuló bilaterális passzív jogsegélyegyezmény lehetőségére, indokolt egy USA (Igazságügyi Minisztérium) – EU (Bizottság) ernyőmegállapodás megkötése, hiszen az Uniónak az EUMSZ 216. cikke szerint lehetősége van harmadik országgal szerződést kötnie azon taxatív esetben is, amikor az a Szerződésekben meghatározott célkitűzések érdekében szükséges, mely jelen esetben az EUSZ 3. cikk (2) bek., valamint az EUMSZ SZBJT érvényesítése érdekében egyértelműen az, valamint az szolgálná az egyes tagállamok biztonság megteremtésére, fenntartására irányuló alkotmányos kötelezettségeit is.[648] Az ernyőmegállapodás esetén – ami kvázi bilaterális, de valójában multilaterális – az EU tagállamok bűnüldözési célú LI szervei így már az USA joghatósága szerinti is felhatalmazást szereznének az USA székhelyű anyavállalattal rendelkező globális alkalmazásszolgáltatóktól történő adatkérésekre, az alkalmazásszolgáltatók irányába pedig az USA normarendszere szerinti jogi kötőerővel bíró kötelezettség keletkezne ezen megkeresések kiszolgálására, a szolgáltatói együttműködés alapú LI érvényesítésére. Tehát a fenti USA – EU CLOUD Act ernyő jogsegélymegállapodás javaslat okszerű, és indokolt.

- **Uniós belső jogalkotás:** Természetesen az USA – EU CLOUD Act ernyő jogsegélyegyezmény előfeltétele a belső uniós jogalkotás, egyfelől a tagállamok közös döntése arra vonatkozóan, másfelől mind az uniós jog, mind az egyes tagállamok bűnüldözési cél LI szabályozásának harmonizálása, megfeleltetése az USA szabályozási elveivel, elsősorban az alapvető jog korlátozásának, engedélyezésének tekintetében. Ez álláspontom alapján a tagállamok szintjén drasztikus normamódosítási trendet nem jelente, tekintettel az EJENY-ben foglalt alapelvek elfogadásával és azok nemzeti jogba történő érvényre juttatásával. Továbbá indokolt közvetlen és kikényszeríthető EU rendeleti szintű jogforrásban kötelezni az alkalmazásszolgáltatókat a hatósági, LI célú együttműködésre.

- **Adatkérések rendje a tagállami LI szervek tekintetében**: Nem EU szintű egykapus adatkérési és -szolgáltatási modell bevezetését javaslom az USA-beli IKT szolgáltatók

[648] Az EUSZ 3. cikk (2) bek alapján „*Az Unió egy belső határok nélküli, a szabadságon, a biztonságon és a jog érvényesülésén alapuló olyan térséget kínál polgárai számára, ahol az […] a bűnmegelőzésre és bűnüldözésre vonatkozó megfelelő intézkedésekkel párosul.*" Az Alaptörvény Nemzeti Hitvallás fejezetében „*Valljuk, hogy a polgárnak és az államnak közös célja a jó élet, a biztonság, a rend, az igazság, a szabadság kiteljesítése.*"

irányba, tekintettel a tagállami bűnüldözői érdek érvényesítésének azon szenzitív vertikumára, amely a tagállamok szuverenitásának szempontjából nem tartozik önkéntes nemzetközi megosztás hatálya alá, azonban mégis szükséges egyfajta egykapus modell bevezetése javaslatom alapján tagállami szintre delegálva. Ennek értelmében adott tagállam kijelölt LI szerve lenne jogosult az érintett alkalmazásszolgáltatótól adatot igényelni a többi nemzetközi LI alkalmazására, adatkérésre jogosult hatóság, szerv számra is, így a jog erejénél fogva kijelölve egy egykapus nemzetközi adatkérést végrehajtó nemzeti központi LI szervet tagállamonként. Magyarország tekintetében az Eht.-ben és az Ekertv.-ben megnyilvánuló koncentrált LI képességre törekvés jog- és szakpolitikai álláspontját javaslom figyelembe venni a szervezet kijelölése során. Azonban ebben az esetben felvetődik a 2.1. alfejezetben tárgyalt nemzetbiztonsági szolgálat külvilág előtti alaki megjelenése is, mely normatív feloldást igényel például a többi partner-, tagállam által is elfogadott törvényi kijelöléssel. Így biztosítottá válna mind az adatkérések egykapus tagállami modellje,[649] mind a tagállamon belüli megrendelőszervek adatkéréseinek kiszolgálása, nemzetközi koordinálása, és a nemzetközi adatkérések egységes joggyakorlatának biztosítása. A tagállami eljárásrend, a részletszabályok kidolgozása a nemzetközi, az uniós joghoz igazodó tagállami szabályozást igényel, kiemelt hangsúllyal a titkos információgyűjtés engedélyezése szabályainak, kontrollmechanizmusainak a partner-, tagállamok közötti normatív összehangolására.

- **Alkalmazásszolgáltatók általi vitathatóan legitim kvázi „törvényességi kontroll" felszámolása**: Végezetül a fenti modellben szükséges megszüntetni az alkalmazásszolgáltatói törvényességi kontroll gyakorlatát a hatósági megkeresések tekintetében, melyre álláspontom alapján a hatályos tagállami és nemzetközi, uniós jogszabályok alapján sincsen jogalap. Ennek egy az alkalmazásszolgáltatók és felhasználóik számára is transzparens, a nemzetközi emberi és alapvető jogok érvényesülését biztosító átlátható és nemzetközi bíróság útján is kikényszeríthető nemzetközi, uniós jogi, továbbá tagállami szinten alkotmányos, törvényi és végrehajtási szintű szabályrendszer a garanciája, melyet a magyar nemzeti szabályozás most is megvalósít a 2.3., 2.5., 3.3. és 4.4. alfejezetek részletes indoklása, bizonyítása alapján.

[649] Tagállamonként egy kijelölt az alkalmazásszolgáltatók irányába nemzetközi adatkérést végrehajtó nemzeti központi LI szerv.

A fenti javasolt bűnüldözési célú nemzetközi szolgáltatói LI együttműködési modellen tovább lépve, egy következő szinten integrálható lenne hozzá a nemzetbiztonsági érdekek bizonyos szintű érvényesítése, azaz a nemzetbiztonsági célú LI biztosítása, azonban ehhez mind az egyes tagállamok kölcsönös bizalma, mind az USA és az egyes tagállamok közötti kölcsönös bizalmon alapuló, egyértelmű, következetes szabályozásra van szükség, amely alapkövei a hatalmi ágak szétválasztásán alapuló fékek és ellensúlyok rendszere, a készletező adatgyűjtés tilalma, a szükségesség, az arányosság, és a törvényesség alapelveknek való megfelelés. Álláspontom szerint a nemzetbiztonsági célú tevékenységnek, titkos információgyűjtésnek, így az LI-nek vannak olyan, az értekezés 2.1. és 4.3. alfejezetében is ismertetett, törvényi szinten szabályozott résztevékenységi elemei, amelyek az egymással együttműködő tagállamok szuverenitását és biztonságát nem érintik, nem érinthetik negatívan, hanem kumulált szinten éppen, hogy erősítik azt, így hozzájárulva a nemzetközi szinten érvényesülő össztársadalmi szintű biztonság fenntartásához. Ilyen nemzetbiztonsági célú, de bűnüldözési érdekkörben is értelmezhető tevékenység például az Nbtv. 74. § ae) alpont szerinti nemzetbiztonsági érdek körében értelmezett terrorizmus és annak konvergenciája okán jelentkező elemi, például a szervezett bűnözéssel összefonódó terrorfinanszírozás, az egyéb transznacionális szervezett bűnözés, például a fegyver-, kábítószer-, ember-, műkincskereskedelem megelőzésében, felderítésében, megakadályozásában és elhárításában való közreműködés adott nemzetbiztonsági szolgálat által. Továbbá ebbe a kategóriába sorolható vizsgálandó cselekményként azonosítom az illegális migrációt, a szövetséges államok szuverenitásába beavatkozó harmadik állam és nem kormányzati szerv tevékenységét, az emberiesség elleni bűncselekményeket, valamint a további kiemelten magas társadalomra veszélyes bűncselekményeket. Innovatív szemléletbe, az IKT környezet változásából adódóan szintén beleérthető ebbe a körbe az E2EE kriptográfia korlátozása terén az uniós politikai egység megteremtésének potenciálját is magában hordozó gyermekek szexuális kizsákmányolása.

Álláspontom alapján a fenti keretek egyértelmű, nemzetközi és sarkalatos állami szabályozásával megteremthető az EU égisze alatt az uniós jog hatálya alá tartozó bűnüldözési érdekkör jelleggel, ugyan nemzetbiztonsági céllal megvalósuló, a részes államok kölcsönös bizalmán és egymás szuverenitásnak tiszteletben tartásán alapuló, az európai biztonsági térség erősítését célzó, uniós jogi kötőerővel és kikényszeríthetőséggel bíró multilaterális nemzetközi LI együttműködés. Az egykapus nemzetközi adatkérést végrehajtó nemzeti központi LI szerv kijelölésénél fontos annak a 2.1. részfejezetben tárgyalt alaki megjelenése, így például egy polgári nemzetbiztonsági szolgálat ilyen irányú feladatköre esetén szükséges a nemzetközi

szereplők számára is transzparens, konszenzuson alapuló törvényi kijelölés a mandátum részletes szabályozásával a kölcsönös bizalom, és az egymás szuverenitásának kölcsönös tiszteletben tartása iránti elköteleződés kifejezése érdekében.

A fenti javasolt nemzetközi szolgáltatói – bűnüldözési és nemzetbiztonsági célú – LI együttműködési modell álláspontom szerint a kor elvárásai szerint automatizálható, elektronikus adatkapcsolat útján megvalósuló technikai LI módszerré is átkonvertálható az ISLI modell keretében, hiszen az elméleti következtetések lényegi, gyakorlati értéket akkor hordoznak, ha azok komplex rendszerbe illeszthetők, implementálhatók és alkalmazhatók, szem előtt tartva a gyakorlatorientált kutatási eredményekkel szembeni alapvető elvárást. Álláspontom alapján ebből következik, hogy a DPI alapú technikai monitorig alkalmazásszolgáltatói LI-t az Eht. 92. § szerinti lenne optimális megvalósítani, természetesen annak a fentieket is figyelembe vevő felülvizsgálatát követően, hiszen ezen szabályozás már 20 éves, azonban előrelátó jellegnél fogva időtállóbbnak bizonyult jóval az Ekertv. 3/B. és 13/B. § rendelkezéseinél.[650] Az Eht. szerinti szabályozás adott, hiszen annak hatálya kiterjed az NI-ICS-re is a Bizottságnak az értekezés 2.6.3. részfejezetben ismertetett döntése alapján a Meta tekintetében a WhatsApp és Messenger, az Apple tekintetében az iMessage vonatkozásában, így a Telegram, a Signal és a Viber is ezen számfüggetlen személyközi hírközlési szolgáltatások közé sorolandó. Az alkalmazásszolgáltatási és hírközlési LI képességeket is integráló ISLI koncepciók fentiek és a 3.3.2. részfejezet szerinti nagyvonalú elméleti modelljét az alábbi 40. ábra hivatott szemléltetni.

[650] Az Ekertv 3/B. és 13/B. § rendelkezései kapcsán fontos kiemelni, hogy azok 2016-os kodifikálásával a jogalkotó egy az IKT környezet fejlődéséből adódó joghézagot volt hivatott a technológiasemlegesség elvét figyelembe véve kitölteni az alkalmazásszolgáltatói együttműködés titkos információgyűjtés során megvalósuló törvényi szintű rendezésével, melyet elsősorban az Európát érő iszlám fundamentalista terrortámadások indukáltak.

Verziószám / Jellemzők	ISLI		ISLI 2.0	
Szolgáltatás típusa	NB-ICS; internet-hozzáférési szolgáltatás	NI-ICS (alkalmazás-szolgáltatás)	NB-ICS; internet-hozzáférési szolgáltatás	NI-ICS (alkalmazás-szolgáltatás)
Javasolt hazai szabályozó norma	Eht. (92. § felülvizsgálatot követően)		Eht. (92. § felülvizsgálatot követően)	
Elsődleges kriptográfiai környezet	C2SE	E2EE	C2SE	E2EE
Ellenőrzött rendszer oldali szabványosított DPI LI képesség	van	nincs	van	nincs
Szükséges-e további normatív kriptográfiai korlátozás	általánosságban nem	igen	általánosságban nem	igen
Monitoring alrendszerrel érintett hírközlő rendszerelem helye	állam (Magyarország)	külföldi állam (pl.: Írország – Meta, Apple)	több állam területe, légtér, világűr (6G VHetNet)	Külföldi állam (pl.: Írország – Meta, Apple)
Monitoring alrendszerrel érintett hírközlő rendszerelem	hírközlő hálózat központi (core)rendszere	kiszolgáló szerver	hírközlő hálózat minden adat-forgalomirányítás végző eleme (műhold, HAPS, UAV, RAN, core stb.)	kiszolgáló szerver
Elsődleges szabályozás terrénuma	nemzeti	nemzetközi (EU-USA)	nemzetközi (EU-USA)	
Képesség nemzeti jellege	nemzeti	nemzetközi együttműködés	nemzetközi együttműködés	

40. ábra: Alkalmazásszolgáltatási/ hírközlési ISLI koncepciók nagyvonalú elméleti modellje (Szerk.: A szerző)

Részkövetkeztetésként megállapítható, hogy a fentiek szerinti prognosztizálható IKT trendek és tendenciák alapján az elektronikus számfüggő személyközi hírközlési szolgáltatás (NB-ICS) alapú kommunikáció hagyományos LI-jével szemben az internettechnológiát alkalmazó, applikáció alapú titkosított online kommunikációt biztosító alkalmazásszolgáltatások (NI-ICS) innovatív LI igényének fokozódása várható, amelyek központi DPI monitoring technikai LI módszere új, innovatív technológiai és szabályozási eljárásrendet követel meg, melyre a fentiek szerinti ISLI koncepcióba is illeszthető javaslatokat fogalmazom meg. Ezen összetett, több lépcsős nemzetközi szolgáltatói együttműködés alapú LI szabályozási keret főbb lépéseiként

azonosítottam az E2EE korlátozásának szükségességét az alkalmazásszolgáltatások tekintetében, az USA – EU CLOUD Act ernyő jogsegélyegyezmény megkötését uniós szinten, az ezzel kapcsolatos uniós belső jogalkotás és az adatkérések, LI rendjének szabályozását a tagállami LI szervek tekintetében, végsősoron pedig az alkalmazásszolgáltatók általi igencsak vitathatóan legitim kvázi „törvényességi kontroll" felszámolását.

A fentiek alapján megállapítható, hogy mind az NB-ICS, mind az NI-ICS keretében végbement kommunikáció nemzetbiztonsági célú LI-jének hatékonysága érdekében nélkülözhetetlen lesz a kölcsönös bizalmon alapuló nemzetközi együttműködés fokozása az információcserén túl a jövő LI képességei kialakításának lehetőségét is figyelembe véve, a nemzeti szuverenitás tiszteletben tartása mellett. Az együttműködés a hazai nemzeti érdekeket figyelembe véve az elektronikus hírközlési szolgáltatások LI-je tekintetében elsődlegesen az EU tagállamaival, Európában a legnépszerűbb vizsgált alkalmazásszolgáltatások LI-je tekintetében pedig elsődlegesen az USA kormányzati szerveivel, az IKT piac szereplőivel kell, hogy megvalósuljon.

Azonban a piaci volumenelemzés alapján előrevetíthető a globális alkalmazásszolgáltatások piacán jelentősebben érvényesülő szabályozási lobbitevékenység, a jóval nagyobb előforrásokon alapuló technológiai innovációval egyetemben, szemben a globális LI piacéval, mely volumene 2030-ig kb. 4-5%-a lesz az alkalmazásszolgáltatások globális piacának. A 2022. december 15-ei „*Digitális jogokról és elvekről szóló európai nyilatkozat*" kapcsán Margrethe Vestager, a Bizottság digitális korszakért felelős ügyvezető alelnöke elmondta, hogy: „*Az emberek javát szolgáló, biztonságos technológiákat akarunk, amelyek tiszteletben tartják jogainkat és értékeinket. Méghozzá az online térben is. És azt szeretnénk, hogy mindenkinek lehetősége legyen aktív szerepet vállalni egyre nagyobb mértékben digitalizált társadalmainkban.*"[651] – Szerzői kiegészítés: A nemzetbiztonsági, bűnüldözési érdekek érvényesülése mellett!

[651] *A Bizottság az EU-n belül mindenkire érvényes digitális jogokról és elvekről szóló nyilatkozatot terjeszt elő.* Európai Bizottság. 2022. Online: https://ec.europa.eu/commission/presscorner/detail/hu/IP_22_452 (Letöltés ideje: 2024. február 29.)

4.5. Részkövetkeztetések

Az értekezés érdemi tartalmi harmadik részében, azaz a 4. fejezetben az alkalmazásszolgáltatások LI-jét érintő IKT trendek, tendenciák komplex elemzése került elvégzésre a meghatározott kutatási módszertan alapján, a hipotézisek alátámasztása és az új tudományos eredmények eléréséhez szükséges részkutatómunka elvégzése érdekében. A fejezeten belül vizsgálat tárgyát képezte az alkalmazásszolgáltatások felhasználói trendjei, az alkalmazásszolgáltatásokkal összefüggő adatvédelmi trendek, a biztonsági kihívási tendenciák és válaszintézkedések a nemzetközi térben, az alkalmazásszolgáltatások LI-jének hatályos hazai normatív, szervezeti evolúciója, trendjei. Az egyes al- és részfejezetekben a meghatározott kutatási módszertan alkalmazása során elvégzett cselekmények alapján az alábbi fő részkövetkeztetések vonhatók le:

4.1. alfejezet: Az alkalmazásszolgáltatások 2030/31-ig tartó piaci tendenciáinak elemzése alapján bizonyítottá vált azok központi szerepének további növekedése a lakossági, személyközi célú kommunikáció kiszolgálásában, a globális piac gazdasági volumenét az előrejelzések alapján 2029 és 2031 között mintegy 1,7-szeresére növelve. A statisztikák 2024-ben 3,42 Mrd, 2025-ben pedig 3,51 Mrd alkalmazásszolgáltatás felhasználót vetítenek globális szinten. Európában a piacvezetők jelenleg és a továbbiakban is a Meta szolgáltatásai (WhatsApp, Messenger), az iMessage, a Telegram, a Signal, és a Viber mellett.

4.2. alfejezet: Az alfejezet következtetéseként megállapítható, hogy a jelentősebb piacvezető alkalmazásszolgáltatók, mint például a Meta folyamatosan javítják az alkalmazások kriptográfiai tulajdonságait a felhasználók kommunikációjának biztonságosabbá tétele valamint, marketing célból egyaránt, amely egyrészről a protokollok, algoritmusok fejlesztéséhez, másrészről az E2EE alkalmazásának általános elterjedéséhez vezetett egyfajta keresleti/kínálati öngerjesztő jelenségként. Erre hatással volt a 2013-as Snowden ügy, amelyet követően a vizsgált alkalmazásszolgáltatások E2EE integrálási tendenciát kezdtek el produkálni, egyben új „titkosított” alkalmazások megjelenésével, a potenciális felhasználói bizalomvesztésre adott piaci válaszként a kereslet fenntartása, helyreállítása érdekében. A Messenger 2023 decemberi alapértelmezett E2EE bevezetése, és az iMessage 2024. márciusi „anti-kvantumszámítás” képességgel bíró E2EE PQ3 kriptográfiai protokollja alapján megállapítható, hogy a 2014/2016-os időszakot követően napjainkra ismét egy „titkosítási verseny” kezd kialakulni az alkalmazásszolgáltatások piacán, már előre reagálva az IKT

környezet fejlődésének kvantumszámítás alapú innovációjára. Bemutatásra került az alkalmazásszolgáltatásokkal kapcsolatos anonimitás kihívása, mely okán javaslatom alapján globális, de legalább is EU szinten követelményként kellene támasztani az alkalmazásszolgáltatók számára a felhasználó természetes személy regisztrációja során a mobil hívószám megadásának kötelezettségét azonosíthatósági célból, amely megőrzésére és szolgáltatására az alkalmazásszolgáltató kötelezett lenne szabályozott módon, így a jogosult rendvédelmi szervek, akár nemzetbiztonsági célú LI keretében közvetetten ugyan, de hazai viszonylatban az Eht. mögöttes szabályai alapján már jóval hatékonyabban be tudnák azonosítani a tevékenységgel érintett természetes személyt, akihez egyértelműen köthető lenne a kommunikációja. **Tehát következtetésképpen bizonyítást nyert, hogy az alkalmazásszolgáltatásokkal kapcsolatos nemzetközi normatív adatvédelmi és elektronikus információbiztonsági környezet fejlődése hátrányosan érinti az azokon végbement kommunikáció LI-jének technológiai hatékonyságát.** [H3] A 2.4. alfejezettel és a 2. fejezet részkövetkeztetéseivel összefüggésben megállapításra került, hogy az EU jogpolitikai törekvései fokozzák az adatvédelmi intézkedések az adatbiztonság szintjére irányuló elvárásokat, melyet az EUB C-311/18. számú ügyében hozott Ítélete is mutat. Ez az EU és USA kapcsolatokban az EU-ból az USA-ba irányuló adatkezelés terén is megnyilvánul, melynek aktuálisan a DPF szab megfelelési keretszabályokat. Azonban az értekezés vizsgálatához kapcsolódó releváns következtetés, hogy **az EU-ból az USA-ba irányuló személyes adatkezelés GDPR ellenességét és annak újraszabályozását az USA nemzetbiztonsági célú titkos információgyűjtő tevékenységével kapcsolatosan feltárt adatvédelmi incidens jellegű tényezők indukálták, melyek okán a DPF megfelelőségével kapcsolatban az EDPB még 2023-ban is kritikát fogalmazott meg.**

4.3. alfejezet: Megállapításra került, hogy a fokozódó személyes adatvédelmi előírások következtében az alkalmazásszolgáltatások kriptográfiai tulajdonságainak fejlődése egyben olyan jogellenes tevékenységek, mint a feldolgozott esettanulmányok alapján a terrorizmus, szervezett bűnözés, extrémizmus stb. számára is konspiratív lehetőséget biztosít. A titkosított kommunikációt biztosító alkalmazásszolgáltatások jogellenes tevékenység során történő kommunikációs célú felhasználásának kiemelt társadalmi jelentőségét az ENSZ Emberi Jogi Főbiztosának fellépése is jelzi, azonosítható a köz- és nemzetbiztonsági érdeksérelem. Tehát **az elvégezett esettanulmányfeldolgozás alapján a gyakorlat jelentősen altámasztja az alkalmazásszolgáltatások LI-jének létjogosultságát, indokoltáság és szükségességét. A fentiek alátámasztják és erősítik a 3.3. alfejezetben levezetett „IKT LI adatvédelmi**

biztonság-deficit" teóriát. Áttekintésre és vizsgálatra került a nemzetközi formális és informális LI együttműködések vertikuma, valamint az egyes nemzeti szabályozások. Ennek keretében **bemutatásra került az USA bilaterális LI célú együttműködési lehetőségének jogilag is szabályozott formája a CLOUD Act megállapodás**, amely értelmében az USA igazságügyi szerve 2018-at követően végrehajtási passzív jogsegélymegállapodást köthet adott partnerország kormányzati szervével. Az EU-t vizsgálva a bűnüldözési célú multilaterális LI együttműködés kapcsán megállapításra került, hogy **tényleges műveleti célú aktív/ passzív jogsegély alapú támogatást biztosítanak az EUMSZ SZBJT keretén belüli másodlagos uniós jogi aktusok (ENYH irányelv, Tanács 2006/960/IB kerethatározata), amelyek implementálásra kerültek a hazai jogban, viszont a Metának és Apple-nek európai székhelyet adó Írország opt out, azaz kimarad a jogforrások hatálya alól**. Az EU-s LI célú bilaterális együttműködés keretében a francia-német tengely E2EE-t korlátozó EUB igénye került vizsgálatra, Németország aktuális E2EE-t áthidaló aktív kémprogram LI módszerének szabályozásával egyetemben. **Vizsgálva az európai országok nemzetbiztonsági célú multilaterális formációit (Berni Klub) megállapításra került, hogy olyan joghatást kiváltó kötőerővel bíró jogalkotási mandátumuk, mint az EU-nak nincsen**. Az alkalmazásszolgáltatások LI-jét érintően a CSAM vitájában képviselt hazai külpolitikai álláspont alátámasztja az értekezés során eddig levont következtetéseket, miszerint **az IKT környezet változásaiból adódó LI jellegű kihívásokra válaszul nemzetközi szintű együttműködésre van szükség a nemzetbiztonsági, bűnüldözési célú LI tevékenység folyamatos, hatékony fenntartása érdekében a 21. században.** [H4]

A CSAM vita mutatja az adatvédelem/biztonság kiegyensúlyozott értékduáljának elmozdulását a biztonság hátrányára, mely alapján az „IKT LI adatvédelmi biztonság-deficit" teória szintén igazolást nyert a gyakorlatban. Tapasztalható egyfajta politikai szintű elköteleződés az uniós tagországok nagyobb hányadánál az E2EE korlátozásának uniós szintű szabályzási keret közé ültetésére a gyermekek szexuális kizsákmányolásának IKT szolgáltatások terén történő visszaszorítása érdekében. Álláspontom alapján a CSAM potenciális egységkovácsoló lehetőséget hordoz magában az EU politikai vezetése tekintetében, egyben eddig nem látott lendülettel, ami az E2EE közbiztonsági, bűnüldözési célú korlátozását jelenti, így megnyitva a lehetőséget az „IKT LI adatvédelmi biztonsági-deficit" visszabillentésére a biztonság javára. **Álláspontom alapján amennyiben az E2EE korlátozása terén jogalkotás várható, az szabályzás jellegű korlátozás lesz**, tekintettel arra, hogy az E2EE kriptográfia jelenlegi ismeretink alapján, a 2.7.2. fejezet szerinti gyakorlati titkosságot biztosít. [H1; H3; H4]

Az európai piacvezető Meta hatósági adatszolgáltatási attitűdjét mintavételezési céllal bemutató tendenciaelemzés során megállapításra kerül a szolgáltatóhoz beérkező hatósági megkeresések globális számának exponenciális növekedése, mely a mobilinternet fogalom bővülésével azonos tendenciát mutat. **Bizonyítható az internet alapú titkosított kommunikációt biztosító alkalmazásszolgáltatások, egyéb közösségi média platformok hatósági – így bűnüldözési, nemzetbiztonsági – érdeket sértő tevékenységgel való fokozódó érintettsége, azaz a jogsértő cselekmények során történő logisztikai, kommunikációs célú alkalmazása**. Az igénybevétel bővülése a mobilinternet szolgáltatások keresletének növekedésével azonos tendencia mentén. [H1] Megállapításra került, hogy **az alkalmazásszolgáltató a hatósági együttműködések keretében az egyes tagállamok jogosult hatóságai, így LI szervezetei által közvetlenül megküldött megkeresések jelentős hányadát átlagosan megválaszolja, míg kb. az ¼-ének teljesítését megtagadja egyfajta vitathatóan legitim szolgáltatói „törvényességi kontroll" keretében a kb. 10 éves gyakorlat alapján.** Álláspontom szerint a vizsgált Meta fenti 10 éves gyakorlata alapjaiban sérti az egyes demokratikus államok szuverenitását, biztonsági érdekeit, hiszen az alkotmányos garanciák, a hatalmi ágak szétválasztása, a fékek és egyensúlyok érvényesülése mellett történő közhatalom gyakorlása során az állami kényszer – mely ez esetben az alkalmazásszolgáltató által a hatóságok, így a bűnüldöző, nemzetbiztonsági szervek tevékenységével érintett természetes személlyel összefüggően kezelt adatok átadására irányul – legitim és feltétlen. Az adatszolgáltatás megtagadása közvetlenül nemzetbiztonsági, bűnüldözési érdeket sérthet, tehát jogszerűtlen, azonban ezen jogsértő magatartás általános szankcionálási formájára, az együttműködés kikényszerítésére nem találtam következetes joggyakorlatot. A fentiek alapján **elengedhetetlen a jövő sikeres LI tevékenysége szempontjából a formális, jogi kötőerővel és hatékony kikényszeríthetőséggel bíró nemzetközi együttműködés a globális alkalmazásszolgáltatók LI terén megvalósuló jogkövető magatartásra bírása érdekében, mely terrénuma álláspontom alapján az európai országok tekintetében az EU kell, hogy legyen, egyben uniós jogalkotást is magával hozva.** [H4]

A vizsgált esettanulmányok, a nemzetközi LI gyakorlat, a szolgáltatói hatósági együttműködési hajlandóság, és a prognosztizálható IKT trendek és tendenciák alapján **bizonyításra került, hogy az elektronikus számfüggő személyközi (mobiltelefon) hírközlési szolgáltatás hagyományos LI-jével szemben az internettechnológiát alkalmazó, applikáció alapú titkosított online kommunikációt biztosító alkalmazásszolgáltatások innovatív LI**

igényének fokozódása várható, amelyek központi monitoring technikai LI módszere új, innovatív technológiai és szabályozási eljárásrendet követel meg, melyre az értekezés javaslatot is megfogalmaz. [H1]

4.4. alfejezet: Az Ekertv. 3/B. és 13/B. § szerinti szolgáltatói együttműködés alapú alkalmazásszolgáltatói LI szabályozás időtállósága kapcsán levonható következtetés, hogy az a 2.4.1. részfejezetben ismertetettek szerint már a hatálybalépésének időpontjában is csak korlátozottan volt hatékony, tekintettel arra, hogy a vizsgált alkalmazásszolgáltatások ¾-e addigra már E2EE-t alkalmazott. Ennek aktualitását nézve megállapítható, hogy az E2EE alapértelmezettségének, azaz kizárólagosságának folyamatos terjedésével (például Messenger 2023. december), valamint a legújabb kvantumszámításnak is ellenálló kriptográfiai algoritmusok megjelenésével (iMessage 2024. március) az LI hatékonysága tovább korlátozódik. Tehát bizonyításra került, hogy az alkalmazásszolgáltatások LI-jének hazai jogszabályi környezete a hatékonyság szempontjából 2023-hoz képest, kb. 8-10 éve fokozódóan korlátozott az alkalmazásszolgáltatások kriptográfiai környezetének fejlődéséhez képest, így **az alkalmazásszolgáltatások globalizációjának, valamint azok kriptográfiai környezeti fejlődésének hatására az elektronikus hírközlési szolgáltatások LI-jét szabályozó hatályos hazai normarendszer hatékonysága erodálódik, e téren az LI képesség rezilienciája korlátozott**. [H1; H3] Azonban az Ekertv. fenti 2016-os módosításával a jogalkotó egy az IKT környezet fejlődéséből adódó joghézagot volt hivatott úttörő módon, a technológiasemlegesség elvét figyelembe véve kitölteni az alkalmazásszolgáltatói együttműködés titkos információgyűjtés során megvalósuló törvényi szintű rendezésével.

A 4.3. alfejezet szerinti átfogó nemzetközi kitekintés során megállapításra került, hogy a vizsgált országok (USA, Egyesült Királyság, Franciaország, Németország) hasonló szabályozási kihívásokkal küzdenek, mint Magyarország az alkalmazásszolgáltatásokat érintő DPI monitoring alapú LI módszer tekintetében. Erre egyfelől „megoldást” a rendkívül nagy pénzügyi erőforrásigényes rejtjelfejtés nyújthat, azonban csak ideiglenesen a kriptográfiai eljárások folyamatos fejlődése okán a 2.7. alfejezetben és a 4.2.1. részfejezetben ismertetettek alapján. Másfelől az aktuális német jogalkotási példánál maradva az aktív kémprogram alapú LI módszer is alternatíva az E2EE kezelésére, azonban ez licencigénye okán csak korlátozott mennyiségű IKT eszköz tekintetében biztosíthatja az LI-t, valamint ez jóval költségesebb, mint a szolgáltatói költségviselés lehetőségét magában hordozó központi DPI monitoring alrendszer alapú LI. Tehát **bizonyításra került, hogy az alkalmazásszolgáltatásokkal kapcsolatos**

nemzetközi normatív adatvédelmi és elektronikus információbiztonsági környezet fejlődése hátrányosan érinti az azokon végbement kommunikáció LI-jének technológiai hatékonyságát. [H3]

A globális alkalmazásszolgáltatók írországi székhelyű disztribútorainak (Meta) hatósági, így a nemzetbiztonsági, bűnüldözési LI célú adatszolgáltatási megkereséseinek kiszolgálását megtagadó gyakorlatával kapcsolatban megállapításra került, hogy azt a letelepedési, származási ország elvén alapló ír nemzeti joghatósági szabályok alapján általuk alkalmazott joggyakorlat szerint teszik, amely esetenként kollízióban állhat a magyar nemzeti joghatóság szerinti LI szabályozással, mely gyakorlat így a hazai törvények alapján jogellenes lehet. Ez feltételezhető a többi tagállam vonatkozásában is. Megoldásként jogi kötőerővel rendelkező szankció, kényszer az együttműködést megtagadó magatartások okán álláspontom szerint jelenleg nincsen biztosítva a Meta 10 éves gyakorlata alapján. Tekintettel Írország opt out státuszára sem az EUMSZ SZBJT, sem az ENYH irányelv, sem a Tanács 2006/960/IB kerethatározat szupranacionális uniós jog szerinti rendelkezései nem nyújtanak a Bizottság, vagy az EUB szintjén kikényszeríthető megoldást. Tehát **bizonyításra került, hogy a jövőben is hatékony alkalmazásszolgáltatási LI képesség biztosítása érdekében nélkülözhetetlen lesz a nemzetközi együttműködés fokozása az információcserén túl a jövő LI képességei kialakításának lehetőségét is figyelembe véve, a nemzeti szuverenitás tiszteletben tartása mellett, az alkalmazásszolgáltatások LI-je tekintetében elsődlegesen az Egyesült Államok kormányzati szerveivel, az IKT piac szereplőivel**. [H4]

A prognosztizálható IKT trendek és tendenciák alapján bizonyításra került, hogy **az elektronikus számfüggő személyközi hírközlési szolgálatás (NB-ICS) hagyományos LI-jével szemben az internettechnológiát alkalmazó, applikáció alapú titkosított online kommunikációt biztosító alkalmazásszolgáltatások (NI-ICS) innovatív LI igényének fokozódása várható, amelyek központi DPI monitoring technikai LI módszere új, innovatív technológiai és szabályozási eljárásrendet követel meg**, melyre 3.3.2. részfejezet szerinti ISLI koncepcióba is illeszthető javaslatokat fogalmaztam meg. Ennek az összetett, több lépcsős nemzetközi szolgáltatói együttműködés alapú LI szabályozási keret főbb lépéseiként azonosítottam és fejtettem ki az E2EE kriptográfia korlátozásának szükségességét az alkalmazásszolgáltatások tekintetében, az USA – EU CLOUD Act ernyő jogsegélyegyezmény megkötését szupranacionális uniós szinten, az ezzel kapcsolatos uniós belső jogalkotás és az

adatkérések, LI rendjének szabályozását a tagállami LI szervek tekintetében, végsősoron pedig az alkalmazásszolgáltatók általi igencsak vitathatóan legitim kvázi „törvényességi kontroll" felszámolását. Álláspontom alapján ebből következik, hogy a DPI alapú technikai monitorig alkalmazásszolgáltatói LI-t az Eht. 92. § szerinti lenne optimális megvalósítani, természetesen annak a fentieket is figyelembe vevő felülvizsgálatát követően, hiszen ezen szabályozás már 20 éves, azonban előrelátó jellegnél fogva időtállóbbnak bizonyult jóval az Ekertv. 3/B. és 13/B. § rendelkezéseinél.[652] Az Eht. szerinti szabályozás adott, hiszen annak hatálya kiterjed az NI-ICS-re is a Bizottság 2.6.3. részfejezetben ismertetett döntése alapján a Meta tekintetében a WhatsApp és Messenger, az Apple tekintetében az iMessage vonatkozásában, így a Telegram, a Signal és a Viber is ezen számfüggetlen személyközi hírközlési szolgáltatások közé sorolandó. Tehát ismét bizonyítást nyert, hogy **a jövőben a személyközi hírközlési szolgáltatások – beleértve az alkalmazásszolgáltatásokat is – keretében végbement kommunikáció nemzetbiztonsági célú LI-jének hatékonysága érdekében nélkülözhetetlen lesz a nemzetközi együttműködés fokozása**. [H4] Az együttműködés a hazai nemzeti érdekeket figyelembe véve az elektronikus hírközlési szolgáltatások LI-je tekintetében elsődlegesen az EU tagállamaival, Európában a legnépszerűbb alkalmazásszolgáltatások LI-je tekintetében pedig elsődlegesen az USA kormányzati szerveivel, az IKT piac szereplőivel kell, hogy megvalósuljon Végezetül következtetésként megállapítható hogy a piaci volumenelemzés alapján előrevetíthető a globális alkalmazásszolgáltatások piacán jelentősebben érvényesülő szabályozási lobbitevékenység, a jóval nagyobb előforrásokon alapuló technológiai innovációval egyetemben, szemben a globális LI piacéval, amely volumene 2030-ig kb. 4-5%-a lesz az alkalmazásszolgáltatások globális piacának.

[652] Az Ekertv 3/B. és 13/B. § rendelkezései kapcsán fontos kiemelni, hogy azok 2016-os kodifikálásával a jogalkotó egy az IKT környezet fejlődéséből adódó joghézagot volt hivatott a technológiasemlegesség elvét figyelembe véve kitölteni az alkalmazásszolgáltatói együttműködés titkos információgyűjtés során megvalósuló törvényi szintű rendezésével, melyet elsősorban az Európát érő iszlám fundamentalista terrortámadások indukáltak.

5. ÖSSZEGZETT KÖVETKEZTETÉSEK

Az értekezés témaválasztásának és a kutatás aktualitásának indoklását, az azzal összefüggő tudományos problémák megfogalmazását követően, az azonosított hipotézisek mentén a kutatás céljaihoz illeszkedően kikötött „*nemzetbiztonsági célú LI kutatás integrált interdiszciplináris tudományos módszertanára*" alapozva, a szakirodalom feldolgozását követően, az értekezés meghatározott szerkezete mentén megvalósultak az egyes kutatási cselekmények, valamint a fejezetekhez illeszkedően az elvégzett vizsgálatok tömör leírásai, a részkövetkeztetések levonásával egyetemben. Az értekezés során átfogó vizsgálat tárgyát képezte az LI garanciális, szervezetrendszeri és módszertani hátterének áttekintése, egyfajta felvezetőként, a szükséges alapvető ismeretek komplex tárgyalásaként, a további érdemi szakmai részek vizsgálatának megalapozása, előkészítése céljából. Ezt követően a mobil hírközlési LI-t érintő IKT trendek majd az információs társadalommal összefüggő alkalmazásszolgáltatási LI-t érintő IKT tendenciák komplex elemzésére került sor a meghatározott kutatási módszertan alapján, a hipotézisek alátámasztásához. Az értekezés IKT környezet változásainak az információgyűjtés 21. századi fejlődésére gyakorolt hatásira irányuló hipotézisekkel kapcsolatos részkutatási eredményeinek összefoglaló jellegű leírását az alábbiak tartalmazzák:

Bizonyításra került az **1. hipotézis**, miszerint a prognosztizálható IKT trendek alapján a GSM alapú személyközi mobil kommunikáció hagyományos LI-jével szemben a mobilinternet alapú titkosított online kommunikációt biztosító alkalmazásszolgáltatások LI igényének fokozódása várható, amelyek szolgáltatói együttműködés alapú és technikai monitoring LI módszerei is innovatív technológiai, szabályozási és szervezeti környezetet követelnek meg. Az egyes alfejezetek kutatási cselekményei alátámasztják a hipotézist az alábbiak szerint:

- A 3.1.; 3.2.; 4.3. alfejezetek kutatási cselekményei alapján a mobil hírközlési technológiák terén kb. 10 évente tapasztalható egy generációváltás, amelyet a hálózati forgalom folyamatos heterogenizációja mellett, a lakossági fogyasztói igények, és az új IKT szolgáltatások kiszolgálása indukál. Trendelemzési kutatási módszerrel megállapításra került, hogy globális szinten kb. 2030-ra az 5G lakossági mobil-előfizetések átveszik a vezető szerepet a 4G-vel szemben, szinte teljesen kiszorítva a korábbi technológiákat (2G, 3G). Összességében a mobil-előfizetések száma folyamatosan emelkedő tendenciát mutat globális szinten, így a hálózati modernizáció mellett megállapítható a növekvő kereslet,

mely tendenciák között összefüggés azonosítható az újgenerációs hálózatok többletszolgáltatási lehetőségei okán. Tendenciaelemzés során megállapításra került, hogy az újgenerációs mobilhálózatok hazai elterjedése (4G, 5G) azonos tendenciát mutat a globális és regionális trendekkel, azaz kiszorító hatással bír a korábbi technológiákra. A regionális 5G trendeket vizsgálva azonban megállapítható, hogy 2023-ban Magyarország túlszárnyalta a közép-kelet-európai átlagot. Az alkalmazásszolgáltatások 2030/31-ig tartó piaci tendenciái alapján bizonyítottá vált azok központi szerepének további növekedése a lakossági célú kommunikációs igények kiszolgálásában, a globális piac gazdasági volumenét az előrejelzések alapján 2029 és 2031 között mintegy 1,7-szeresére növelve. Európában az előrejelzések szerint a piacvezetők a továbbiakban is a Meta szolgáltatásai (WhatsApp, Messenger), az iMessage, a Telegram, a Signal, és a Viber mellett.

- A 2.4.; 3.2.; 3.3.; 4.1.; 4.3.; 4.4. alfejezetek alapaján a Meta hatósági adatszolgáltatási attitűdjének tendenciaelemzése során megállapításra kerül a szolgáltatóhoz beérkező hatósági megkeresések globális számának exponenciális növekedése, amely a mobilinternet fogalom bővülésével azonos tendenciát mutat. Bizonyítható az internet alapú titkosított kommunikációt biztosító alkalmazásszolgáltatások bűnüldözési, nemzetbiztonsági érdeket sértő tevékenységgel való fokozódó érintettsége. A fokozódó személyes adatvédelmi előírások és a kereslet következtében az alkalmazásszolgáltatások kriptográfiai tulajdonságainak, elsősorban a központi DPI monitoring technikai LI módszer hatékonyságát kiemelten korlátozó E2EE fejlődése, egyben olyan jogellenes tevékenységek, mint a feldolgozott esettanulmányok alapján a terrorizmus, szervezett bűnözés, extrémizmus stb. számára is konspiratív lehetőséget biztosít. Sem tagállami szinten, sem az EU-t vizsgálva álláspontom alapján jelenleg nincsen hatályos hatékony bűnüldözési célú uniós jogi eszköz, és nemzetbiztonsági célú multilaterális együttműködés az USA-beli anyavállalattal és például írországi EU disztribúciós székhellyel rendelkező globális alkalmazásszolgáltatók (Meta, Apple) együttműködés alapú LI-je tekintetében.

- A 2.5.; 3.3.; 4.4. alfejezetek alapján a jogalkotó mind a hazai nemzetbiztonsági és bűnüldözési célú LI, mind a bűnüldözési célú nemzetközi LI együttműködés tekintetében a végrehajtásra az NBSZ-t jelölte ki mára, mint hazai központi LI szolgáltató szervezet, mely szolgáltatást nyújt a megrendelő nemzetbiztonsági, rendvédelmi, igazságügyi szervek számára speciális titkos információgyűjtő eszközeivel, módszereivel. Összevetve a 2015/2016-os kutatási eredményekkel, akkoriban az LI decentralizáltabb volt, akkor még

nem nyerte el a mai centralizált, egy szervezetbe koncentrált formáját, amely mind jogalkalmazási egységességet, erőforrásoptimalizációt, koncentrált K+F+I tevékenységet, és ágazati szintű független szervezeti belső kontrollt is biztosít. A 2.5. alfejezetben feltárásra került, hogy az igazságügyi miniszteri és bíró engedélyhez kötött nemzetbiztonsági célú titkos információgyűjtés, így az LI számossága is átlagosan laposabb exponenciálisan növekvő tendenciát mutat, az előrejelzések szerint előrejelezhető a nemzetbiztonsági ügyjelleg dominanciája. Az aktuális képességfejlesztési törekvéseket pedig a nyílt szakirodalom alapján alátámasztja a TIF, InfoLab, MiLab tudományos, kutatás-fejlesztési formációk létrejöttét, és azok céljai.

- A 2.5.3. részfejezet alapján az LI hagyományos rendszertani osztályozása az alkalmazásszolgáltatások kriptográfia kihívásainak az FBI által vezetett nemzetközi bűnüldözési koalícióban végrehajtott „Trójai Pajzs" akció keretében megvalósuló egyedi kezelése során a „lehallgathatatlannak" titulált ANOM alkalmazásszolgáltatás (NI-ICS) szervezett bűnözői körökben történő elterjesztésével, és ellenőrzésének konspirált technikai biztosításával kiegészült az új, innovatív „hamis zászlós" LI módszerrel.

Alátámasztásra került a **2. hipotézis**, miszerint a jövőben a légi, világűr infrastruktúrára épülő elektronikus hírközlő hálózatok várható elterjedése, valamint az újgenerációs mobilhálózatok LI-je forradalmasíthatja az összadatforrású titkos információgyűjtés technikai képességeit az egyre heterogénebb jellegű és forrású adatforgalom okán, amennyiben az információgyűjtő szervezetek képesek technológiai szempontból kiaknázni a lehetőségeket, például a kutatómunka során elméletben kidolgozott „Integrált Smart LI" (értekezésben: ISLI) koncepció keretében. . Az egyes alfejezetek kutatási cselekményei alátámasztják a hipotézist az alábbiak szerint:

- A 2.5.; 3.1.; 3.2.; 3.3.4.; 4.4. alfejezetek cselekményei során trendelemzési kutatási módszerrel megállapításra került a globális, de elsősorban európai viszonylatban az elektronikus hírközlési szolgáltatások tagállami jellegének eltolódása a régiós, globalizálódó jelleg irányába, melyet alátámaszt a 6G alapú, MI támogatott, integrált VHetNet elektronikus hírközlő koncepció. Így a hírközlési LI tekintetében indokolt és szükséges a régiós prognosztikus előrejelzések figyelembevétele a hazai LI K+F+I-je és a jogalkotás szempontjából, amelyek az elkövetkező 6 éves időszakban a közép-kelet-európai régióban a lakossági célú, személyközi hírközlési kommunikációt érintően a 4G

vezető szerepét vetítik előre, az 5G exponenciális erősödése, majd a 4G fokozatos kiszorítása mellett. Magyarország a 2030-ig szóló Űrstratégiájának célrendszere alapján erőteljes szerepet kíván betölteni az űripar fejlesztésében, és innovatív szolgáltatásainak hazai elterjesztésében, például a hírközlés területén, mely már aktuálisan is indokolttá teszi az LI képesség biztosítására irányuló ilyen jellegű kutatásokat, a fejlesztések előkészítését.

- A 2.7.; 3.1.; 3.2.; 3.3.; 4.4. alfejezetek részkutatási eredményei alapján a jövőben az 5G, 6G elektronikus hírközlő hálózatokon rendkívül nagy mennyiségű, és igen heterogén típusú adat fog megjelenni, például az okos város komplex digitális ökoszisztéma egyes olyan szolgáltatásai tekintetében, melyek mind a terrorizmus, illegális migráció, transznacionális szervezett bűnözés elleni tevékenység során hozzáadott értéket képezhetnek a nemzetbiztonsági, bűnüldözési célú LI számára. Optimális stratégiai kutatás-fejlesztési irányként a 3.3.2. részfejezetben bemutatott és bizonyított ISLI koncepció szerinti LI képesség kialakítását javaslom.

- A 6G alapú VHetNet műholdas hírközlési infrastruktúra előrejelzések szerinti 2030/2040 körüli elterjedése esetén legalább uniós szintű nemzetközi együttműködés keretében, a nemzeti szuverenitást tiszteletben tartó ISLI 2.0. koncepció szerinti LI képesség lehetőségének megvizsgálását javaslom. Az ISLI 2.0. képesség lehetősége kapcsán felmerül a nemzetbiztonsági tevékenység szupranacionális uniós jog alóli kivétel jellege, továbbá az egyes alkalmazásszolgáltatások kriptográfiai környezete is erőteljesen befolyásolja a koncepció hatékonyságát, így a kérdéskör további vizsgálata indokolt. A 4.4.3. részfejezetben javasolt szolgáltatói együttműködésen alapuló bűnüldözői és nemzetbiztonsági célú LI modell álláspontom alapján a kor elvárásai szerint automatizálható, elektronikus adatkapcsolat útján megvalósuló technikai LI módszerré is átkonvertálható az ISLI modell keretében. Azonban az ISLI koncepció is csak akkor tud teljes körű hatékonyságot biztosítani, ha az E2EE visszaszorítása esetén sikerül egy olyan nemzetközi standardizált kriptográfiai eljárás megalkotása, amely egyszerre biztosítja az LI eredményességét a megfelelő szintű adatvédelemmel egyetemben, így biztosítva az adatvédelem/biztonság értékduáljának kiegyensúlyozott érvényesülését.

Igazolásra került a **3. hipotézis**, miszerint az alkalmazásszolgáltatások globalizációja, a nemzetközi adatvédelmi normatív és technológiai környezet fejlődése hátrányosan érintheti az azokon végbement kommunikáció LI-jének hatékonyságát, valamint azok kriptográfiai fejlődésének hatására a kommunikációellenőrzést szabályozó hatályos hazai normarendszer hatékonysága erodálódhat, e téren az LI képesség rezilienciája korlátozódhat. Az egyes alfejezetek kutatási cselekményei alátámasztják a hipotézist az alábbiak szerint:

- A 2.7.; 4.2.; 4.3.; 4.3.; 4.4. alfejezetek kutatási cselekményei alapján a jelentősebb piacvezető alkalmazásszolgáltatók, mint például a Meta folyamatosan javítják az alkalmazások kriptográfiai tulajdonságait a felhasználók kommunikációjának biztonságosabbá tétele valamint, marketing célból egyaránt, amely egyrészről a protokollok, algoritmusok fejlesztéséhez, másrészről az E2EE alkalmazásának általános elterjedéséhez vezetett egyfajta keresleti/kínálati öngerjesztő jelenségként. A 2014/2016-os időszakot követően napjainkra ismét egy „titkosítási verseny" kezd kialakulni az alkalmazásszolgáltatások piacán, már előre reagálva az IKT környezet fejlődésének kvantumszámítás alapú innovációjára. Bemutatásra került az alkalmazásszolgáltatásokkal kapcsolatos anonimitás kihívása, mely okán javaslatom alapján globális, de legalább is EU szinten követelményként kellene támasztani az alkalmazásszolgáltatók számára a felhasználó természetes személy regisztrációja során a mobil hívószám megadásának kötelezettségét azonosíthatósági célból. Így a jogosult rendvédelmi szervek, akár nemzetbiztonsági célú LI keretében közvetetten ugyan, de hazai viszonylatban az Eht. mögöttes szabályai alapján már jóval hatékonyabban be tudnák azonosítani az LI-vel érintett valós felhasználót.

- A 2.5.; 2.7.; 3.1.; 3.3.; 4.2.; 4.3.; 4.4. alfejezetekben elvégzett kutatási cselekmények szerint az úttörő Ekertv. 3/B. és 13/B. § szerinti szolgáltatói együttműködés alapú alkalmazásszolgáltatói LI szabályozás időtállósága kapcsán levonható következtetés, hogy az a 2.4.1. részfejezet alapján már a hatálybalépésének időpontjában is korlátozottan volt hatékony – hiszen a technológiasemlegesség elvének érvényesülnie kellett – tekintettel arra, hogy a vizsgált alkalmazásszolgáltatások ¾-e addigra már E2EE-t alkalmazott. A rendelkezések hatékonyságának aktualitását nézve megállapítható, hogy az E2EE alapértelmezettségének folyamatos terjedésével, valamint legújabban a kvantumszámításnak is ellenálló kriptográfia megjelenésével tovább korlátozódik.

- A 2.4. és 4.3. alfejezet részkutatásai alapján megállapításra került, hogy az IKT környezet fejlődéséből adódó EU-s digitalizációs stratégiai célkitűzések koherens, következetes jog- és szakpolitikai törekvést követnek a felhasználói adatvédelem, bizalom fokozását célzó normatív és technológiai információbiztonság erősítése érdekében, így elősegítve a digitális, IKT termékek és szolgáltatások elterjedését elsősorban gazdaság-, társadalompolitikai okokból. Azonban az alkalmazásszolgáltatások és az LI globális piacainak összehasonlító volumenelemzése árnyalja a fenti megállapítást, miszerint az LI piac volumene 2030-ig kb. 4-5%-a lesz az alkalmazásszolgáltatások globális piacának. Így nem zárható ki a magasabb technológiai (elsősorban kriptográfiai) K+F+I beruházási erőforrásokkal rendelkező piacvezető „zászlóshajók" lobbitevékenysége sem a fokozódó felhasználói adatvédelmi igények marketing jellegű megalapozás érdekében, és a szabályozás szigorítása céljából, így növelve piaci részesedésüket, terjeszkedésüket, végső soron a profitjukat, a versenytársak kiszorításával egyetemben, de ez már inkább versenyjogi kérdéseket felvető következtetés. A marketing jellegű fölény pedig abban teljesedhet ki a biztonság szempontjából negatívan, miszerint az alkalmazások az E2EE kapcsán hirdetik tájékoztatójukban, hogy az erős kriptográfia által a felhasználók kommunikációs adatai „biztonságban vannak" még a szolgáltató előtt is – így ebből következtetve a kormányzati, nemzetbiztonsági, bűnüldöző szervek, hatóságok előtt.

Bizonyításra került a **4. hipotézis**, miszerint a jövőben a személyközi hírközlési szolgáltatások – beleértve az alkalmazásszolgáltatásokat is – keretében végbement kommunikáció nemzetbiztonsági célú LI-jének hatékonysága érdekében nélkülözhetetlen lesz a nemzetközi, uniós együttműködés fokozása, az információcserén túl a jövő LI képességei kialakításának lehetőségét is figyelembe véve, a nemzeti szuverenitás tiszteletben tartása mellett. Az egyes alfejezetek kutatási cselekményei alátámasztják a hipotézist az alábbiak szerint:

- A 2.1.; 2.3; 3.1.; 3.3.; 4.3. részfejezetek kutatási cselekményei, a nemzetközi kitekintés, együttműködések vizsgálata alapján az Európai Unió terrénumán a bűnüldözési célú LI-re irányuló tagállamközi együttműködéssel ellentétben, a nyilvános szakirodalom alapján a nemzetbiztonsági célú LI vonatkozásában továbbra sem tapasztalható akár csak a részleges multilaterális együttműködés normatív keretrendszerének kialakítására irányuló szervezett törekvés. Azonban álláspontom alapján a nemzetbiztonsági célú tevékenységnek, titkos információgyűjtésnek, így az LI-nek vannak a szabályozás áttöréséhez vezethető olyan vetületei, amelyek az egymással együttműködő tagállamok szuverenitására és biztonságára

pozitívan hatnak. Ilyen a nemzetbiztonsági célú, de bűnüldözési érdekkörben is értelmezhető tevékenység például az Nbtv. 74. § ae) alpont szerinti nemzetbiztonsági érdek körében értelmezett terrorizmus, transznacionális szervezett bűnözés, például a fegyver-, kábítószer-, ember-, műkincskereskedelem megelőzésében, felderítésében, megakadályozásában és elhárításában való közreműködés adott nemzetbiztonsági szolgálat által. Továbbá ebbe a kategóriába sorolható az illegális migrációt, a szövetséges államok szuverenitásába beavatkozó harmadik állam és nem kormányzati szerv tevékenységét, az emberiesség elleni bűncselekményeket.

- Az értekezés komplex részkutatási eredményei szerint a hírközlési LI tevékenység már az 5G, de igazából a 6G kapcsán megjelenő VHetNet légi és világűr hírközlő infrastruktúrái már csak elhelyezkedésükből adódóan is fel fogják vetni az EU szintjén a tagállami joghatóságok kollízióját, amit a GDPR adatvédelmi oldalról prognosztikusan már igyekezett kezelni. A tagállami alkalmazandó jogok összeütközése az LI szabályozása és végrehajtása terén is jelentkezni fog. Így elengedhetetlen az uniós szintű felsőbb keretjogalkotás a jövő hatékony LI képességeinek kialakítása érdekében, például a 3.3.2 részfejezetben javasolt ISLI modell szerint. A jövő sikeres LI tevékenysége szempontjából elengedhetetlen a formális, jogi kötőerővel és hatékony kikényszeríthetőséggel bíró nemzetközi együttműködés a globális alkalmazásszolgáltatók LI terén megvalósuló jogkövető magatartásra bírása érdekében, egyben uniós jogalkotást is magával hozva, együttműködve az USA-val, például a 4.4.3. részfejezetben javasolt bűnüldözési és nemzetbiztonsági célú nemzetközi szolgáltatói együttműködés alapú LI szabályozási keret szerinti módon, mely elvi modellje alapján átkonvertálható az ISLI-be integrálható DPI monitoring technikai LI módszerré. A javasolt LI modellek hatékonyságának foka nagyban függ az E2EE-t korlátozó olyan normatív intézkedésektől, amelyek mellett azonban érvényesülni tudnak a személyes adatvédelmi törekvések, egyensúlyban tartva az adatvédelem/biztonság értékduált, de mégis felszámolva a már jelenleg is fennálló „IKT LI adatvédelmi biztonság-deficitet”.

A kutatómunka további érdemi eredményeként feltárásra és bizonyításra került, hogy a nemzetközi, uniós adatvédelmi törekvések, piaci igények hátrányosan érintik az LI tevékenység hatékonyságát az adatvédelem/biztonság értékduált vizsgálva a biztonság hátrányára egyfajta „IKT adatvédelmi biztonság-deficit”-et előidézve, az azokkal visszaélő egyes globális IKT szolgáltatók pedig kialakítottak egyfajta vitathatóan legitim kvázi „törvényességi kontrollt”,

mely keretében intézményesülten magas százalékban tagadják meg az LI jogosult szerveztek nemzeti jogrendjén alapuló adatszolgáltatási megkereséseit. A 3.3.; 4.3.; 4.4. alfejezetek kutatási cselekményei alátámasztják a fenti kutatási eredményt az alábbiak szerint:

- A kutatómunka során azonosításra és alátámasztásra került az „**IKT adatvédelmi biztonság-deficit**” teória, elmélet, mely során az adatvédelem a biztonság hátrányára érvényesül az adatvédelem/biztonság értékduál egyensúlyával szemben. A 3.3.; 4.3.; 4.4. alfejezetek kutatási cselekményei alapján a fokozódó uniós adatvédelmi előírások, a kriptográfia erősödése hátrányosan érintik/ fogják érinteni az LI hatékonyságát, így a nemzet- és közbiztonság alkotmányos közérdekek érvényesülését. Ennek oka, hogy az Unió éppen a felhasználói bizalom erősítése, a többlet fogyasztás elősegítése, így végső soron a gazdasági növekedés érdekében fogalmazza meg az IKT termékeket és szolgáltatásokat érintő fokozott adatvédelmi követelményeket. Azonban, ha ezáltal a nemzetbiztonsági, bűnüldözési célú LI korlátozottsága miatt végsősoron közvetve sérül az egyes tagállamok, így összességében az EU biztonsághoz fűződő közérdek érvényesítését célzó eszközrendszerének hatékonysága, akkor össztársadalmi szinten csökken a komplex biztonság. Mindez a vállalkozások eredményességén és a fogyasztás visszaesésén keresztül hátrányosan érheti a gazdasági növekedési törekvéseket, így az általános digitális ökoszisztéma, a digitális társadalom megteremtésének uniós szakpolitikai, stratégiai célját. Tehát az E2EE általi „túltitkosítás” közvetlen nemzetbiztonsági, bűnüldözési érdeket sérthet az LI-vel érintett célszemélyek kommunikációja ellenőrzési hatékonyságának korlátozása okán, mely jelentőségét az ENSZ Emberi Jogi Főbiztosának fellépése is jelzi. A CSAM vita is mutatja az adatvédelem/biztonság kiegyensúlyozott értékduáljának adatvédelem felé történő kibillenését. A CSAM potenciális egységkovácsoló lehetőséget hordoz magában az EU politikai vezetése szintjén, egyben eddig nem látott lendülettel, ami az E2EE közbiztonsági, bűnüldözési célú korlátozását jelenti, így megnyitva a lehetőséget az „IKT adatvédelmi biztonság-deficit” visszabillentésére a biztonság javára.

- Azonosításra és bizonyításra került a globális alkalmazásszolgáltatók együttműködés alapú hatósági adatszolgáltatási megkeresések igencsak vitathatóan legitim kvázi **„törvényességi kontrollja**” és a teljesítés korlátozásának 10 éves ilyen jellegű gyakorlata, amely a nemzetbiztonsági és bűnüldözési célú LI során is érvényesül, így közvetlenül sértve a nemzetbiztonsági, bűnüldözési érdeket. A 4.3.; 4.4. alfejezetek kutatási cselekményei során megállapításra került, hogy a Meta a hatósági együttműködések

keretében az egyes tagállamok jogosult hatóságai, így LI szervezetei által közvetlenül megküldött megkeresések kb. ¼-ének teljesítését megtagadja egyfajta, álláspontom szerinti vitathatóan legitim szolgáltatói „törvényességi kontroll" keretében. Ezen „intézményesült" gyakorlat sérti az egyes demokratikus államok szuverenitását, biztonsági érdekeit, hiszen az alkotmányos garanciák, a hatalmi ágak szétválasztása, a fékek és egyensúlyok érvényesülése mellett történő közhatalom gyakorlása során az állami kényszer legitim és feltétlen. A fentiek alapján elengedhetetlen a jövő sikeres LI tevékenysége szempontjából a formális, jogi kötőerővel és hatékony kikényszeríthetőséggel bíró nemzetközi együttműködés a globális alkalmazásszolgáltatók LI terén megvalósuló jogkövető magatartásra bírása érdekében, mely terrénuma álláspontom alapján az európai országok tekintetében az EU kell, hogy legyen, egyben uniós jogalkotást is magával hozva, együttműködve az USA kormányzati szerveivel, IKT szolgáltatóival.

Egyéb kiemelt következtetések, megállapítások:

A hazai biztonsági stratégiai evolúciós elemzés során láthatóvá vált, hogy a „nemzetbiztonsági érdek", így az abból absztrahálható „nemzetbiztonsági célzat" tartalma dinamikusan, a kor elvárásai mentén változik, alakul a hagyományos területektől elmozdulva a digitális kihívások, vagy éppen a K+F+I irányába. Megállapításra és bizonyításra került, hogy az uniós jog hazai jogforrási etimológiai és tartalmi interpretálása során a „nemzetbiztonság" fogalom alkalmazása nem egységes, nem konzekvens, összemosódik a „nemzeti biztonság" az „állam biztonsága" fogalmakkal, amely pedig a normaalkalmazás során kihívásként azonosítható. Továbbá a 2.3.2. részfejezetben az Infotv. alapján ismertetésre került a nemzetbiztonsági és bűnüldözési célzat adatkezelési szempontú értelmezése.

Feltárásra és bizonyításra került az Ekertv. tárgyi hatálya szerinti alkalmazásszolgáltatásnak az Eht. tárgyi hatálya szerinti NI-ICS-sel való összefüggése az Ekertv. és az Eht., DMA, Hírközlési Kódex alapján, illetve azok funkcionális azonossága okán előállva az Ekertv. és az Eht. tárgyi hatályának összeütközése, konfliktusa. A 2.4., 2.6.; 3.3.; 4.4. alfejezetekben a kutatási cselekmények során megállapításra kerültek a fentiek. Az információs társadalommal összefüggő infokommunikációs és elektronikus hírközlési szolgáltatások szabályozásának integrált uniós jog- és szakpolitikai szemlélete végül a DMA és a Hírközlési Kódex kicsúcsosodása során 2023-ra lényegében a hatályos és alkalmazandó uniós jog tételévé vált. Így uniós és tagállami szintű jogalkotói, jogalkalmazói kötelezettségeket testesítve meg, az

alkalmazásszolgáltatások körében először az Európai Bizottság 2023 végétől érvényesülő intézményi joggyakorlata körében a WhatsApp, Messenger és iMessage DMA szerinti alapvető platformszolgáltatások (NI-ICS/alkalmazásszolgáltatás) tekintetében. Az EU digitalizációs törekvései mentén a DMA és a DSA hatályának bázisán kialakult a digitális ágazat, amely beékelődött és jelentős hatást gyakorol mind az elektronikus hírközlési, mind a kiberbiztonsági ágazatra és szabályozásra (NIS2), amely jogterületek éles elhatárolása még az Unió szintjén is egy alakulóban lévő folyamat, nemhogy a tagállami jog szintjén. Az NI-ICS/ alkalmazásszolgáltatás szabályozása LI szempontjából egy kardinális kérdés, hiszen a DMA – és már a Hírközlési Kódex is – az NI-ICS tekintetében átnyúl az elektronikus hírközlési ágazati szabályozásba, amely hazai jogforrási szinten az Eht.-ben került adoptálásra, átültetésre, úgyhogy egyébként az Ekertv. tárgyi hatálya pedig továbbra is kiterjed az alkalmazásszolgáltatásra, mely jogi konfliktus azonosítása álláspontom alapján egy javasolt új tudományos eredmény is egyben.

Meghatározásra kerültek a 21. század IKT boom-jának, az IKT környezet alkalmazásszolgáltatásokkal kapcsolatos fejlődésének nemzetbiztonsági érdekeket veszélyeztető olyan várható főbb kihívásai, mint az infokommunikációs felhasználói anonimitás lehetőségének fokozódása; az állami, az uniós és a nemzetközi jog „felett állás" státuszát gyakorló globális szolgáltatók hatósági együttműködése korlátozódásának veszélye; az E2EE-t integráló online kommunikációt biztosító alkalmazásszolgáltatások igénybevételének további terjedése a titkos információgyűjtéssel érintettek körében; valamint a kommunikációs szolgáltatásoknál az E2EE általánossá válása, és a további innovatív kriptográfiai eljárások fejlődése.

Az összegzett következtetések alapján tehát, az új „*nemzetbiztonsági célú LI kutatás integrált interdiszciplináris tudományos módszertana*" alkalmazásával teljesítésre kerültek a doktori értekezés fő célkitűzései az IKT környezet változásainak az információgyűjtés 21. századi fejlődésére gyakorolt hatásira irányuló hipotézisek igazolásán, valamint további kutatási eredményeken keresztül. A módszertan keretében elvégzett elemzések, vizsgálatok során elért tudományos következtetésekre alapozva olyan gyakorlatorientált, az alkalmazott kutatásokhoz integrálható nyilvános, a következő fejezetben taxatíve felsorolásra kerülő új javasolt tudományos eredmények kerültek elérésre, amelyek magukban hordozzák a hazai LI képességek hatékonyságfokozásában való közreműködés tényleges lehetőségét, elsősorban jogalkotási és kutatás-fejleszti irányok, szemléletformálás, további részkutatási irányok

meghatározása által. Egyfajta keretet adva az értekezésnek, a témaválasztás és a kutatás aktualitásának záróindoklásként az Alaptörvény 2023. december 22-ei módosítása általános indokolás 3. pontját idézem, amely szerint az Alaptörvény az új tudományos és műszaki eredmények alkalmazásának, valamint a digitális ügyintézés állami szintű előmozdítására hivatott „*XXVI. cikkének […] kiegészítése mögött az a felismerés áll, hogy az információs és kommunikációs technológiák [IKT] fejlődése életünk gyökeres átalakulását hozza magával*.”

6. ÚJ TUDOMÁNYOS EREDMÉNYEK

Disszertációs kutatómunkám során az értekezésben kidolgozott új tudományos eredményként történő elfogadását javaslom az alábbiaknak:

1. Bizonyítottam, hogy a prognosztizálható IKT trendek alapján a GSM alapú személyközi mobil kommunikáció hagyományos LI-jével szemben a mobilinternet alapú titkosított online kommunikációt biztosító alkalmazásszolgáltatások LI igényének fokozódása várható, amelyek szolgáltatói együttműködés alapú és technikai monitoring LI módszerei is innovatív technológiai, szabályozási és szervezeti környezetet követelnek meg. **[Bizonyítás: 2.4.; 2.6.; 3.1.; 3.2.; 3.3.; 4.1.; 4.3.; 4.4.]**

2. Alátámasztottam, hogy a jövőben a légi, világűr infrastruktúrára épülő elektronikus hírközlő hálózatok várható elterjedése, valamint az újgenerációs mobilhálózatok LI-je forradalmasíthatja az összadatforrású titkos információgyűjtés technikai képességeit az egyre heterogénebb jellegű és forrású adatforgalom okán, amennyiben az információgyűjtő szervezetek képesek technológiai szempontból kiaknázni a lehetőségeket, például a kutatómunka során elméletben kidolgozott „Integrált Smart LI” (az értekezésben: ISLI) koncepció keretében. **[Bizonyítás: 2.5.; 2.7.; 3.1.; 3.2.; 3.3; 4.4]**

3. Igazoltam, hogy az alkalmazásszolgáltatások globalizációja, a nemzetközi adatvédelmi normatív és technológiai környezet fejlődése hátrányosan érinti az azokon végbement kommunikáció LI-jének hatékonyságát, valamint azok kriptográfiai fejlődésének hatására a kommunikációellenőrzést szabályozó hatályos hazai normarendszer hatékonysága erodálódik, e téren az LI képesség rezilienciája korlátozott. **[Bizonyítás: 2.4.; 2.5.; 2.7.; 3.1.; 3.3.; 4.2.; 4.3.; 4.3.; 4.4.]**

4. Bizonyítottam, hogy a jövőben a személyközi hírközlési szolgáltatások – beleértve az alkalmazásszolgáltatásokat is – keretében végbement kommunikáció nemzetbiztonsági célú LI-jének hatékonysága érdekében nélkülözhetetlen lesz a nemzetközi, uniós együttműködés fokozása, az információcserén túl a jövő LI képességei kialakításának lehetőségét is figyelembe véve, a nemzeti szuverenitás tiszteletben tartása mellett. **[Bizonyítás: 2.1.; 2.3.; 2.4.; 2.6.3.; 3.1.; 3.2.; 3.3.; 4.1.; 4.2.; 4.3.; 4.4.]**

5. Feltártam és bizonyítottam, hogy a nemzetközi, uniós adatvédelmi törekvések, piaci igények hátrányosan érintik az LI tevékenység hatékonyságát az adatvédelem/biztonság értékduált vizsgálva a biztonság hátrányára egyfajta „IKT adatvédelmi biztonság-deficit”-et előidézve, az azokkal visszaélő egyes globális IKT szolgáltatók pedig kialakítottak egyfajta vitathatóan legitim kvázi „törvényességi kontrollt”, mely keretében intézményesülten magas százalékban tagadják meg az LI jogosult szervezetek nemzeti jogrendjén alapuló adatszolgáltatási megkereséseit. **[Bizonyítás: 3.3.; 4.3.; 4.4.]**

7. AJÁNLÁSOK A KUTATÁS EREDMÉNYEINEK GYAKORLATI FELHASZNÁLHATÓSÁGÁRA

A disszertációs kutatómunka során elért eredmények gyakorlati felhasználhatósága az értekezése egyik fő célkitűzése a tényleges pozitív társadalmi hatás kiváltása érdekében. Az eredmények, következtetések álláspontom alapján valós hozzáadott értéket képezhetnek a komplex biztonsági ökoszisztéma számára, így azok gyakorlati felhasználását az alábbi ajánlások szerint javaslom mind a hazai, mind az uniós, nemzetközi jogalkotás, a nemzetbiztonsági ipari Triple Helix modell szerinti K+F+I ágazati, akadémia és egyetemi, valamint piaci szereplői számára, továbbá a felsőfokú és doktori képzések során.

Hazai, uniós és nemzetközi jogalkotás:

Javaslom a 2. hipotézis bizonyításával kapcsolatos eredmények, valamint az Eht. és Ekertv. hatályának összeütközésével kapcsolatos megállapítások felhasználását a hírközlési és online platform jogalkotás keretében. Javaslom a 1.-4. hipotézisekkel összefüggő eredmények, valamint a nemzetközi jogforrásokban megjelenő „nemzetbiztonság" fogalom eltérő hazai interpretálásával, továbbá a hatósági adatkérések vitathatóan legitim alkalmazásszolgáltatói „törvényességi kontrolljával" kapcsolatos megállapítások hasznosítását a nemzetbiztonsági és bűnüldözési célú titkos információgyűjtéssel, LI-vel kapcsolatos jogalkotás során. Javaslom a személyes adatvédelemmel kapcsolatos jogalkotás során szemlézni a 3. hipotézissel kapcsolatos megállapításokat. Javaslom a gyermekek szexuális kizsákmányolása elleni uniós jogalkotás keretében a 3.-4. hipotézisek eredményeinek hasznosítását, mely hazai vetületű aktualitását, és a magyar álláspont fokozottabb érvényesíthetőségét a 2024 második féléves Magyarország általi EU Tanács soros elnöksége még inkább elősegíthet.

Ágazati nemzetbiztonsági ipari K+F+I:

Javaslom az 1-4. hipotézis bizonyítása, vizsgálata során feltárt eredmények hasznosítását a nemzetbiztonság elméleti kutatások, továbbá az LI gyakorlati kutatás-fejlesztés, a kettős felhasználási lehetőségek vizsgálata során. Ezen eredményeket különösen figyelmébe ajánlom a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal felügyeletében működő InfoLab, MiLab, illetve a KNBSZ IKK keretében zajló alkalmazott kutatások számára. Továbbá a TIF keretében folyó polgári nemzetbiztonsági tudományos munka, alapkutatások számára.

Akadémiai és egyetemi nemzetbiztonsági ipari K+F+I:

A HUN-REN figyelmébe ajánlom az 1-3. hipotézisek vizsgálata keretében elért eredmények hírközlési, online platform kutatás során történő hasznosítását. Az NKE figyelemébe ajánlom a formális had- és rendészettudományi doktori, azon belül is nemzetbiztonsági kutatási céllal az 1. és 3. hipotézisekkel összefüggő eredmények falhasználását. A BME figyelmébe ajánlom szintén az 1. és 3. hipotézisek hasznosítását, különösen a CrysyLab keretében zajló kriptográfiával, kibervédelemmel kapcsolatos alkalmazott kutatások számára. A Pázmány Péter Katolikus Egyetem (a továbbiakban: PPKE), valamint a Pécsi Tudományegyetem (a továbbiakban: PTE) állam- és jogtudományi doktori, valamint felsőfokú képzései során figyelembe ajánlom az 1. és 4. hipotézisekkel, a „nemzetbiztonság" fogalom eltérő hazai interpretálásával, továbbá az alkalmazásszolgáltatói „törvényességi kontrollal" kapcsolatos megállapítások jogtudományi hasznosítását, akár új kutatási irányok meghatározása céljából.

Piaci nemzetbiztonsági ipari K+F+I:

Javaslom az 1.-4. hipotézisek vizsgálata során feltárt eredmények, megállapítások hasznosítását olyan kutatási területeken, mint a MI, az autonóm rendszerek, és a diszruptív IKT technológiák, elsősorban az ipari K+F technikai támogatása, valamint a nemzeti innovációs platformokhoz való hozzájárulás érdekében. Javaslom az eredmények hazánkban és a régióban rendelkezésre álló mélyreható szakértelem kiaknázásával, a jövőbeni védelmi képességeknek, így a komplex védelmi innovációs ökoszisztémának a kettős felhasználású termékek és szolgáltatások fejlesztése során történő felhasználását. Javaslom az eredmények hasznosítását például az európai információs műveletekkel foglalkozó kettős felhasználási célú K+F projektek keretében, az EU tagállamai közös biztonságának növelése, az európai védelmi piac integrációjának és hatékonyságának fokozása céljából.

Oktatás, képzés:

Figyelembe ajánlom az értekezés következtetéseinek, kutatási eredményeinek általános hasznosítását az NKE számára a nemzetbiztonsági elméleti oktatás, a BME számára a kibervédelem és nemzetbiztosági technológiák gyakorlati kapcsolódásaival kapcsolatos képzés, valamint a PPKE, PTE számára nemzetbiztonsági, hírközlési jogi képzés során. Továbbá aktualitás, időszerűség, szükségesség esetén javaslom a nemzetbiztonsági célú LI tevékenység jogállami garanciális feltételeinek való magas szintű megfelelése alátámasztásának lakossági tájékoztatási célú, tudományos megalapozottságú edukációs, kommunikációs felhasználását.

8. IRODALOMJEGYZÉK

8.1. Szakirodalmi hivatkozások, statisztikák

- AL SAADI, Maiya – KUMAR, Basant (2020): A Review on Elliptic Curve Cryptography. *International Journal of Future Generation Communication and Networking,* 13(3), 1597-1601. ISSN: 2233-7857.
  Online: https://www.researchgate.net/publication/350048546_A_Review_on_Elliptic_Curve_Cryptography (Letöltés ideje: 2024. február 18.)
- ALMAZROI, Abdulaleem Ali (2018): Performance analysis of 4G broadband cellular networks. *International Journal of Advanced and Applied Sciences,* 5(9), 12-17. ISSN: 2722-2594.
  Online: http://science-gate.com/IJAAS/Articles/2018/2018-5-9/03%202018-5-9-pp.12-17.pdf (Letöltés ideje: 2023. december 19.)
- ALMÁSI Miklós (2016): A láthatatlan hatalmak. *Magyar Tudomány*, 177(6), 681-689. ISSN: 1588-1245.
  Online: https://epa.oszk.hu/00600/00691/00153/pdf/EPA00691_mtud_2016_06_681-689.pdf (Letöltés ideje: 2024. július 7.)
- ANDREWS, Thomas at al. (2023): *Myanmar: Social media companies must stand up to junta's online terror campaign say UN experts*. Genewa: The Office of the High Commissioner for Human Rights, United Nations
  Online: https://www.ohchr.org/en/press-releases/2023/03/myanmar-social-media-companies-must-stand-juntas-online-terror-campaign-say (Letöltés ideje: 2023. december 26.)
- ANWAR, Toni (2008): Performance Analysis of 3G Communication Network. *ITB Journal of Information and Communication Technology,* 2(2), 130–157. ISSN: 1675-414X,
  Online: https://doi.org/10.5614/itbj.ict.2008.2.2.4 (Letöltés ideje: 2023. december 19.)
- ARA, Israt – KELLEY, Brian (2023): 6G Physical Layer Security. PH.D. DOMÍNGUEZ-MORALES, Manuel Jesus at al. (edit.): *Deep Learning - Recent Findings and Researches*. London: IntechOpen.

Online: https://www.intechopen.com/online-first/88429 (Letöltés ideje: 2024. február 22.)

- ARORA, Mohit (2012): Long Term Evolution (LTE) Technology. *International Journal of Latest Technology in Engineering Management & Applied Science*, 1.(3), 69-71. ISSN: 2278 – 2540. Online:www.researchgate.net/publication/319465003_LONG_TERM_EVOLUTION_LTE_TECHNOLOGY (Letöltés ideje: 2023. december 19.)
- ASTELY, David - VON BUTOVITSCH, Peter – FAXÉR, Sebastian – LARSSON, Erik (2022): Meeting 5G network requirements with Massive MIMO. *Ericsson Technology Review*, 7(1), 2-11. ISSN: 0014-0171. Online: https://www.ericsson.com/4917a1/assets/local/reports-papers/ericsson-technology-review/docs/2022/the-role-of-massive-mimo-in-5g-networks.pdf (Letöltés ideje: 2024. február 22.)
- AUMASSON, Jean-Philippe (2018): *Serious Cryptography - A Practical Introduction to Modern Encryption*. San Francisco: No Starch Press, Inc. ISBN-10: 1-59327-826-8. Online: https://theswissbay.ch/pdf/Books/Computer%20science/Cryptography/SeriousCryptography.pdf (Letöltés ideje: 2023. július 17.)
- BABOS Sándor (2020): Az alapvető jogok korlátozása a nemzetbiztonsági tevékenység során II. *Nemzetbiztonsági Szemle*, 8(4), 45-58. ISSN 2064-3756. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/5008/4313 (Letöltés ideje: 2024. február 18.)
- BÁCS Zoltán György (2022): Viribus Unitis, avagy civil professzionális konvergencia a 21. században. In DOBÁK Imre (szerk.): *Nemzetbiztonság a 21. század elején*. Budapest: Ludovika Kiadó. 42-49. ISBN: 978-963-5316-37-3.
- BÁCS Zoltán György (2023): Gondolatok az információ szerepéről – más, egyéni szemszögből. *Nemzetbiztonsági Szemle*, 11(3), 83-92. ISSN 2064-3756. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/6862/5705 (Letöltés ideje: 2024. február 19.)
- BAKOS Ferenc (2009): *Idegen szavak és kifejezések szótára*. Budapest: Akadémiai Kiadó Zrt. ISBN 978-963-0587-98-3.

- BALOGH Péter (2013): Rádióelektronika (jel-) felderítés (SIGINT). In DR. KOBOLKA István (szerk.): *Nemzetbiztonsági alapismeretek*. Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó. 125-144. ISBN 978-615-5344-32-9.
- BALOGH Zsolt (2011): Alapjogok korlátozása az új alkotmányban. *Pázmány Law Working Papers,* 2(19), 1-10.
  Online: https://plwp.eu/docs/wp/2012/2011-19.pdf (Letöltés ideje: 2024. július 7.)
- BÁNYAI Balázs - FELDHOFFER Gergely - TIHANYI Attila (2008): *Helymeghatározás GSM hálózat felhasználásával.* Budapest: PPKE ITK.
  Online: https://docplayer.hu/12551470-Helymeghatarozas-gsm-halozat-felhasznalasaval.html (Letöltés ideje: 2023. július 30.)
- BÁNYÁSZ Péter – TÓTH András – MAGYAR Sándor – KOLLER Marco (2022): A videókonferencia-alkalmazások biztonsági kockázatai. *Acta Humana*, 10(4), 19-34. ISSN 0866-6628.
  Online: https://folyoirat.ludovika.hu/index.php/actahumana/article/view/6731/5286 (Letöltés ideje: 2024. február 16.)
- BÁNYÁSZ Péter (2017): Kiberbűnözés és közösségi média. *Nemzetbiztonsági Szemle*, 5(4), 55-74. ISSN 2064-3756.
  Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1634/946 (Letöltés ideje: 2024. február 27.)
- BÁNYÁSZ Péter (2018): Social engineering and social media. *Nemzetbiztonsági Szemle*, 6(1), 60-74. ISSN 2064-3756.
  Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1511/829 (Letöltés ideje: 2024. február 27.)
- BARNÓCZKI László – KENEDLI-TÓTH Eszter (2021): A nemzetbiztonsági szolgálatok megszervezése és működése az eltelt harminc év során – változások az ágazatot érő legfontosabb kihívások tükrében. In CHRISTIÁN László - LIPPAI Zsolt - NÉMETH Zsolt (szerk.): *A rendszerváltás hatása a rendészetre*. Budapest: Ludovika Egyetemi Kiadó. 71-102. ISBN: 978-963-5315-54-3.
- BARTOLITS István (2000): A távközlés regénye. *Élet és Irodalom*, 64(19-28). 1-29. ISSN: 1588-0362.
  Online: http://w3.tmit.bme.hu/thsz/TavkReg.pdf (Letöltés ideje: 2024. február 22.)
- BÉKÉSI Nikolett – SABJANICS István (2017): A terrorizmus elleni fellépés magánszférát érintő kérdései. In CSINK Lóránt (szerk.): *A nemzetbiztonság kihívásainak hatása a*

magánszférára. Budapest: Pázmány Press. 227-260. ISBN 978-963-308-319-2. Online: https://jak.ppke.hu/uploads/articles/1185528/file/Csink_maganszfera_TAN40.pdf (Letöltés ideje: 2024. február 28.)

- BETKER, Michael R. – FERNANDO, John S. – WHALEN, Shaun P. (1997): The history of the microprocessor. *Bell Labs Technical Journal*, 2(4), 29–56. ISSN: 1538-7305. Online: https://doi.org/10.1002/bltj.2082 (Letöltés ideje: 2024. február 21.)
- BIBALBENIFA, J.V. - KRISHNANN, Saravanan – LONG, Hoang Viet, - KUMAR, Raghvendra – Taniar, David (2021): *Performance Analysis of Machine Learning and Pattern Matching Techniques for Deep Packet Inspection in Firewalls*. Online: https://doi.org/10.21203/rs.3.rs-260788/v1 (Letöltés ideje: 2024. február 15.)
- BIKKI István (2010): A titkos operatív technikai rendszabályok és módszerek, valamint a K-ellenőrzés alkalmazására vonatkozó szabályok 1945–1990 között (rövid áttekintés). *Betekintő*, 4(1), 1-16. ISSN 1788 – 7569.
  Online: https://betekinto.hu/sites/default/files/betekinto-szamok/2010_1_bikki.pdf (Letöltés ideje: 2023. július 26.)
- BLAISE, O. – AWODELE, O. – YEWANDE, O. (2021): An Understanding and Perspectives of End-To-End Encryption; *IRJET International Research Journal of Engineering and Technology*, 8(4), 1086.
  Online: https://www.researchgate.net/publication/350850077_An_Understanding_and_Perspectives_of_End-To-End_Encryption (Letöltés ideje: 2024. február 19.)
- BLASKÓ Béla - BUDAHÁZI Árpád (2019): *A nemzetközi bűnügyi együttműködés joga*. Budapest: Dialóg Campus Kiadó. ISBN 978-615-5920-65-3.
  Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/13041/web_PDF_Nemzetkozi_bunugyi_egyuttmukodes_joga.pdf?sequence=1 (Letöltés ideje: 2024. február 28.)
- BODA József (2012): A Nemzetbiztonsági Szakszolgálat helye és szerepe a rendvédelemben. *Pécsi Határőr Tudományos Közlemények,* 11(13), 113-130. ISSN: 1589-1674.
  Online: http://www.pecshor.hu/periodika/XIII/boda.pdf (Letöltés ideje: 2023. július 26.)

- BODA József (2016): *„Szigorúan titkos!”? – Nemzetbiztonsági almanach*. Budapest: Zrínyi Kiadó. ISBN: 978-963-327-670-9.
- BODÓ Attila Pál – BOGNÁR Balázs (2019): *Kritikus információs infrastruktúrák védelme*. Budapest: NKE. ISBN 978-963-498-238-8.
  Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/13801/Kritikus%20informacios%20infrastrukturak%20vedelme_Eves%20tovabbkepzes_felelos%20vezeto.pdf?sequence=3&isAllowed=y (Letöltés ideje: 2024. február 16.)
- BOKORNÉ SZEGŐ Hanna (1995): Az emberi jogokról való időleges eltérés, illetve az emberi jogok állandó jellegű törvényes korlátozása. *Acta Humana*, (18-19), 24-39. ISSN 0866-6628.
- BORAM, Kim (2023): *S. Korea plans to launch 6G network service in 2028*. Seul:Yohnap News.
  Online: https://en.yna.co.kr/view/AEN20230220003000320 (Letöltés ideje: 2024. február 22.)
- BUTTYÁN Levente – VAJDA István (2005): *Kriptográfia és alkalmazásai*. Budapest: Typotex. ISBN: 978-963-9548-13-8.
- BUZAN, Barry (1983): *People, states, and fear: the national security problem in international relations*. Brighton: Wheatsheaf Books.
- BUZÁS Péter - PÉTERFALVI Attila - RÉVÉSZ Balázs (szerk.) (2021): *Magyarázat a GDPR-ról*. Budapest: Wolters Kluwer. ISBN: 978-963-5940-03-5.
- CECI, Laura (2024): *Most popular messenger apps worldwide in January 2024, by monthly downloads*. Statista.
  Online: https://www.statista.com/statistics/1263360/most-popular-messenger-apps-worldwide-by-monthly-downloads/ (Letöltés ideje: 2024. február 26.)
- CHEN, L.– JORDAN, S. – LIU, Y.– MOODY, D. – PERALTA, R. – PERLNER, R.- DANIEL, S. (2016): *Report on Post-Quantum Cryptography*. NIST.IR 8105. Online: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (Letöltés ideje: 2024. február 16.)
- *Competitiveness Council 28 and 29 May in Brussels*. Council of the European Union. 2015. Online: https://www.consilium.europa.eu/media/23442/background-note-compet-may_en.pdf (Letöltés ideje: 2024. február 17.)

- CSIKI VARGA Tamás – TÁLAS Péter (2020): Magyarország új nemzeti biztonsági stratégiájáról. *Nemzet és Biztonság*, 13(3), 89-112. ISSN 2559-8651. https://www.nemzetesbiztonsag.hu/cikkek/4906-cikk_szoveg-16687-1-10-20210426.pdf (Letöltés ideje: 2023. augusztus 08.)
- DAKKAK, M. Rabih - RIVIELLO, Daniel Gaetano - GUIDOTTI, Alessandro - VANELLI-CORALLI, Alessandro (2023): Evaluation of multi-user multiple-input multiple-output digital beamforming algorithms in B5G/6G low Earth orbit satellite systems. *International Journal of Satellite Communications and NetworkingEarly View*, Special Issue, 1-16. ISSN: 1542-0981.
  Online: https://onlinelibrary.wiley.com/doi/epdf/10.1002/sat.1493 (Letöltés ideje: 2024. február 22.)
- DE, Rajesh – CHRISTIAN, Marcus A. – GLICK, Veronica R. – KOURINIAN, Arsen – LILLEY, Stephen – LEIPZIG, Dominique Shelton – SIMON, David A. – WALTZMAN, Howard W. – YAROS, Oliver – BRUDER, Hadnes Ana – HEPWORTH, Ellen - VON BORSTEL, Megan P. (2022): *President Biden Signs Executive Order on U.S.* Intelligence *Activities to Implement EU-U.S. Data Privacy Framework*. MayerBrown. Online: https://www.mayerbrown.com/en/perspectives-events/publications/2022/10/president-biden-signs-executive-order-on-us-intelligence-activities-to-implement-eu-us-data-privacy-framework (Letöltés ideje: 2024. február 27.)
- DELI Tamás (2021): *Adaptív moduláció támogatása gépi tanulási módszerekkel műholdas rádiócsatornán*. Budapest: BME VIK. Online: https://tdk.bme.hu/VIK/DownloadPaper/Adaptiv-modulacio-tamogatasa-gepi-tanulasi3 (Letöltés ideje: 2024. február 25.)
- DESSEWFFY, Tibor (2003): *Mapping the future*. Budapest: ITTK-TÁRKI. 7. Online: www.tarki.hu/adatbank-h/kutjel/pdf/a687.pdf (Letöltés ideje: 2023. július 30.)
- DHAPTE, Aarti (2024): Lawful Interception Market Overview. Market Research Report. Online: https://www.marketresearchfuture.com/reports/lawful-interception-market-9596?utm_term=&utm_campaign=&utm_source=adwords&utm_medium=ppc&hsa_acc=2893753364&hsa_cam=20298941735&hsa_grp=151951244833&hsa_ad=663291708226&hsa_src=g&hsa_tgt=dsa-2088470533900&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gad_source=1 (Letöltés ideje: 2024. február 29.)

- DINYA Lajos - RAÁB Mihály (2012): A Nemzetbiztonsági Szakszolgálat technikai fejlődésé a rendszerváltástól napjainkig. In CSÓKA Ferenc (szerk.): *Szakszolgálat Magyarországon, avagy tanulmányok a hírszerzés és titkos adatgyűjtés világából*. Budapest: NBSZ. 487-496. ISBN: 978-963-08-3211-3.
- DIXON, S. (2022): *Most popular global mobile messaging apps 2022*. Statista. Online: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (Letöltés ideje: 2024. január 20.)
- DIXON, Stacy Jo (2024): M*ost popular global mobile messenger apps as of January 2024, based on number of monthly active users*. Statista. Online: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (Letöltés ideje: 2024. február 26.);
- DOBÁK Imre – KENEDLI Tamás (2023): Információszerzési tendenciák és kihívások a kibertérben rejlő lehetőségek és a mesterséges intelligencia viszonylatában. *Military and Intelligence CyberSecurity Research Paper*, 3(2). 1-41. ISSN: 2786-3778.
  Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/MIC%20RP%202023-3%20-%20Dob%C3%A1k%20Imre-Kenedli%20Tam%C3%A1s%20-%20Inform%C3%A1ci%C3%B3szerz%C3%A9si%20tendenci%C3%A1k%20%C3%A9s%20kih%C3%ADv%C3%A1sok%20a%20kibert%C3%A9rben%20rejl%C5%91%20lehet%C5%91s%C3%A9gek%20%C3%A9s%20a%20mesters%C3%A9ges%20intelligencia%20viszonylat%C3%A1ban.pdf Letöltés ideje: 2024. február 18.)
- DOBÁK Imre – SOLITI István (2016): Az „operatív technika" fejlesztésének helye és szerepe az állambiztonság szervezetrendszerében - a szobalehallgatás. *Hadmérnök*, 9(3), 121-134. ISSN 1788-1919.
  Online: http://www.hadmernok.hu/163_10_bobak.pdf (Letöltés ideje: 2023. július 26.)
- DOBÁK Imre – TÓTH Tamás (2022): Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering). *Belügyi Szemle*, 69(2), 195-212. ISSN 2677-1632.
  Online: https://ojs.mtak.hu/index.php/belugyiszemle/article/view/5345/4209 (Letöltés ideje: 2024. február 15.)
- DOBÁK Imre – TÓTH Tamás (2023): A külső környezet, és tendenciák nyomon követésének szükségessége a stratégiaalkotás tükrében. In DOBÁK Imre – RESPERGER István (szerk.): *Stratégiák, stratégiai gondolkodás, nemzetbiztonság*. Budapest: Ludovika Egyetemi Kiadó. 33-50. ISBN: 978-963-5318-51-3.

- DOBÁK Imre (2013): A belügyi, állambiztonsági rádióelhárítás nemzetközi viszonyrendszere az 1960-1970-es években. *Pécsi Határőr Tudományos Közlemények,* 12(14). 113-120. ISSN: 1589-1674.
  Online: http://www.pecshor.hu/periodika/XIV/dobaki.pdf (Letöltés ideje: 2023. július 26.)
- DOBÁK Imre (2015): Nemzetbiztonsági szolgálatok – Betekintés a visegrádi országok (V4) nemzetbiztonsági rendszereibe. *Hadtudományi Szemle*, 8(4), 113-130. ISSN 2060-0437.
  Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/10159/2015_4_visegr%c3%a1di%20orsz%c3%a1gok.pdf?sequence=2&isAllowed=y (Letöltés ideje: 2024. február 20.)
- DOBÁK Imre (2017): A telefonlehallgatás kialakulásának nyomai a 19-20. század fordulóján, Magyarországon. *Hadtudományi Szemle*, 10(1), 392-409. ISSN 2060-0437.
  Online: https://tudasportal.uni-nke.hu/xmlui/static/pdfjs/web/viewer.html?file=https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/14042/17_1_alt_dobak.pdf?sequence=1&isAllowed=y (Letöltés ideje: 2023. július 26.)
- DOBÁK Imre (2017): Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében. *Hadmérnök,* 12(2), 235-249. ISSN 1788-1919.
  Online: http://hadmernok.hu/172_19_dobak.pdf (Letöltés ideje: 2024. február 28.)
- DOBÁK Imre (2022): A nemzetbiztonság 21. századi értelmezése és jellemzői. In DOBÁK Imre (szerk.): *Nemzetbiztonság a 21. század elején*. Budapest: Ludovika Kiadó. 13-28. ISBN: 978-963-5316-37-3.
- DOKMAN, Tomislav (2019): Defining the term "Intelligence" - insight into existing intelligence knowledge. *Informatologia*, 52(3-4), 194-204. ISSN 1330-0067
  Online: https://hrcak.srce.hr/file/341342 (Letöltés ideje: 2024. február 19.)
- DR. AZANI, Eitan (2018). *Global Jihad – The Shift from Hierarchal Terrorist Organizations to Decentra-lized Systems*. Herzlia: International Institute for Counter-Terrorism. 12-15.
  Online: https://www.ict.org.il/images/Global%20Jihad%20%E2%80%93%20The%20Shift%20from%20Hierarchal.pdf
  (Letöltés ideje: 2023. december 9.)

- DR. BALOGH Gyöngyi - DR. HACKSPACHER Andrea - DR. BÍRÓ János - DR. SZABÓ Endre Győző - DR. SZÁMADÓ Tamás (2020): *A Nemzeti Adatvédelmi és Információszabadság Hatóság eljárásai*. Budapest: NKE. ISBN 978-963-498-296-8.
  Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/15005/A%20Nemzeti%20Adatvedelmi%20%C3%A9s%20Informacioszabadsag%20Hatosag%20eljarasai.pdf?sequence=3&isAllowed=y (Letöltés ideje: 2024. február 29.)
- DR. BARNÓCZKI László (2019): *Az elszakított testvérek, avagy a titkosszolgálati eszközök hazai szabályozásának lehetséges fejlődési irányai a legújabb kori adatvédelmi jogfejlődés tükrében*. Budapest: ELTE JTI.
- DR. BARTOLITS István (2013): Az over-the-top (OTT) szolgáltatások. In LAPSÁNYSZKY András (szerk.): *Hírközlési-szabályozás, hírközlési-igazgatás hazánkban és az Európai Unióban.* Budapest: Wolters Kluwe CompLex Kiadó. 801-803. ISBN: 978-963-295-236-9.
- DR. BÉRES János (2018): *Külföldi nemzetbiztonsági szolgálatok*. Budapest: Zrínyi Kiadó. ISBN: 978-963-12-9548-1.
- DR. BODA József – DR. DOBÁK Imre (2016): Titkosszolgálatok fejlődése – technikai szemmel. *Nemzetbiztonsági Szemle*, 4(4), 17-25. ISSN 2064-3756
  Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1879/1168 (Letöltés idej: 2024. március 3.)
- DR. DOBÁK Imre – KOVÁCS Zoltán (2014): Új technológiák hatása a hírszerzésre. In DR. DOBÁK Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. 206-200. ISBN: 978-615-5305-49-8.
  Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/100414/609.pdf?sequence=1 (Letöltés ideje: 2024. július 7.);
- DR. DOMOKOS Márton - DR. HORVÁTH Anna Zsófia (2022): *Érkezik a Privacy Shield 2.0? – Nagyító alatt az USA hírszerzési tevékenységek fokozottabb védelméről szóló elnöki rendelete*. Jogi Fórum.
  Online: https://www.jogiforum.hu/blog-adatvedelem-10/2022/10/21/privacy-shield-2-0-nagyito-alatt-az-usa-hirszerzesi-tevekenysegek-fokozottabb-vedelmerol-szolo-elnoki-rendelete/ (Letöltés ideje: 2024. február 27.)

- DR. FÁBIÁN Péter (2021): Az állambiztonságtól a nemzetbiztonságig II. - A nemzetbiztonsági intézményrendszer jogfejlődése 2010-től napjainkig. *Büntetőjogi Szemle*, 10(13), 11-18. ISSN 2063-8183.
  Online: https://ujbtk.hu/wp-content/uploads/lapszam/BJSZ_202002_11-18o_FabianPeter.pdf (Letöltés ideje: 2023. szeptember 11.).
- DR. FIRNIKSZ Judit (2023): *Pillanatkép a digitális piacok szabályozásáról - A DMA a vállalati compliance tükrében.* Doktori (PhD) értekezés. Budapest: PPKE JÁDI 68-69.
  Online:
  https://jak.ppke.hu/storage/tinymce/uploads/Firniksz_Judit_dolgozatv.pdf?u=1c3e6s
  (Letöltés ideje: 2024. február 18.)
- DR. HABIL KISS-BENEDEK József – DR. KENEDLI Tamás (2018): Nemzetközi szervezetek. In DR. BÉRES János (szerk.): *Külföldi nemzetbiztonsági szolgálatok*. Budapest: Zrínyi Kiadó. 251-290. ISBN: 978-963-12-9548-1.
- DR. KARÁCSONY-PRETSNER Kamilla (2013): A hírközlési igazgatás, hírközlési szabályozás hazai története, fejlődése. In LAPSÁNYSZKY András (szerk.): *Hírközlési-szabályozás, hírközlési-igazgatás hazánkban és az Európai Unióban.* Budapest: Wolters Kluwe CompLex Kiadó. 57-82. ISBN: 978-963-295-236-9.
- DR. KOVÁCS Zoltán (2016): Az alkalmazásszolgáltatók törvényes ellenőrzésének jövője – a technológiák konvergenciájának tükrében. *Nemzetbiztonsági Szemle*, 4(1), 79-99. ISSN 2064-3756
  Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1815/1105 (Letöltés ideje: 2023. július 8.)
- DR. NYITRAI Endre (2014): titkos információgyűjtés és a titkos adatszerzés alkalmazása során felmerülő kérdések. *Büntetőjogi Szemle*, 4(3), 32-40. ISSN 2063-8183.
  Online: https://ujbtk.hu/wp-content/uploads/2014/12/bjsz_201403_Nyitrai_Endre.pdf (Letöltés ideje: 2024. február 22.)
- DR. PAPP János Tamás (2021): *A közösségi média platformok szabályozása a demokratikus nyilvánosság védelmében.* Doktori (PhD) értekezése. Budapest: PPKE JÁDI.
  Online: https://real-phd.mtak.hu/1167/1/Papp_Janos_Tamas_dolgozatv.pdf (Letöltés ideje: 2024. február 16.)
- DR. RESPERGER István (2018): *A válságkezelés és a hibrid hadviselés*. Budapest: Dialóg Campus Kiadó. ISBN 978-615-5877-53-7.

Online: https://nbi.uni-nke.hu/document/nbi-uni-nke-hu/Resperger%20Istv%C3%A1n_A%20v%C3%A1ls%C3%A1g kezel%C3%A9s%20%C3%A9s%20a%20hibrid%20hadvisel%C3%A9s.pdf (Letöltés ideje: 2023. július 16.)

- DR. SAARINEN, O. (2023): *Intro to Side-Channel Security of NIST PQC Standards*. NIST PQC Seminar, 04 April 2023.
  Online: https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/pqc-seminars/presentations/2-side-channel-security-saarinen-04042023.pdf (Letöltés ideje: 2024. február 16.)
- DR. SOLTI István (2017): *A titkos információgyűjtés, elvei, eszközei és módszerei, alkalmazásának lehetőségei a nemzetbiztonsági munkában*. Doktori (PhD) értekezés. Budapest: NKE HDI.
  Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12393/ertekezes.pdf?sequence=1 (Letöltés ideje: 2023. július 27.)
- DRUSZA Tamás (2021): A nemzetbiztonsági terület funkciói rendkívüli helyzetekben. In GAÁL Gyula – HAUTZINGER Zoltán (szerk.): *Rendészet a rendkívüli helyzetekben*. Pécs: MHTT. 143-152. ISBN: 978-615-595-40-9-2.
  Online: https://www.pecshor.hu/periodika/XXIII/druszа.pdf (Letöltés ideje: 2024. február 17.)
- DWIVEDI, Vidya Kant – SHUKLA, Manoj (2007): *Code Division Multiple Access (CDMA) System in Multipath Environment.* National Conference on Communication Technology. 1-3.
  Online:www.researchgate.net/publication/200783159_Code_Division_Multiple_Access_CDMA_System_in_Multipath_Environment/link/09984da86bc439f832012f0a/downloadL (Letöltés ideje: 2023. december 19.)
- EHRENBERGER Róbert (2017): A BM III/V. Csoportfőnökség szervezettörténete 1962–1971 között. *Betekintő,* 10(3), 1-13. ISSN 1788 – 7569.
  Online: https://www.betekinto.hu/sites/default/files/betekinto-szamok/2017_3_ehrenberger.pdf (Letöltés ideje: 2023. július 26.)
- ENBERG, Jasmine (2021): *Global Mobile Messaging Forecast 2021 (2021). Business Insider eMarket,* Komandotech.

Online: https://www.insiderintelligence.com/content/global-mobile-messaging-forecast-2021 (Letöltés ideje: 2024. február 26.)

- ERDÉLYI Áron (2021): *Cryptography vizsgajegyzet*. Budapest: PPKE ITK. Online:https://users.itk.ppke.hu/~erdar2/wp-content/uploads/2021/09/Cryprography.pdf (Letöltés ideje: 2024. február 20.)
- ÉRDI Péter (2008): *GSM-UMTS rendszerek szolgáltatásai*. Budapest: NSZFI. Online:https://www.nive.hu/Downloads/Szakkepzesi_dokumentumok/Bemeneti_kompetenciak_meresi_ertekelesi_eszkozrendszerenek_kialakitasa/6_0909_tartalomelem_013_munkaanyag_100331.pdf (Letöltés ideje: 2023. július 30.)
- ERDOGAN, Eylem at al. (2023): Optical HAPS Eavesdropping in Vertical Heterogeneous Networks. *IEEE Open Journal of Vehicular Technology*, 4(1), 208-216. ISSN: 2644-1330.
  Online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10004986 (Letöltés ideje: 2024. február 22.)
- *European Union Serious and Organised Crime Threat Assessment* (SOCTA) 2021. Europol, 2021. 32.
  Online:
  https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf
  (Letöltés ideje: 2023. december 8.)
- FEDERRATH, Hannes (1999): Protection in Mobile Communications. In MÜLLER, Günter – RANNENBERG, Kai (szerk.): *Multilateral Security in Communications*. Harlow, Essex: Addison-Wesley-Longman, 349-364.
  Online: https://epub.uni-regensburg.de/7382/1/Fede3_99Buch3Mobil.pdf (Letöltés ideje: 2024. február 15.)
- FERGUSON, Niels – SCHNEIER, Bruce – KOHNO, Tadayoshi (2010): *Cryptography Engineering: Design Principles and Practical Applications.* Indianapolis: Wiley Publishing, Inc. ISBN: 978-0-470-47424-2.
  Online: https://zlibrary.to/pdfs/cryptography-engineering-pdf (Letöltés ideje: 2024. február 18.)
- FRIESE, Ingo - GALKOW-SCHNEIDER, Mandy – BASSBOUSS, Louay – ZOUBAREV, Alexander (2024): *True 3D Holography: A Communication Service of Tomorrow and Its Requirements for a New Converged Cloud and Network Architecture on the Path to 6G*. Paris: IEEE 2023 2nd International Conference on 6G Networking (6GNet).

Online: https://pfandzelter.com/publication/2023-6gnet/holography-6gnet2023.pdf (Letöltés ideje: 2024. február 22.)

- FÜRJES János (2008): Korszerű rádiófelderítés kihívásai az információs műveletekben. Hadtudomány, 3(2), 88-95. ISSN 1215-4121.
  Online: http://hadmernok.hu/archivum/2008/2/2008_2_furjes.pdf (Letöltés ideje: 2024. február 16.)
- GALLAGHER, Aoife - O'CONNOR, Ciarán (2021): *Layers of Lies: A First Look at Irish Far-Right Activity on Telegram.* London: Institute for Strategic Dialogue. 7-8. Online: https://www.isdglobal.org/wp-content/uploads/2021/04/Layers-of-Lies.pdf (Letöltés ideje: 2023. december 25.)
- GAO, Zhen - KE, Malong - MEI, Yikun- QIAO, Li (2023): Compressive Sensing-Based Grant-Free Massive Access for 6G Massive Communication. *IEEE Internet of Things Journal*, 10(5), 7411 – 7435. ISSN: 2327-4662.
  Online: https://arxiv.org/pdf/2311.06770.pdf (Letöltés ideje: 2024. február 22.)
- GÁRDOS-OROSZ Fruzsina (2020): Az alapjogok korlátozása. In JAKAB András – KÖNCZÖL Miklós – MENYHÁRD Attila – SULYOK Gábor (szerk.): *Internetes Jogtudományi Enciklopédia.* Budapest: ORAC Kiadó. 1-15. ISBN: 978-963-3083-07-9.
  Online: https://ijoten.hu/uploads/az-alapjogok-korlatozasa.pdf (Letöltés ideje: 2024. február 14.)
- GREENWALD, Glenn (2014): *A Snowden-ügy - Korunk legnagyobb nemzetbiztonsági botránya.* Budapest: HVG Könyvek. ISBN: 978-963-3041-83-3.
- GUBICZA József – LAUFER Balázs (2014): Az illegális migráció aktuális trendjei nemzetbiztonsági szemszögből. *Pécsi Határőr Tudományos Közlemények*, 13(10), 293-287-295. ISSN: 1589-1674.
  Online: https://epa.oszk.hu/04500/04581/00015/pdf/EPA04581_pecsi_hataror_2014_287-295.pdf (Letöltés ideje: 2023. szeptember 11.).
- Gyaraki Réka Eszter (2018): *A számítógépes bűnözés nyomozásának problémái.* Doktori (PhD) értekezése. Pécs: PTE ÁJKDI.
  Online: https://ajk.pte.hu/files/file/doktori-iskola/gyaraki-reka/gyaraki-reka-muhelyvita-ertekezes.pdf (Letöltés ideje: 2024. február 20.)

- GYÖRGY András - KOVÁCS László (2001): Az amerikai Minden Adatforrást Elemző Rendszer" (ASAS) és a magyar elektronikai-harc vezetési komplexumok rendszertechnikai összehasonlítása. *Hallgatói Közlemények*, 5(1), 112-128. ISSN: 1417-7307.
- HAIG Zsolt – KOVÁCS László –VÁNYA László – VASS Sándor (2014): *Elektronikai hadviselés*. Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. ISBN: 978-615-5305-87-0.
  Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/100390/564.pdf?sequence=1 (Letöltés ideje: 2024. február 16.)
- HAIG Zsolt (2018): *Információs műveletek a kibertérben*. Budapest: Dialóg Campus Kiadó. ISBN: 978-615-5945-05-2.
  Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/12651/web_PDF_Informacios_muveletek_a_kiberterben.pdf?sequence=1&isAllowed=y (Letöltés ideje: 2024. február 21.)
- HALMAI Gábor - TÓTH Gábor Attila (2023): Az emberi jogok korlátozása. In HALMAi Gábor - TÓTH Gábor Attila (szerk.): *Emberi jogok*. Budapest: Osiris Kiadó. 108-136. ISBN: 978-963-389-952-6.
  Online: https://www.academia.edu/43016928/Emberi_jogok_Human_Rights_ (Letöltés ideje: 2024. február 20.)
- HANKISS Ágnes (2019): Az Iszlám Állam titkosszolgálata - Diverzifikációs Folyamatok. *Arc És Álarc*, 3(1), 117-137. ISSN: 1587-7949
  Online: http://real.mtak.hu/112356/1/HAMVAS_2019_1.pdf (Letöltés ideje: 2023. december 8.)
- HASSAN, Zakaria Abdelwahab - ELGARF1, Talaat A. – ZEKRY, Abdelhalim (2020): Analyzing SNOW and ZUC Security Algorithms Using NIST SP 800-22 and Enhancing their Randomness. *Journal of Cyber Security and Mobility* 9(4), 535–576. ISSN: 2245-4578.
  Online: https://journals.riverpublishers.com/index.php/JCSANDM/article/view/2963/5089 (Letöltés ideje: 2024. február 21.)
- HETESY Zsolt (2011): *A titkos felderítés*. Doktori (PhD) értekezés. Pécs: PTE ÁJKDI.
  Online: https://pea.lib.pte.hu/bitstream/handle/pea/15668/hetesy-zsolt-phd-2012.pdf?sequence=1&isAllowed=y Letöltés ideje: 2023. november 08.)

- HOFFMAN, Frank (2007): *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies. Online:https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf (Letöltés ideje: 2024. március 30.)
- HORMAN aka HORMS, Simon (2005): *SSL and TLS An Overview of A Secure Communications Protocol; Security*. Canbera: Mini-Conf at Linux.Conf.Au. Online: https://projects.horms.net/projects/ssl_and_tls/stuff/ssl_and_tls.pdf (Letöltés ideje: 2024. február 18.)
- HORVÁTH Attila (1991): A tőzsde és a spekuláció. *Rubicon*, 2(9), 20-22. ISSN: 0865-6347.
  Online: https://rubicon.hu/cikkek/a-tozsde-es-a-spekulacio (Letöltés ideje: 2023. december 19.)
- INTOCI, Francesco - STURM, Julian - FRAUNHOLZ, Daniel – PYRGELIS, Apostolos – BARSCHEL, Colin (2023): *P3LI5: Practical and confidEntial Lawful Interception on the 5G core.* New York: Cornell University. ISBN: 979-8-3503-3945-1.
  Online:
  https://www.researchgate.net/publication/373451462_P3LI5_Practical_and_Confidential_Lawful_Interception_on_the_5G_Core (Letöltés ideje: 2024. február 23.)
- JAGADICS Péter – RAJOS Sándor – SIMON László – SZABÓ Károly (2018): *A magyar katonai elhárítás története 1918–2018*. Budapest: Univerzum Könyvek. ISBN: 978-615-5628-66-5.
- JANCSÓ Gábor (2018): Leplezett eszközök alkalmazása: titkos információgyűjtés az új büntetőeljárási törvényben. *Acta Humana*, 6(1), 19-34. ISSN: 0866-6628.
  Online:https://folyoirat.ludovika.hu/index.php/actahumana/article/download/880/255/4337 (Letöltés ideje: 2024. február 15.)
- KAHATE, Atul (2013): *Cryptography and Network Security*. Delhi: Tata McGraw Hill Education Private Limited. ISBN 13: 978-0-07-064823-4.
  Online: https://nayakuch.files.wordpress.com/2015/08/cryptography-network-security-atul-kahate.pdf (Letöltés ideje: 2024. február 20.)
- KASSAI Károly (2023): A honvédelmi célú elektronikus információs rendszerek fejlesztéséhez szükséges, továbblépést megalapozó vizsgálat – egy zöld könyv kialakításának támogatása. *Military and Intelligence CyberSecurity Research Paper*, 2(5). 1-18. ISSN: 2786-3778.

Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/MICRP%202022_5%20Kassai%20K%C3%A1roly%20-%20A%20honv%C3%A9delmi%20c%C3%A9l%C3%BA%20elektronikus%20inform%C3%A1ci%C3%B3s%20rendszerek%20fejleszt%C3%A9s%C3%A9hez%20sz%C3%BCks%C3%A9ges,%20tov%C3%A1bbl%C3%A9p%C3%A9st%20megalapoz%C3%B3%20vizsg%C3%A1lat%20%E2%80%93%20Egy%20z%C3%B6ld%20k%C3%B6nyv%20kialak%C3%ADt%C3%A1s%C3%A1nak%20t%C3%A1mogat%C3%A1sa.pdf (Letöltés ideje: 2024. február 16.);

- Kassai Károly (2023): Az ellenálló képességre (resilience) vonatkozó NATO, EU általános követelmények fontosabb megjelenítéseinek áttekintése. *Military and Intelligence CyberSecurity Research Paper*, 3(8). 1-26. ISSN: 2786-3778. Online: file:///D:/_PC16%20-%20t%C3%B6r%C3%B6lni%20TILOS!/FORWARD/Felhaszn%C3%A1l%C3%B3/Let%C3%B6lt%C3%A9sek/MIC%20RP%202023-8%20-%20Kassai%20K%C3%A1roly%20-%20Az%20ellen%C3%A1ll%C3%B3%20k%C3%A9pess%C3%A9gre%20(resilience)%20vonatkoz%C3%B3%20NATO,%20EU%20%C3%A1ltal%C3%A1nos%20k%C3%B6vetelm%C3%A9nyek%20fontosabb%20megjelen%C3%ADt%C3%A9seinek%20%C3%A1ttekint%C3%A9se.pdf (Letöltés ideje: 2024. február 14.)
- KAUFMAN, C. - PERLMAN, R. - SPECINER, M. (2017): *Network Security: Private Communication in a Public World.* Delhi: Pearson India Education Services Pvt. ISBN: 978-013-0460-19-6.
  Online: https://dokumen.pub/network-security-private-communication-in-a-public-world-2nd-ed-14th-printing-9780130460196-9789332578210-9789332586000-0076092018469-0130460192.html (Letöltés ideje: 2024. február 20.)
- KAUR, Roop Kamal – KAUR, Kamaljit (2015): A New Technique for Detection and Prevention of Passive Attacks in Web Usage Mining. I. *Journal of the Western Mystery Tradition*, 15(6), 53-62. ISSN: 1759-0795.
  Online: https://www.mecs-press.org/ijwmt/ijwmt-v5-n6/IJWMT-V5-N6-7.pdf (Letöltés ideje: 2023. december 20.)
- KENEDLI Tamás (2020): A Katonai Nemzetbiztonsági Szolgálat szakmai fejlődésének legfontosabb sajátosságai az elmúlt években. *Nemzetbiztonsági Szemle*, 8(1), 74-94. ISSN 2064-3756.

Online:https://epa.oszk.hu/02500/02538/00032/pdf/EPA02538_nemzetbiztonsagi_szemle_2020_01_074-094.pdf (Letöltés ideje: 2024. február 19.)

- KIRÁLY Péter Bálint (2021): A videómegosztóplatform-szolgáltatók szabályozásának kihívásai. *In Medias Res*, 10(2), 312-330. ISSN: 2786-152X.
  Online: https://inmediasresfolyoirat.hu/imr/article/view/236/237 (Letöltés ideje: 2024. február 16.)
- KIRCANSKI, Aleksandar – YOUSSEF, Amr M. (2012): On the Sliding Property of SNOW 3G and SNOW 2.0. *IET Information Security*, 5(4), 199-206. ISSN: 1751-8717.
  Online:https://users.encs.concordia.ca/~youssef/Publications/Papers/On%20the%20Sliding%20Property%20of%20SNOW%203G%20and%20SNOW.pdf (Letöltés ideje: 2024. február 21.)
- KIS-BENEDEK József (2013): A nemzetbiztonsági szolgálatok együttműködése. *Hadtudomány,* 13 (1–2), 100-114. ISSN 1215-4121.
  Online: https://www.mhtt.eu/hadtudomany/2013/1_2/HT_2013_1-2_mhtt.pdf (Letöltés ideje: 2023. július 26.)
- KISS Barnabás (2010): Az alapjogok korlátozása az Európai Unió nemzeti alkotmányaiban. *Acta Universitatis Szegediensis: acta juridica et politica*, 54(1), 455-465. ISSN 0324-6523.
  Online: https://acta.bibl.u-szeged.hu/7457/1/juridpol_073_455-465.pdf (Letöltés ideje: 2023. november 08.)
- KISS Petra (2012): A magyar stratégiai gondolkodás változása a nemzeti biztonsági stratégiák tükrében. *Hadtudomány*, 22(3-4), 68-79. ISSN 1215-4121.
  Online: https://www.mhtt.eu/hadtudomany/2012/3_4/HT_2012_3-4_Kiss_Petra.pdf (Letöltés ideje: 2024. február 16.)
- KISS Tamás (2018): *Massive MiMo megvalósitása az 5G-ben*. Budapest: HTE Rádiószakosztály Rendezvény. 9-22.
  Online: https://www.hte.hu/documents/10180/4582184/HTE+MiMo.pdf/b96bc127-afbc-8a1c-001f-a20a907c731b (Letöltés ideje: 2024. február 22.)
- KISS-BENEDEK József (2013): A nemzetbiztonsági szolgálatok nemzetközi együttműködése. In DR. KOBOLKA István (szerk.): *Nemzetbiztonsági alapismeretek*. Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó. 341-365. ISBN 978-615-5344-32-9.

- KOLTAY András - MAYER Annamária - NYAKAS Levente - POGÁCSÁS Anett (2014): *A médiaszolgáltatás és a sajtótermék fogalma az új magyar médiaszabályozásban*. Budapest: NMHH Médiatudományi Intézet. 21-27. Online: https://nmhh.hu/dokumentum/162242/tajekoztato02.pdf (Letöltés ideje: 2024. február 16.)
- KÓNYÁNÉ KUTRUCZ Katalin – PETRIKNÉ VÁMOS Ida (2017): *Ügynöksorsok – Ügynök? Sorsok? A hálózati lét sokfélesége és a megismerés korlátai*. Budapest: Nemzeti Emlékezet Bizottsága. ISBN: 978-615-5656-04-0.
  Online: https://kiadvanyok.neb.hu/asset/phpNR3lWe.pdf (Letöltés ideje: 2023. július 26.)
- KOPPÁNYI Zoltán (2012): *GSM-alapú helymeghatározás*. Budapest: BME. Online: https://www.researchgate.net/publication/291331803_GSM-alapu_helymeghatarozas (Letöltés ideje: 2023. július 30.)
- KOUTSOS, Adrien (2019): *The 5G-AKA Authentication Protocol Privacy*. Stockholm: IEEE Institute of Electrical and Electronics Engineers. 464-479. ISBN:978-1-7281-1148-3.
  Online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8806761 (Letöltés ideje: 2024. február 21.)
- KOVÁCS Anita (2019): A végfelhasználók jogai az új Európai Elektronikus Hírközlési Kódexben. *Híradástechnika*, 74(1), 44-48. ISSN: 0018-2028.
  Online:
  https://www.hiradastechnika.hu/documents/4743302/0/HT_2019_Infokom2018.pdf
  (Letöltés ideje: 2024. február 21.)
- KOVÁCS István (2023): A nemzetközi szervezett bűnözés statisztika elemzése a SOCTA és Eurostat rendszerekben. *Belügyi Szemle*, 71(5), 849-866. ISSN 2677-1632.
  Online: https://doi.org/10.38146/BSZ.2023.5.6 (Letöltés ideje: 2023.december 8.)
- KOVÁCS László (2000): Az összadatforrású felderítés és a pilótanélküli felderítő repülő eszközök kapcsolata. *Repüléstudományi közlemények*, 12(1), 231-238. ISSN 2064-7123.
  Online: https://epa.oszk.hu/02600/02694/00026/pdf/EPA02694_rtk_2000_01_231-238.pdf (Letöltés ideje: 2024. április 1.)
- KOVÁCS László (2020): A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle*, 145(5.) 3-18.

ISSN 2060-1506
Online:https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/120/121 (Letöltés ideje: 2023. november 08.)

- KOVÁCS László (2023): *Hadviselés a 21. században: kiberműveletek.* Budapest: Ludovika Egyetemi Kiadó. ISBN: 978-963-531-765-3.
- KOVÁCS László mk. őrnagy (2003): *Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmazhatósága a Magyar Honvédségben*. Doktori (PhD) értekezés. Budapest: ZMNE.
  Online:https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/11964/Teljes%20sz%C3%B6veg!.pdf?sequence=1 (Letöltés ideje: 2024. február 16.)
- KOVÁCS Zoltán (2013): Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. *Hadmérnök,* 8(3), 184-197. ISSN 1788-1919. Online: http://hadmernok.hu/133_18_kovacsz_2.pdf (Letöltés ideje: 2023. július 8.)
- KOVÁCS Zoltán (2013): Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II. *Hadmérnök,* Hadmérnök. 8(3), 198-210. ISSN 1788-1919. Online: http://hadmernok.hu/133_19_kovacsz_3.pdf (Letöltés ideje: 2023. július 8.)
- KOVÁCS Zoltán (2015): *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai.* Doktori (PhD) értekezés. Budapest: NKE KMDI. Online https://adoc.tips/az-infokommunikacios-rendszerek-nemzetbiztonsagi-kihivasai.html (Letöltés ideje: 2023. július 8.)
- KOVÁCS Zoltán (2016): Biztonság vs. törvényes ellenőrzés az internet alapú kommunikációban - ellentétes vagy egymással megférő követelmények? I. *Hadmérnök*, 11(4), 126-141. ISSN 1788-1919.
  ISSN: 1788-1929
  Online: http://hadmernok.hu/164_11_kovacs.pdf (Letöltés ideje: 2024. február 20.)
- KOVÁCS Zoltán (2020): Bűnügyi technikai hírszerzés – A mobilhírközlő hálózatok törvényes ellenőrzésének jövője. In RUZSONYI Péter (szerk.): *Közbiztonság: Fenntartható biztonság és társadalmi környezet tanulmányok III.* Budapest: Ludovika Kiadó. 899-923.
  Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16197/TKP_Kozbiztonsag.pdf#page=900;j

sessionid=F91F1F5C208E65004CE571CB742794DB?sequence=1 (Letöltés ideje: 2024. február 25.)

- KOVÁCS Zoltán (2021): *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai*. Budapest: Ludovika Egyetemi Kiadó.
- KOVÁCS, László (2018): Cyber Security Policy and Strategy In The European Union and NATO. *Land Forces Academy Review,* 23(1), 16-24. ISSN: 2247-840X. Online: https://doi.org/10.2478/raft-2018-0002 (Letöltés ideje: 2024. február 25
- KOVÁTS Ildikó (2006): Információs társadalom, emberi tényező, civil társadalom, média – Adalékok a magyarországi digitális műsorszórás előrejelzéséhez. *Jel-kép*, 26(29, 19-36. ISSN: 0209-584X. Online: http://real-j.mtak.hu/5612/2/JelKep 2006 2.pdf (Letöltés ideje: 2023. július 9.)
- KRAHULCSÁN Zsolt (2007): KGB és III. Főcsoportfőnökség: egy kapcsolat vége…(?) (A szovjet– magyar állambiztonsági együttműködés szabályozása 1989-ben). *Betekintő*, 1(4), 1-24. ISSN: 1788-7569. Online: https://www.betekinto.hu/sites/default/files/betekinto-szamok/2007_4_krahulcsan.pdf (Letöltés ideje: 2023. július 26.)
- KULKARNI, Mandar M.– BHIDE, Prof. A. S. – CHAUDHARI, Prafull P. (2013): Encryption Algorithm Addressing GSM Security Issues - A Review. *International Journal of Latest Trends in Engineering and Technology*, 2(2), 268-273. ISSN: 2278-621X. Online: https://www.ijltet.org/wp-content/uploads/2013/04/40.pdf (Letöltés ideje: 2024. február 21.)
- KUR, Gunes Karabulut at al. (2021): A Vision and Framework for the High Altitude Platform Station (HAPS) Networks of the Future. *IEEE Communications Surveys & Tutorials*, 23(2), 729-779. ISSN: 1553-877X. Online: https://ieeexplore.ieee.org/document/9380673 (Letöltés ideje: 2024. február 22.)
- LAPSÁNYSZKY András (szerk.) (2013): *Hírközlési-szabályozás, hírközlési-igazgatás hazánkban és az Európai Unióban.* Budapest: Wolters Kluwe CompLex Kiadó. ISBN: 978-963-295-236-9.
- LIU, Edward C. (2021): *Foreign Intelligence Surveillance Act (FISA): An Overview*. Congressional Research Service. Online: https://sgp.fas.org/crs/intel/IF11451.pdf (Letöltés ideje: 2024. február 28.)

- MAJOR Iván (1998): *A távközlés privatizációja*. Budapest: Állami Privatizációs és Vagyonkezelő Rt.
- MALLINSON, Keith (2016): *The path to 5G: as much evolution as revolution*. 3GPP News. ISSN: 2246-0853.
  Online: https://www.3gpp.org/news-events/3gpp-news/5g-wiseharbour (Letöltés ideje: 2024. február 21.)
- MARQUIS-BOIRE, Morgan – MARCZAK, Bill – GUARNIERI, Claudio – SCOTT-RAILTON, John (2013): *For their eyes only - The Commercialization of Digital Spying*. Citizen Lab and University of Toronto.
  Online: https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf (Letöltés ideje: 2024. február 15.)
- MCADAM, James G. (2026): *Foreign Intelligence Surveillance Act (FISA): An Overview.* Glynco: Federal Law Enforcement Training Centers.
  Online: https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf (Letöltés ideje: 2024. február 28.)
- MÉSZÁROS István: *Oktatási segédlet a Telekommunikáció tantárgy Vezetékes távközlés részéhez.* Győr: Széchenyi István Egyetem.
  Online: http://vip.tilb.sze.hu/~wersenyi/TKJ2.pdf (Letöltés ideje: 2024. február 22.)
- MOHAY Ágoston (2014): Opt-out/opt-in megoldások az uniós bel- és igazságügyi együttműködés terén: sokféleség az egységben? *Közjogi Szemle*, 8(1), 33-43. ISSN: 1789-6991.
  Online: https://szakcikkadatbazis.hu/doc/3328139 (Letöltés ideje: 2024. február 28.)
- MOHSAN, Syed Agha Hassnain – LI, Yanlong (2023): *IRS-assisted UAV Communications: A Comprehensive Review*. New York: Cornell University. 1-29.
  Online: https://arxiv.org/ftp/arxiv/papers/2306/2306.15838.pdf (Letöltés ideje: 2024. február 22.)
- MUHA Lajos – KRASZNAY Csaba (2018): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem. ISBN: 978-963-498-059-9.
  Online: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/12932 (Letöltés ideje: 2024. február 15.)

- MUHA Lajos (2007): *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme*. Doktori (PhD) értekezés. Budapest: ZMNE. Online: http://real-phd.mtak.hu/74/1/1228916.pdf (Letöltés ideje: 2024. február 12.)
- NAGY Anita (2017): Európai nyomozási határozat a kölcsönös elismerés elve tükrében. *Kúria Lapja*, 65(6), 1-9. ISSN: 2063-9767. Online: https://real.mtak.hu/86782/1/NagyanitaEur%c3%b3painyomoz%c3%a1si.pdf (Letöltés ideje: 2024. február 28.)
- NAGY Eszter (2022): *Digital Market és Digital Services Act – Hatályba léptek az online platformokra vonatkozó uniós szabályok*. Pécs-Baranyai Kereskedelmi és Iparkamara. Online: https://pbkik.hu/2022/11/22/een/digital-market-es-digital-services-act-hatalyba-leptek-az-online-platformokra-vonatkozo-unios-szabalyok/ (Letöltés ideje: 2024. február 18.)
- NAIR, Suresh – KHARE, Saurabh – PING, Jing (2022): Authentication and Key Management for Applications (AKMA) in 5G. *Highlights,* 2(5), 4-5. ISSN: 2246-0853. Online: https://www.3gpp.org/newsletter-issue-05-oct-2022 (Letöltés ideje: 2024. február 21.)
- *NATO Glossary of Terms and Definitions AAP-06 (2021)*. NATO Standardization Office. 2021. 65.
- NEGREIRO, Mar (2023): A*t a Glance - Digital issues in focus - E2E encryption and protection of children online*. European Parliament ResearchService. Online: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/751473/EPRS_ATA(2023)751473_EN.pdf (Letöltés ideje: 2024. február 27.)
- NEMESLAKI András (2018): *Információs társadalom*. Budapest: Dialóg Campus Kiadó. ISBN 978-615-5920-01-1 Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12655/web_PDF_ATMA_Informacios_tarsadalom.pdf;jsessionid=33682253A09701DAF4AF3EDB5EC40EE4?sequence=1 (Letöltés ideje: 2024. február 21.)
- NÉMETH Attila (2018): Az infokommunikáció szabályozási környezetének fejlődése a nemzetbiztonsági tevékenység vonatkozásában. *Szakmai Szemle*, 16(2), 53-68. ISSN: 1785-1181.

Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2018_2_szam.pdf (Letöltés ideje: 2023. április 9.)

- OLÁH István – MAGYAR Sándor (2023): Biztonsági kérdések egy publikus felhőben. *Military and Intelligence CyberSecurity Research Paper*, 3(1). 1-8. ISSN: 2786-3778. Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/MIC%20RP%202023-1%20Ol%C3%A1h%20Istv%C3%A1n%20-%20Magyar%20S%C3%A1ndor%20Biztons%C3%A1gi%20k%C3%A9rd%C3%A9sek%20egy%20publikus%20felh%C5%91ben.pdf (Letöltés ideje: 2023. december 19.)
- OSZTOVITS András (szerk.) (2011): *Az Európai Unió és az Európai Unió Működéséről szóló Szerződések magyarázata*. Budapest: Complex. ISBN: 978-963-2951-36-2.
- PAAR, Christof – PELZ, Jan (2010): *Understanding Cryptography*. New York: Springer Publishing Company. ISBN: 978-3-642-04101-3.
  Online: https://link.springer.com/book/10.1007/978-3-642-04101-3 (Letöltés ideje: 2024. február 20.)
- PÉTEFALVI Attila (2013): A nemzetbiztonsági ellenőrzés új szabályairól. *Acta Humana*, 1(1), 49-66. ISSN: 0866-6628.
  Online: https://real.mtak.hu/122840/1/AH_2013_1_Peterfalvi_Attila.pdf (Letöltés ideje: 2024. február 14.)
- PÉTERFALVI Attila (2022): *A magánszféra védelme a nemzetbiztonsági célú titkos információgyűjtés során*. Habilitációs tézisek. Budapest: PPKE JÁKDI. Online: https://jak.ppke.hu/storage/tinymce/uploads/old/uploads/articles/2198023/file/Peterfalvi_Attila_habilitacios_tezis.pdf (Letöltés ideje: 2024. február 20.)
- PFEFFERKORN, Riana (2023): *EU member states still cannot agree about end-to-end encryption*. Stanford: The Center for Internet and Society, Stanford Law School. Online: https://cyberlaw.stanford.edu/blog/2023/06/eu-member-states-still-cannot-agree-about-end-end-encryption (Letöltés ideje: 2024. február 27.)
- PÓSERNÉ OLÁH Valéria (2008): Rejtjelező módszerek vizsgálata. *Hadtudományi Szemle*, 1(1), 43-52. ISSN: 2060-0437.
  Online:https://www.epa.hu/02400/02463/00001/pdf/EPA02463_hadtudomanyi_szemle_2008_1_043-052.pdf (Letöltés ideje: 2024. február 16.)

- POZSÁR-SZENTMIKLÓSY Zoltán (2014): Az alapjogi teszt újrafogalmazása. *Jogtudományi Közlöny*, 69(1), 23-34. ISSN: 0021-7166. Online: https://real.mtak.hu/108751/1/jk1401_3.pdf (Letöltés ideje: 2024. február 14.)
- *Preliminary findings on traffic management practices in Europe show that blocking of VoIP and P2P traffic is common, other practices vary widely*. BEREC. 2012. 8-9.; 22. Online:https://www.berec.europa.eu/sites/default/files/files/document_register/2012/7/BoR12_30_tm-snapshot.pdf (Letöltés ideje: 2024. február 15.)
- PRIYANKA, A. – GAUTHAMARAYATHIRUMAL, P. – CHANDRASEKAR, C. (2023): Machine learning algorithms in proactive decision making for handover management from 5G & beyond 5G. *Egyptian Informatics Journal*, 24(3), 1-11. ISSN: 1110-8665. Online: https://www.sciencedirect.com/science/article/pii/S1110866523000452 (Letöltés ideje: 2024. február 22.)
- RÉVÉSZ Béla (2003): Az állambiztonságtól a nemzetvédelemig. *Acta Universitatis Szegediensis Acta Juridica et Politica*, 63(17). 1-92. ISSN: 0324-6523. Online: https://mek.oszk.hu/01500/01582/01582.pdf (Letöltés ideje: 2023. július 27.)
- RIZZO, Carmine (2022): *Lawful Interception in mobile networks*, 3GPP MCC. ISSN: 2246-0853. Online: https://www.3gpp.org/technologies/li (Letöltés ideje: 2023. július 27.)
- SABJANICS István (2013): Adatvédelem és terrorellenes intézkedések az Egyesült Államokban: A MATRIX modellkísérlet története és visszhangjai. In GERENCSÉR Balázs Szabolcs (szerk.): *Modellkísérletek a közigazgatás fejlesztésében: Az ún. „pilot projektek" határai elméletben és gyakorlatban.* Budapest: Pázmány Press. 79-88. ISBN 978-963-308-135-8. Online: https://jak.ppke.hu/uploads/articles/227518/file/modellkiserletek_kotet.%20_0515pdf.FINAL.pdf (Letöltés ideje: 2024. július 13.)
- SABJANICS István (2017): A nemzetbiztonság jogi koncepciója. In CSINK Lóránt (szerk.): *A nemzetbiztonság kihívásainak hatása a magánszférára*. Budapest: Pázmány Press. 103-124. ISBN 978-963-308-319-2. Online: https://jak.ppke.hu/uploads/articles/1185528/file/Csink_maganszfera_TAN40.pdf (Letöltés ideje: 2024. február 19.)

- SABJANICS István (2017): Az Alkotmánybíróság határozata a bírák nemzetbiztonsági ellenőrzéséről: A jogállamiság gyakorlati értelmezésének két konkuráló oldala. *Jogesetek magyarázata*, 8(4), 19-24. ISSN: 2061-4837.
- SABJANICS István (2021): *A terrorizmus hatásai és megjelenése a demokratikus jogrendben*. Budapest: Akadémiai Kiadó. 2.3 fejezet. ISBN: 978-963-454-710-5.
- SABJANICS, István (2022): Rebooting US-EU Data Transfers in the Pipeline - The Resurrection of the Acclaimed Privacy Shield. *Hungarian Yearbook of International Law And European Law*, 10(1), 205-216. ISSN: 2666-2701. Online: https://www.elevenjournals.com/tijdschrift/HYIEL/2022/1/HYIEL_2666-2701_2022_010_001_012.pdf (Letöltés ideje: 2024. július 7.)
- SAGARKUMAR B. Patel (2018): Comparative Study of 2G, 3G and 4G. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 3(3), 1962-1964. ISSN: 2456-3307. Online:https://www.researchgate.net/publication/327763959_Comparative_Study_of_2G_3G_and_4G (Letöltés ideje: 2023. július 25.)
- SALLAI Gyula (2018): *Az okos városok - (Smart City)*. Budapest: Dialóg Campus Kiadó. ISBN: 978-615-5920-23-3. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12649/Web_PDF_Smart_City.pdf (Letöltés ideje: 2024. február 21.)
- SANENGA, Abraham – MAPUNDA, Galefang Allycan – JACOB, Tshepiso Merapelo Ludo – CHUMA, Joseph Monamati at al. (2020): An Overview of Key Technologies in Physical Layer Security. *Entropy Reviews*, 22(11), 1261. ISSN: 1099-4300. Online: https://www.mdpi.com/1099-4300/22/11/1261 (Letöltés ideje: 2024. február 22.)
- SCHNEIER, Bruce (1996*): Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C.* New Jersey: John Wiley & Sons. ISBN: 978-047-1128-45-7.
- SCHWAB, Klaus (2017): *The Fourth Industrial Revolution*. London: Penguin. ISBN: 978-024-1300-75-6.
- SHANNON, Claude E. (2001): A mathematical theory of communication. *Mobil Computing and Communications Review*, 5(1) 3–55. ISSN: 1931-1222.

Online: https://dl.acm.org/doi/10.1145/584091.584093 (Letöltés ideje: 2024. február 22.)

- SHAO, Yulin- CAO, Qi – GUNDUZ, Deniz (2023): *A Theory of Semantic Communication*. New York: Cornell University.
  Online: https://arxiv.org/pdf/2303.05181.pdf Letöltés ideje: 2024. február 22.)
- SHERIF, Ahmed (2024): *Global information technology industry forecast 2019-2022, by region*. Statista.
  Online: https://www.statista.com/statistics/507365/worldwide-information-technology-industry-by-region/ (Letöltés ideje: 2024. február 23.)
- SIMON László – DR. MAGYAR Sándor (2017): A terrorizmus és indirekt hatása a kibertérben. *Nemzetbiztonsági Szemle*, 5(3), 98-101. ISSN: 2064-3756.
  Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1685/991 (Letöltés ideje: 2023. július 9.)
- SOLTI István (2014): A nemzetbiztonsági stratégia a Nemzeti Biztonsági Stratégia tükrében. *Nemzetbiztonsági Szemle*, 2(3), 47-60. ISSN: 2064-3756. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/2084/1362 (Letöltés ideje: 2024. február 14.)
- SYI (2018): Az adatkor hajnalán. *Jel-kép*, 7(1), 20-33. ISSN: 0209-584X. Online: https://communicatio.hu/jelkep/2018/1/JelKep_2018_1_Syi.pdf (Letöltés ideje: 2024. február 20.)
- SZABÓ Hedvig – DOBÁK Imre (2021): Az információs társadalom nemzetbiztonsága. *Nemzet és Biztonság – Biztonságpolitikai Szemle*, 14(2), 93-110. ISSN: 2559-8651. Online: https://folyoirat.ludovika.hu/index.php/neb/article/view/5781/4819 (Letöltés ideje: 2023. július 9.)
- SZABÓ Hedvig (2023): A tudomány és a nemzetbiztonsági érdek, mint a polgári nemzetbiztonsági szolgálatok tudományos működésének új modellje, különféle tényezők hatása innovációs tevékenységükre a mesterséges intelligencia korában. *Nemzetbiztonsági Szemle*, 11(2), 47-56. ISSN: 2064-3756.
  Online:
  https://folyoirat.ludovika.hu/index.php/nbsz/article/download/6823/5491/29642
  (Letöltés ideje: 2024. február 14.)

- SZABÓ Marcell (2022): Az Európai Unió jogrendszere. In SZABÓ Marcell – GYENEI Laura – LÁNCOS Petra Lea – PÜNKÖSTY András (szerk.): *Az Európai Unió jogának alapjai*. Budapest: Pázmány Press. 97-173. ISBN 978-963-308-418-2
- SZABÓ Mátyás (2018): Állambiztonsági eszköztár – az operatív-technikai rendszabályok és módszerek. *Szakmai Szemle*, 16(1), 7-32. ISSN: 1785-1181. Online: http://real.mtak.hu/85808/1/7_PDFsam_2018_1_szam.pdf (Letöltés ideje: 2023. július 26.)
- SZABÓ Zsuzsanna (2017): *Kriptográfiai protokollok*. Budapest: Eötvös József Tudományegyetem.
  Online:
  https://web.cs.elte.hu/blobs/diplomamunkak/bsc_matelem/2018/szabo_zsuzsanna.pdf
  (Letöltés ideje: 2024. február 16.)
- SZÁDECZKY Tamás (2016): Kriptográfiai protokollok megfelelősége; *Hadmérnök*, 11(4), 178-183. ISSN: 1788-1919.
  Online: http://real.mtak.hu/49982/1/164_15_szadeczky.pdf (Letöltés ideje: 2024. február 16.)
- SZÉKELY Dénes (2003): *Hálózati biztonság és védelem*. Csíkszereda: Babes-Bolyai Egyetem.
  Online: https://konyv.webgobe.com/3-fej/3titkos.html (Letöltés ideje: 2023. december 20.)
- SZENDREI Ferenc (2020): A rendészeti célú titkos információgyűjtés. *Rendőrségi Tanulmányok*, 3(3), 58-80. ISSN: 2630-8002.
  Online:https://epa.oszk.hu/04000/04093/00012/pdf/EPA04093_rendorsegi_tanulmanyok_2020_3_058-080.pdf (Letöltés ideje: 2024. február 15.)
- SZŐKE Gergely László (2013): Az adatvédelem szabályozásának történeti áttekintése. *Infokommunikáció és jog*, 56(3), 107-112. ISSN: 1786-0776.
  Online: https://infojog.hu/wp-content/uploads/pdf/201356_SzokeGergelyLaszlo.pdf
  (Letöltés ideje: 2024. július 9.)
- TAKÁCS Péter (2009): *Kriptográfiai protokollok formális vizsgálata a CSN logikai rendszer bővítésével*. Doktori (PhD) értekezés. Debrecen: DE ITDI.
  Online: https://dea.lib.unideb.hu/server/api/core/bitstreams/7eca2ade-7dfa-4d4f-9360-c12c8f592019/content (Letöltés ideje: 2024. február 20.)

- TAKIELDEEN, Ali - ASHRAF, Eman - FAYEZ, Nihal - MOHAMED, Mohamed Abdel-Azim (2017): Novel Cryptographic Algorithm for 4G / LTE-A. *International Journal of Computer Applications*, 143(1), 5-9. ISSN: 0975-8887. Online:https://www.researchgate.net/publication/316220876_Novel_Cryptographic_Algorithm_for_4G_LTE-A (Letöltés ideje: 2024. február 22.)
- TÁLAS Péter (2013): A nemzeti katonai stratégia és a magyar stratégiai kultúra. *Hadtudomány*, 23(3-4), 14-28. ISSN: 1215-4121. Online: https://www.mhtt.eu/hadtudomany/2013/3_4/Hadtudomany_2013_3-4_3.pdf (Letöltés ideje: 2024. február 16.)
- TALVITIE, Jukka – SÄILY, Mikko – VALKAMA, Mikko (2023) Orientation and Location Tracking of XR Devices: 5G Carrier Phase-Based Methods. *IEEE Journal Of Selected Topics In Signal Processing*, 17(5), 919-934. ISSN: 1941-0484. Online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10232971 (Letöltés ideje: 2024. február 22.)
- TANENBAUM, Andrew S. – WETHERALL, David J. (2013): *Számítógép-hálózatok*. Budapest: Panem Könyvek. 60-61. ISBN: 978-963-5455-29-4. Online: http://gbb2.atw.hu/kieg/szte/tanenbaum_szamhalo.pdf (Letöltés ideje: 2024. február 18.)
- TARJÁN M. Tamás: *1838. január 6. – Morse első sikeres távírókísérlete.* Rubiconline. Online:www.rubicon.hu/magyar/oldalak/1838_januar_6_morse_elso_sikeres_taviroki serlete (Letöltés ideje: 2024. február 22.)
- THANKAPPAN, Manesh - RIFA-POUS, Helena - GARRIGUES, Carles (2022): Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review. *Expert Systems with Applications*, (210). ISSN: 0957-4174. Online: https://doi.org/10.1016/j.eswa.2022.118401 (Letöltés ideje: 2024. február 15.)
- TÓTH Tamás (2019): Az Európai Unió tervezett kiberbiztonsági tanúsítási keretrendszerének bemutatása *Szakmai Szemle*, 17(1), 97-115. ISSN: 1785-1181. Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2019_1_szam.pdf (Letöltés ideje: 2024. február 17.)
- TÓTH Tamás (2020): A mobilhálózatok technológiai fejlődéstörténete: Az analóg hangátviteltől az 5G-hálózatokig. *Nemzetbiztonsági Szemle*, 7(4), 44-60. ISSN: 2064-3756. Online: https://doi.org/10.1007/s11276-015-1165-z (Letöltés ideje: 2023. július 26.)

- TÓTH Tamás (2020): Az egyes social engeneering módszerek elhatárolása és rendszerezése. *Szakmai Szemle*, 18(1), 87-110. ISSN: 1785-1181. Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2020_1_szam.pdf#page=87 (Letöltés ideje: 2024. február 27.);
- TÓTH Tamás (2020): Az információgyűjtő szervezetek technikai képességeire ható külső közvetett tényezők. *Felderítő Szemle*, 19(2), 43-57. ISSN: 1588-242X. Online: https://www.knbsz.gov.hu/hu/letoltes/fsz/2020-2.pdf#page=43 (Letöltés ideje: 2024. február 14.)
- TÓTH Tamás (2022): Magyarország nemzeti biztonsági stratégiai evolúciója, annak aktualitásai és főbb nemzetbiztonsági vetületei. *Szakmai Szemle*, 20(2), 58-73. ISSN: 1785-1181. Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_2_szam.pdf#page=58 (Letöltés ideje: 2024. február 16.)
- TÓTH Tamás (2022): Magyarország Nemzeti Biztonsági Stratégiájának nemzetbiztonsági aspektusú elemzése. *Szakmai Szemle,* 20(3), 69-99. ISSN: 1785-1181. Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_3_szam.pdf (Letöltés ideje: 2024. február 16.)
- TÓTH Tamás (2022): Az információgyűjtés új típusú kihívásai a mobil hírközlési hálózatok technológiai fejlődésének aspektusából. In SZELEI Ildikó (szerk.): *A hadtudomány aktuális kérdései napjainkban*. Budapest: Ludovika Egyetemi Kiadó. 105-122. ISBN: 978-963-531-61-6-8. Online: https://webshop.ludovika.hu/termek/konyvek/hadtudomany/a-hadtudomany-aktualis-kerdesei-napjainkban-ii/ (Letöltés ideje: 2024. február 23.)
- TÓTH Tamás (2023): *A kibervédelem és a nemzetbiztonsági célú törvényes kommunikációellenőrzés viszonyrendszere*. Diplomamunka. Budapest: NKE.
- TÓTH Tamás (2023): Actualities of certain security aspects of cryptography with regard to information societies. *National Security Review*, 9(1), 107-118. ISSN: 2416-3732. Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2023_1_NSR.pdf#page=107 (Letöltés ideje: 2024. február 16.)
- TÓTH, Tamás (2019): General description of social engineering and its place in information warfare. *National Security Review*, 5(1), 42-55. ISSN: 2416-373. Online: https://doi.org/10.38146/BSZ.SPEC.2020.2.9 (Letöltés ideje: 2024. február 27.)

- VAILSHERY, Lionel Sujay (2022): *Number of IoT connected devices worldwide 2019-2021, with forecasts to 2030*. Statista.
  Online: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (Letöltés ideje: 2024. február 23.)
- VAJDA István (1998): *Kriptográfia bevezető*. Budapest: BME VIK. Online: http://www.hit.bme.hu/~buttyan/courses/BMEVIHI4363/theory.pdf (Letöltés ideje: 2024. február 20.)
- VÁRI Péter (2020): *Ég és Föld közötti kapcsolatok – Az űrtávközlés története, elmélete és gyakorlata*. Budapest: Wolters Kluwer. ISBN: 978-963-2959-59-7.
- VEBLEN, Thorstein (1978): *The Theory of Business Enterprise*. London: Routledge. ISBN: 978-087-8556-99-1.
- VIRÁG Tamara (2015): *Telefon.* Budapest: Magyar Szabadalmi Hivatal. Online: https://www.sztnh.gov.hu/en/node/2748 (Letöltés ideje: 2023. december 19.)
- WANG, Dawei – LI, Xuanrui - HE, Yixin – ZHOU, Fuhui – WU, Qihui (2023): Intelligent reflecting surface assisted untrusted NOMA transmissions: a secrecy perspective. *Science China Information Sciences Research Paper*, 66(192302). ISSN: 1869-1919. Online: https://doi.org/10.1007/s11432-022-3653-y (Letöltés ideje: 2024. február 22.)
- XIAOYU, Shi (2016): *Breaking Down iMessage's End-to-End Encryption, and How It Got Hacked in iOS 9.3*. Medford: Tufts University.
  Online: http://www.cs.tufts.edu/comp/116/archive/fall2016/xshi.pdf (Letöltés ideje: 2023. november 13.)
- ZEIDLER Sándor (2014): Pokorny Hermann kitüntetései és ami mögötte van. In BODA József – PARÁDI József (szerk.): *A XIX-XX. századi magyar állam nemzetbiztonsági szervezetei*. Budapest: Nemzetbiztonsági Szakszolgálat és a Szemere Bertalan Magyar Rendvédelem-történeti Tudományos Társaság. ISBN: 978-963-89-8280-3.
- ZENTAI Dániel (2021): *Kriptográfia a kvantumszámítógépek világában*. Budapest: „Infokommunikáció 2021" Konferencia kiadvány és korreferátum gyűjtemény, *Hírvillám*, 12(3), 201-208. ISSN: 2061-9499.
  Online: https://comconf.hu/kiadvany/H%C3%ADrvill%C3%A1m_2021_3.pdf (Letöltés ideje: 2024. február 18
- *20 éves a Nemzetbiztonsági Szakszolgálat*. Budapest: NBSZ. 2016.

Statisztikák:

- *A mobilpiaci jelentés adattáblái – 2022. II. félé. 22.* NMHH. 2023. Online: https://nmhh.hu/cikk/238782/A_mobilpiaci_jelentes_adattablai__2022_II_felev (Letöltés ideje: 2023. július 29.)
- *A mobilpiaci jelentés adattáblái – 2023. II. negyedév.* NMHH. 2024. Online: https://nmhh.hu/dokumentum/243792/mobilpiaci_jelentes_adattablak_2023_ii_negyedev.xlsx (Letöltés ideje: 2023. július 29.);
- *Az NMHH mobilpiaci jelentése - 2018. II. félév.* NMHH. 2019. Online: https://nmhh.hu/dokumentum/203075/NMHH_mobilpiaci_jelentes_2015Q42018Q4.pdf (Letöltés ideje: 2024. július 15.);
- *Az NMHH mobilpiaci jelentése - 2023. II. negyedév*. NMHH. 2024. Online: https://nmhh.hu/dokumentum/243790/nmhh_mobilpiaci_jelentes_2023_ii_negyedev.pdf (Letöltés ideje: 2024. február 24.)
- *Global Overview – Czech Republic.* Meta. 2024. Online https://transparency.fb.com/reports/government-data-requests/country/CZ/ (Letöltés ideje: 2024. február 27.)
- *Global Overview - France.* Meta. 2024 . Online: https://transparency.fb.com/reports/government-data-requests/country/FR/ (Letöltés ideje: 2024. február 27.)
- *Global Overview - Germany.* Meta. 2024. Online: https://transparency.fb.com/reports/government-data-requests/country/DE/ (Letöltés ideje: 2024. február 27.)
- *Global Overview - Hungary.* Meta. 2024. Online: https://transparency.fb.com/reports/government-data-requests/country/HU/ (Letöltés ideje: 2024. február 27.)
- *Global Overview - Poland.* Meta. 2024. Online: https://transparency.fb.com/reports/government-data-requests/country/PL/ (Letöltés ideje: 2024. február 27.)

- *Global Overview - Romania.* Meta. 2024.
  Online: https://transparency.fb.com/reports/government-data-requests/country/RO/ (Letöltés ideje: 2024. február 27.)
- *Global Overview - Slovakia.* Meta. 2024.
  Online: https://transparency.fb.com/reports/government-data-requests/country/SK/ (Letöltés ideje: 2024. február 27.)
- *Global Overview - Spanis.* Meta. 2024.
  Online: https://transparency.fb.com/reports/government-data-requests/country/ES/ (Letöltés ideje: 2024. február 27.)
- *Global Overview – United Kingdom*. 2024.
  Online: https://transparency.fb.com/reports/government-data-requests/country/GB/ (Letöltés ideje: 2024. február 27.)
- *Global Overview – United States*. 2024.
  Online: https://transparency.fb.com/reports/government-data-requests/country/US/ (Letöltés ideje: 2024. február 27.)
- *Global Overview.* Meta. 2024.
  Online: https://transparency.fb.com/reports/government-data-requests/ (Letöltés ideje: 2024. február 27.)
- *Internet-előfizetések száma hozzáférés szerint, az év végén (1999-2020)*. NMHH EHMMSA. 2021.
  Online: http://ehmmsa.nmhh.hu/informatika-internet/6-02/013,001,002,003,006,008,014,009,007,015,010,a/#6-02 (Letöltés ideje: 2023. július 29.)
- *Internetszolgáltatás, 2023. I. negyedév*. KSH.
  Online: https://www.ksh.hu/infografika/2023/internet_infografika_20231.pdf (Letöltés ideje: 2024. február 24.)
- *Internetszolgáltatás, 2023. III. negyedév*. KSH.
  Online: https://www.ksh.hu/infografika/2023/internet_infografika_20233.pdf (Letöltés ideje: 2024. február 24.)
- *Mobile Messaging Services Market Size & Share | Industry Forecast – 2030*. Global Market Research. 2023.
  Online: https://www.linkedin.com/pulse/mobile-messaging-services-market-size-share-industry-ampfe (Letöltés ideje: 2024. február 26.)

- *Mobile Messaging Services Market Size & Share | Industry Forecast – 2031*. Global Market Research. 2024.
  Online: https://www.businessresearchinsights.com/market-reports/mobile-messaging-services-market-104760 (Letöltés ideje: 2024. február 26.)
- *Mobil rádiótelefon szolgáltatás (1990-2008)*. NMH EHMMSA. 2009. Online: http://ehmmsa.nmhh.hu/mobil-tavkozlesi-szolgaltatas/3-04/001,002,003,004,005,a/#3-04 (Letöltés ideje: 2023. július 29.)
- *Mobil rádiótelefon-hívások jellemzői: Hívások időtartama (1990-2001)*. NMHH: EHMMSA. 2023.
  Online: http://ehmmsa.nmhh.hu/mobil-tavkozlesi-szolgaltatas/3-02/006/#3-02 (Letöltés ideje: 2023. július 29.)
- *Mobiltelefon előfizetések száma*. NMHH.
  Online: http://ehmmsa.nmhh.hu/nemzetkozi-adatok/9-28/021/#9-28 (Letöltés ideje: 2023. július 27.)
- *Távbeszélő központokba bekapcsolt fővonalak száma a központ típusa szerint* (1990-2008). NMHH EHMMSA. 2009.
  Online: http://ehmmsa.nmhh.hu/tavbeszelo-szolgaltatas/2-06/006/#2-06 (Letöltés ideje: 2023. július 29.)
- *Távközlés, internet, 2015. IV. negyedév*. KSH. 2016.
  Online: https://www.ksh.hu/docs/hun/xftp/gyor/tav/tav21412.pdf (Letöltés ideje: 2023. július 29.)
- *Távközlé*s. KSH.
  Online: https://www.ksh.hu/stadat_files/ikt/hu/ikt0003.html (Letöltés ideje: 2023. július 27.)
- *12.1.1.2. A távközlés (vezetékes, mobil) fontosabb adatai.* KSH. 2023.
  Online: https://www.ksh.hu/stadat_files/ikt/hu/ikt0002.html (Letöltés ideje: 2023. július 29.)
- *12.1.1.5. A mobil-előfizetések száma és a mobilhálózatból kiinduló hívások száma és időtartama, adatforgalma*. KSH. 2023.
  Online: https://www.ksh.hu/stadat_files/ikt/hu/ikt0005.html (Letöltés ideje: 2023. július 29.)
- *12.2.1.2. Bekapcsolt vezetékes telefon fővonalak és hívások száma negyedévente*. KSH. 2024.

Online: https://www.ksh.hu/stadat_files/ikt/hu/ikt0030.html (Letöltés ideje: 2024. február 23.)

- *12.2.1.4. Mobil-előfizetések és hívások száma, mobil adatforgalom negyedévente*. KSH. 2024.
  Online: https://www.ksh.hu/stadat_files/ikt/hu/ikt0032.html (Letöltés ideje: 2024. február 23.)

8.2. Jogforrások, nemzetközi szabványok

Hazai jogforrások:

- Magyarország Alaptörvénye (2011. április 25.)
- 1888. évi XXXI. törvénycikk a távírda, a távbeszélő és egyéb villamos berendezésekről
- 1987. évi 12. törvényerejű rendelettel kihirdetett, a szerződések jogáról szóló, Bécsben 1969. évi május hó 23. napján kelt szerződés 2. cikk 1. bekezdés *a)* pontjában
- 1991. évi XVI. törvény a koncesszióról
- 1992. évi. LXXI. törvény a távközlésről (Tt.)
- 1993. évi XXXI. törvény az emberi jogok és az alapvető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt Egyezmény és az ahhoz tartozó nyolc kiegészítő jegyzőkönyv kihirdetéséről
- 1994. évi XXXIV. törvény a rendőrségről (Rtv.)
- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról
- 1995. évi XXVIII. törvény a nemzeti szabványosításról
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről (Ekertv.)
- 2001. évi XL. törvény a hírközlésről
- 2001. évi XL. törvényt a hírközlésről (Hkt.)
- 2002. évi LIV. törvény a bűnüldöző szervek nemzetközi együttműködéséről
- 2003. évi C. törvény az elektronikus hírközlésről (Eht.)
- 2005. évi L. törvény a nemzetközi szerződésekkel kapcsolatos eljárásról
- 2007. évi CLXXIV az elektronikus hírközlésről szóló 2003. évi C. törvény módosításáról

- 2010. évi CIV. törvény a sajtószabadságról és a médiatartalmak alapvető szabályairól (Smtv.)
- 2010. évi CLXXXV. törvény a médiaszolgáltatásokról és a tömegkommunikációról (Mttv.)
- 2010. évi CXXII. törvény a Nemzeti Adó- és Vámhivatalról (NAV tv.)
- 2011. évi CLXIII. törvény az ügyészségről (Ütv.)
- 2011. évi CVII. törvény az egyes elektronikus hírközlési tárgyú törvények módosításáról
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
- 2012. évi CLXXX. törvény az Európai Unió tagállamaival folytatott bűnügyi együttműködésről
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
- 2015. évi CLXXXVIII. törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről
- 2016. évi LXIX. törvény a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról
- 2017. évi C. törvény a büntetőeljárásról (Be.)
- 2017. évi XCIII. törvény a titkos információgyűjtés szabályainak az új büntetőeljárási törvénnyel összefüggő, továbbá a bírósági végrehajtás során a sértettnek megítélt polgári jogi követelések kielégítési sorrendjére vonatkozó rendelkezések módosításáról
- 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről (Kibertan. tv.)
- 75/1998. (IV. 24.) Korm. rendelet a titkos információgyűjtésre felhatalmazott szervezetek együttműködésének rendjéről és szabályairól
- 180/2004. (V.26.) Korm. rendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről
- 293/2010. (XII. 22.) Korm. rendelet a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve kijelöléséről, valamint feladatai ellátásának, a kifogástalan életvitel ellenőrzés és a megbízhatósági vizsgálat részletes szabályainak megállapításáról (NVSZ Korm. rendelet)

- 295/2010. (XII. 22.) Korm. rendelet a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól (TEK Korm. rendelet)
- 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről
- 185/2016. (VII.13.) Korm. rendelet a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről
- 7/2015. (XI. 13.) NMHH rendelet a nemzeti frekvenciafelosztásról, valamint a frekvenciasávok felhasználási szabályairól
- 20/2020. (XII. 18.) NMHH rendelet az elektronikus hírközlési építmények elhelyezéséről és az elektronikus hírközlési építményekkel kapcsolatos hatósági eljárásokról.
- 10/2023. (V. 15.) SZTFH rendelet az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról
- 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
- 2144/2002. (V. 6.) Korm. határozat Magyar Köztársaság nemzeti biztonsági stratégiájáról

AB határozatok, egyéb határozatok, jelentések:

- 13/2001. (V. 14.) AB határozat.
  Online: https://njt.hu/jogszabaly/2001-13-30-75 (Letöltés ideje: 2024. február 14.)
- 2/2007. (I. 24.) sz. AB határozat A Rendőrségről szóló 1994. évi XXXIV. törvény 69. § (3) bekezdése, továbbá a büntetőeljárásról szóló 1998. évi XIX. törvény 201. § (1) bekezdésének b) pontja, c) pontja, d) pontjának "sorozatban vagy szervezett elkövetéssel megvalósuló (ideértve az", továbbá "elkövetést is)" szövegrészei, e) pontja és f) pontja, valamint 2006. június 30-ig hatályban volt 206. § (3) bekezdése, illetve a jövedéki adóról és a jövedéki termék forgalmazásának különös szabályairól szóló 2003. évi CXXVII. törvény 111. § (2) bekezdés g) pontja alkotmányellenességéről. ABH 2007/2, 12-33.

Online:https://net.jogtar.hu/printiframe?docid=A07H0002.AB&targetdate=&printTitle=2/2007.%20%28I.%2024.%29%20AB%20hat%C3%A1rozat&referer=http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid%3DA0300127.TV&getdoc=1 (Letöltés ideje: 2024. február 19.)

- 19/2013. (VII. 19.) AB határozat az egyes törvényeknek a nemzetbiztonsági ellenőrzés új szabályainak megállapítása érdekében szükséges módosításáról szóló 2013. évi LXXII. törvény 9. és 13. §-a hatálybalépésének felfüggesztéséről
- 32/2013. (XI. 22.) AB határozat a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 58. § (3) bekezdésével kapcsolatos alkotmányos követelmény megállapításáról és alkotmányjogi panasz elutasításáról. ABH 2012/23. 1176. Online: http://www.kozlonyok.hu/kozlonyok/Kozlonyok/1/PDF/2013/22.pdf (Letöltés ideje: 2024. február 20.)
- 32/2013. (XI. 22.) AB határozat a Rendőrségről szóló 1994. évi XXXIV. törvény 7/E. § (3) bekezdésével összefüggésben benyújtott alkotmányjogi panaszról. ABH 2013/924.
  Online:https://public.mkab.hu/dev/dontesek.nsf/0/16E8FCEE21074786C1257ADA00524AC5?OpenDocument (Letöltés ideje: 2024. február 15.)
- 32/2021. NVB határozat - a Hajnal Miklós magánszemély által benyújtott országos népszavazási kezdeményezés tárgyában III. fejezet. Online: https://www.valasztas.hu/hatarozat-megjelenito/-/hatarozat/32-2021-nvb-hatarozat-a-hajnal-miklos-maganszemely-altal-benyujtott-orszagos-nepszavazasi-kezdemenyezes-targyaban (Letöltés ideje: 2024. február 18.)
- *A Nemzeti Adatvédelmi és Információszabadság Hatóság hivatalból indított vizsgálatának megállapításai a „Pegasus” kémszoftver Magyarországon történő alkalmazásával összefüggésben (NAIH-423-2/2022.)*. NAIH. 2022.01.31. Online: https://www.naih.hu/adatvedelmi-jelentesek/file/486-jelentes-a-nemzeti-adatvedelmi-es-informacioszabadsag-hatosag-hivatalbol-inditott-vizsgalatanak-megallapitasai-a-pegasus-kemszoftver-magyarorszagon-torteno-alkalmazasaval-osszefuggesben (Letöltés ideje: 2024. február 20.)

Törvényjavaslatok, indokolások:

- T/10307. számú törvényjavaslat a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról, Részletes indokolás a 42-48. §-hoz. Magyarország Kormánya. 2016. április.
  Online: https://www.parlament.hu/irom40/10307/10307.pdf (Letöltés ideje: 2024. január 12.)
- T/48. számú törvényjavaslat egyes törvényeknek a Magyarország minisztériumainak felsorolásáról szóló 2022. évi … törvényhez kapcsolódó módosításáról. Magyarország Kormánya. 2022. május.
  Online: https://www.parlament.hu/irom42/00048/00048.pdf (Letöltés ideje: 2024. február 22.)
- T/5141. számú törvényjavaslat az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről. Magyarország Kormánya. 2001. szeptember.
- T/6064. számú törvényjavaslat az internetes közvetítő szolgáltatások egyes szabályairól. Magyarország Kormánya. 2023. november 24.
  Online: https://www.parlament.hu/irom42/06064/06064.pdf (Letöltés ideje: 2024. február 29.)
- T/6064. számú törvényjavaslat az internetes közvetítő szolgáltatások egyes szabályairól. Magyarország Kormánya. 2023. november 24.
  Online: https://www.parlament.hu/irom42/06064/06064.pdf (Letöltés ideje: 2024. február 18.)
- Végső előterjesztői indokolás a médiaszolgáltatással kapcsolatos egyes törvények módosításáról szóló 2019. évi LXIII. törvényhez. Indokolások tára, Magyar Közlöny Melléklete, 2019. július 9. 110–120.
  Online: https://jogkodex.hu/doc/1631572 (Letöltés ideje: 2024. március 3.)
- Magyarország Alaptörvényének tizenkettedik módosítása indokolás. Magyarország Kormánya. 2023. december 22.
  Online: https://njt.hu/jogszabaly/2023-12-K4-00 (Letöltés ideje: 2024. március 3.)

Nemzetközi jogforrások:

- Európai Unió Alapjogi Chartája (2012/C 326/02)
- Az Európai Parlament és a Tanács (EU) 2016/794 rendelete (2016. május 11.) a Bűnüldözési Együttműködés Európai Uniós Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről, OJ L 135, 24.5.2016, 53–114.
- Az Európai Parlament és a Tanács (EU) 2022/612 rendelete (2022. április 6.) az Unión belüli nyilvános mobilhírközlő hálózatok közötti barangolásról (roaming), OJ L 115, 13.4.2022, 1–37.
- 2/2022. számú a Meta Platforms Ireland Limited (Instagram) ügyében az ír felügyeleti hatóság döntéstervezetéről kialakult vitában az általános adatvédelmi rendelet 65. cikke (1) bekezdésének a) pontja értelmében elfogadott kötelező erejű határozat. EDPB. 2022
- Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR) Adopted on 27 October 2023. EDPB.
  Online: https://edpb.europa.eu/system/files/2023-12/edpb_urgentbindingdecision_202301_no_metaplatformsireland_en_0.pdf (Letöltés ideje: 2024. február 29.)
- Végrehajtási utasítás a Meta Platforms Ireland Limited ügyében az ír adatvédelmi törvény (Data Protection Act) 133. cikk (9) cikk és 133. cikk (10) bekezdései, valamint a GDPR 60. és 66. cikkei alapján. EDPB.
  Online: https://edpb.europa.eu/system/files/2023-12/nationalenforcementnotice202311_ie_metaplatformsireland_en_0.pdf (Letöltés ideje: 2024. február 29.)
- The Foreign Intelligence Surveillance Act (FISA) of 1978. Public law 95-511, 92 Stat. 1783.
  Online: https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf (Letöltés ideje: 2024. február 28.)
- Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008. Public law 110-261, 122 Stat. 2436.

Online: https://www.govinfo.gov/content/pkg/STATUTE-122/pdf/STATUTE-122-Pg2436.pdf (Letöltés ideje: 2024. február 28.)

- Investigatory Powers Act 2016. Online: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted (Letöltés ideje: 2024. február 28.)
- Clarifying Lawful Overseas Use of Data Act (CLOUD Act) March 23, 2018. Public law 115–141, Stat. 1213-25. Online: https://www.govinfo.gov/content/pkg/PLAW-115publ141/pdf/PLAW-115publ141.pdf (Letöltés ideje: 2024. február 28.)
- Lawful Interception – Strengthening EU cooperation. 11517/1/20 (1) 1-2. Brüsszel 2020. Online: https://data.consilium.europa.eu/doc/document/ST-11517-2020-REV-1/en/pdf (Letöltés ideje: 2024. február 28.)
- Javaslat az Európai Parlament és a Tanács rendelete a gyermekek szexuális bántalmazásának megelőzésére és az ellene folytatott küzdelemre vonatkozó szabályok megállapításáról, COM/2022/209 final. Brüsszel. 2022.5.11. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52022PC0209 (Letöltés ideje: 2024. február 27.)
- Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - comments from delegations on Articles 12 to 15 (9068/22, 14143/22). Council Law Enforcement Working Party (Police). 2022. 31-40. Online: https://s3.documentcloud.org/documents/23819681/law-enforcement-working-party-document-encryption.pdf (Letöltés ideje: 2024. február 27.)
- Javaslat az Európai Parlament és a Tanács rendelete a gyermekek szexuális bántalmazásának megelőzésére és az ellene folytatott küzdelemre vonatkozó szabályok megállapításáról, COM/2022/209 final. Brüsszel. 2022.5.11. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52022PC0209 (Letöltés ideje: 2024. február 27.)

- Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - comments from delegations on Articles 12 to 15 (9068/22, 14143/22). Council Law Enforcement Working Party (Police). 2022. 31-40. Online:https://s3.documentcloud.org/documents/23819681/law-enforcement-working-party-document-encryption.pdf (Letöltés ideje: 2024. február 27.)
- Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR) Adopted on 27 October 2023. EDPB. 2023. Online: https://edpb.europa.eu/system/files/2023-12/edpb_urgentbindingdecision_202301_no_metaplatformsireland_en_0.pdf (Letöltés ideje: 2024. február 27.)
- Végrehajtási utasítás a Meta Platforms Ireland Limited ügyében az ír adatvédelmi törvény (Data Protection Act) 133. cikk (9) cikk és 133. cikk (10) bekezdései, valamint a GDPR 60. és 66. cikkei alapján. EDPB. 2023. Online: https://edpb.europa.eu/system/files/2023-12/nationalenforcementnotice202311_ie_metaplatformsireland_en_0.pdf (Letöltés ideje: 2024. február 27.)
- C-311/18. számú, Data Protection Commissioner kontra Facebook Ireland és Maximillian Schrems ügyben az Európai Unió Bírósága 2020. július 16-án hozott ítélete [ECLI:EU:C:2020:559] Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:62018CJ0311&from=EN (Letöltés ideje: 2024. február 27.)
- 14086 of October 7, 2022, on Enhancing Safeguards for United States Signals Intelligence Activities.
- Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (notified under document C(2023)4745), OJ L 231, 20.9.2023, 118–229.

- 5/2023.sz. vélemény a személyes adatoknak az EU–USA adatvédelmi keret szerinti megfelelő védelméről szóló európai bizottsági végrehajtási határozat tervezetéről. EDPB. 2023.
  Online: https://edpb.europa.eu/system/files/2023-09/edpb_opinion52023_eu-us_dpf_hu.pdf (Letöltés ideje: 2024. február 27.)
- 2/2022. számú a Meta Platforms Ireland Limited (Instagram) ügyében az ír felügyeleti hatóság döntéstervezetéről kialakult vitában az általános adatvédelmi rendelet 65. cikke (1) bekezdésének a) pontja értelmében elfogadott kötelező erejű határozat. EDPB. 2022.
- 5/2023.sz. vélemény a személyes adatoknak az EU–USA adatvédelmi keret szerinti megfelelő védelméről szóló európai bizottsági végrehajtási határozat tervezetéről. EDPB. 2023.
  Online: https://edpb.europa.eu/system/files/2023-09/edpb_opinion52023_eu-us_dpf_hu.pdf (Letöltés ideje: 2024. február 27.)
- A Meta Platforms Ireland Limited (Instagram) ügyében az ír felügyeleti hatóság döntéstervezetéről kialakult vitában az általános adatvédelmi rendelet 65. cikke (1) bekezdésének a) pontja értelmében elfogadott 2/2022. sz. kötelező erejű határozat. EDPB. 2022
- *British-US Communication Intelligence Agreement*. The National Archives: Catalogue Reference: HW/80/4.
  Online: https://discovery.nationalarchives.gov.uk/details/r/C11536914 (Letöltés ideje: 2023. július 26.)
- Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról. L 105/54 13.4.2006
- C/2023/1092 a Bizottság határozatának összefoglalója (2023. szeptember 5.) az (EU) 2022/1925 rendelet 3. cikke szerinti határozatról (Ügyek DMA.100020 – Meta – online social networking services; DMA.100024 – Meta – Number-independent interpersonal communications services; DMA.100035 – Meta – Online advertising services; DMA.100044 – Meta – Online intermediation services – Marketplace).

Online:https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:C_202301092 (Letöltés ideje: 2024. február 19.)

- Commission Decision of 5.9.2023 designating Apple as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector, DMA.100020 Meta - online social networking services, DMA.100013 Apple – online intermediation services – app stores, DMA.100025 Apple – operating systems és DMA.100027 Apple – web browser. Brussels, 5.9.2023, C(2023) 6100 final.
  Online:https://ec.europa.eu/competition/digital_markets_act/cases/202344/DMA_100027_197.pdf
- A Bizottság határozatának összefoglalója (2023. szeptember 5.) az Apple-nek a digitális ágazat vonatkozásában a versengő és tisztességes piacokról szóló (EU) 2022/1925 európai parlamenti és tanácsi rendelet 3. cikke értelmében történő kapuőrré minősítéséről (DMA.100013 Apple – online intermediation services – app stores, DMA.100025 Apple – operating systems és DMA.100027 Apple – web browsers)
  Online:https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:C_202300548 (Letöltés ideje: 2024. február 19.)
- Az Európai Parlament és a Tanács (EU) 2018/1808 irányelve (2018. november 14.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról szóló 2010/13/EU irányelvnek (Audiovizuális médiaszolgáltatásokról szóló irányelv) a változó piaci körülményekre tekintettel való módosításáról. HL L 303, 2018. november 28. 69–92. (AVMS)
- Az Európai Parlament és a Tanács (EU) 2015/1535 irányelve (2015. szeptember 9.) a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról. HL L 241., 2015.9.17. 1-15.
- 37138/14. sz. EJEB ítélet, 2016. január 2-án: Szabó és Vissy kontra Magyarország. Online: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]} (Letöltés ideje: 2024. február 20.)

- Az Európai Parlament és a Tanács 2014/41/EU irányelve (2014. április 3.) a büntetőügyekben kibocsátott európai nyomozási határozatról. OJ L 130, 1.5.2014, 1–36. (ENYH irányelv)
- A Tanács 2006/960/IB kerethatározata (2006. december 18.) az Európai Unió tagállamainak bűnüldöző hatóságai közötti, információ és bűnüldözési operatív információ cseréjének leegyszerűsítéséről. OJ L 386, 29.12.2006, 89–100.
- Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet) OJ L 277, 27.10.2022, 1–102. (DSA)
- Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály) OJ L 265, 12.10.2022, 1–66. (DMA)
- *BEREC report on interoperability of NumberIndependent Interpersonal Communication Services (NI-ICS)*. BEREC, BoR (23) 92. 2023. Online: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-interoperability-of-number-independent-interpersonal-communication-services-ni-ics (Letöltés ideje: 2024. február 17.)
- Commission Decision of 5.9.2023 designating Meta as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector, DMA.100020 Meta - online social networking services, DMA.100024 Meta - number-independent interpersonal communications services, DMA.100035 Meta - online advertising services, DMA.100044 Meta - online intermediation services – marketplace. Brussels, 5.9.2023, C(2023) 6105 final.
  Online:https://ec.europa.eu/competition/digital_markets_act/cases/202346/DMA_100024_206.pdf (Letöltés ideje: 2024. február 19.)
- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv). OJ L 333, 27.12.2022, 80–152.

- A Bizottság (EU) 2024/482 végrehajtási rendelete (2024. január 31.) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról. OJ L, 2024/482, 2024.07.02.
- The European Parliament, the Council and the Commission solemnly proclaim the following joint Declaration on Digital Rights and Principles for the Digital Decade. 15 December 2022. OJ C 23, 23.1.2023, 1–7.
- A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Európai digitális egységes piaci stratégia, COM(2015) 192 final. (Európai adatstratégia)
  Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52020DC0066 (Letöltés ideje: 2024. február 14.)
- Az Európai Parlament és a Tanács (EU) 2018/1972 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáró. OJ L 321, 17.12.2018, 36–214.
- Lisszaboni Szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról, OJ C 306, 17.12.2007, 1–271. o.
- Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 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 (bűnügyi irányelv), OJ L 119, 4.5.2016, 89–131.
- C-207/16 számú Ministerio Fiscal ügyben az Európai Unió Bírósága 2018. október 2-ián hozott ítélete [ECLI:EU:C:2018:788]; C-623/17 számú Privacy International ügyben az Európai Unió Bírósága által 2020. október 6-án hozott ítélete [ECLI:EU:C:2020:790[; C-511/18, C-512/18 és C-520/18. számú La Quadrature du Net és társai ügyében az Európai Unió Bírásaga által hozott ítélet [ECLI:EU:C:2020:79]
- Javaslat az Európai Parlament és a Tanács rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a

2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet), COM/2017/010 final - 2017/03 (COD).

- Az Európai Unió Alapjogi Chartája (2012/C 326/02) OJ C 326, 26.10.2012, 391–407. (Charta)
- C-140/20. számú Commissioner of An Garda Síochána ügyben az Európai Unió Bírósága 2022. április 5-én hozott ítélete [ECLI:EU:C:2022:258]
- Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata, OJ C 202, 7.6. 2016, 1–388. (EUSZ, EUMSZ)
- Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, OJ L 281, 23/11/1995, 0031 – 0050.
- Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv), OJ L 201, 31/07/2002, 0037 – 0047. (e-hírközlési irányelv)
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), OJ L 119, 4.5.2016, 1–88. (GDPR)
- Decision (EU) 2022/2481 of The European Parliament And of The Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance).
  Online: https://eur-lex.europa.eu/eli/dec/2022/2481/oj (Letöltés ideje: 2023. július 9.)
- Lawful Interception – Strengthening EU cooperation (Brussels, 5 November 2020), 11517/1/20 REV 1.
  Online: https://data.consilium.europa.eu/doc/document/ST-11517-2020-REV-1/en/pdf (Letöltés ideje: 2023. július 9.)
- Proposal for a Regulation of The European Parliament and of The Council laying down rules to prevent and combat child sexual abuse COM/2022/209 final (Brussels, 11.5.2022).

Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN (Letöltés ideje: 2023. július 9.)

- Written comments submitted by Member States Proposal for a Regulation laying down rules to prevent and combat child sexual abuse (9068/22) (Brussels, 12.4.2023) WK 10235/2022 ADD 10 REV 2.
  Online: https://www.documentcloud.org/documents/23819681-law-enforcement-working-party-document-encryption (Letöltés ideje: 2023. július 9.)
- 2/13. sz. EUB vélemény [ECLI:EU:C:2014:2454.]

Nemzetközi szabványok:

- Y.2770: Requirements for deep packet inspection in next generation networks. Online: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2770-201211-I!!PDF-E&type=items (Letöltés ideje: 2024. február 15.)
- 3GPP TR 33.908 - 3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms
- 3GPP TS 55.216 - Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS
- 3GPP TS 35.202. - Key Allocation and Stream ciphering UMTS Interface
- NIST Special Publication 800-38B (2005
- 3GPP TS 35.205 - 3G Security: Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*.
- 3GPP TS 35.215 - SNOW 3G
- 3GPP TS 35.221 – ZUC: Zu Chongzhi stream Chiper
- 3GPP TS 33.501 version 17.5.0 Release 17
- ETSI TS 133 501 V17.5.0 (2022-05.)
- 3GPP TS 33.535. - Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)
- 3GPP TS 05.08. - Radio subsystem link control
- 3GPP TS 33.126 - Lawful Interception requirements

- ETSI 133.127 - LTE; 5G; Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Lawful Interception (LI) architecture and functions (3GPP TS 33.127 version 16.5.0 Release 16)
- 3GPP TS 33.128 - Security; Protocol and procedures for Lawful Interception (LI)
- RFC-TLS13-28: TLS 1.3
- U.S. FIPS PUB 197 (FIPS 197): AES - Advanced Encryption Standard
- *ISO 15489-1:2016 Information and documentation — Records management*. International Organization for Standardization. 3.12. Online: https://www.iso.org/obp/ui/#iso:std:iso:15489:-1:ed-2:v1:en (Letöltés ideje: 2024. február 19.)
- ISO/IEC DIR 2:2016 - Principles and rules for the structure and drafting of ISO and IEC documents.
  Online: https://www.iec.ch/members_experts/refdocs/iec/isoiecdir-2%7Bed7.0%7Den.pdf (Letöltés ideje: 2024. július 7.)

8.3. Internetes hivatkozások

- *„Elsőnek lenni dicsőség, elsőnek lenni felelősség”*. Magyarország Kormánya. 2021. Online: https://kormany.hu/hirek/elsonek-lenni-dicsoseg-elsonek-lenni-felelosseg (Letöltés ideje: 2024. február 25.)
- *4 arrested in takedown of dark web child abuse platform with some half a million users*. Europol.
  Online: https://www.europol.europa.eu/media-press/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users (Letöltés ideje: 2024. február 27.)
- *4 arrested in takedown of dark web child abuse platform with some half a million users*. Europol.
  Online: https://www.europol.europa.eu/media-press/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users (Letöltés ideje: 2024. február 27.)

- *5G hálózati szeletelés optimalizációja megerősítéses tanulás segítségével*. BME VIK. Online: https://www.hit.bme.hu/edu/project/data?id=20448 (Letöltés ideje: 2024. február 22.)
- *800 criminals arrested in biggest ever law enforcement operation against encrypted communication.* Europol. 2021. Online: https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication (Letöltés ideje: 2024. február 15.)
- *A 4G hálózat adat mellett már a hangunkat is viszi – Elindítja a 4G Hangot a Magyar Telekom.* Magyar Telekom. 2017. Online: www.telekom.hu/rolunk/sajtoszoba/sajtokozlemenyek/2017/aprilis_27 (Letöltés ideje: 2023. december 19.)
- *A Bizottság az EU-n belül mindenkire érvényes digitális jogokról és elvekről szóló nyilatkozatot terjeszt elő.* Európai Bizottság. 2022. Online: https://ec.europa.eu/commission/presscorner/detail/hu/IP_22_452 (Letöltés ideje: 2024. február 29.)
- *A gigabites infrastruktúráról szóló jogszabály: a Tanács és a Parlament megállapodott a nagy sebességű hálózatok EU-szerte történő gyorsabb kiépítéséről*. EU Tanácsa. 2024. február 06. Online: https://www.consilium.europa.eu/hu/press/press-releases/2024/02/06/gigabit-infrastructure-act-council-and-parliament-strike-a-deal-for-faster-deployment-of-high-speed-networks-in-the-eu/ (Letöltés ideje: 2024. február 14.)
- *A jövő lehetősége az 5G*. DJP. 2019. Online: https://digitalisjoletprogram.hu/hu/hirek/a-jovo-lehetosege-az-5g (Letöltés ideje: 2024. február 21.)
- AGAOUA Djamel (2020): *Viber is 10*! Rakuten Viber. Online: https://www.viber.com/en/blog/2020-12-02/viber-is-10/ (Letöltés ideje: 2023. november 13.)
- ALWEN, Joël (2020): *End-to-End Encryption vs. Client-to-Server Encryption*. Wickr. Online: https://wickr.com/end-to-end-encryption-vs-client-to-server-encryption/ (Letöltés ideje: 2024. február 18.)
- *Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms.* NIST. 2022.

Online: https://csrc.nist.gov/News/2016/Public-Key-Post-Quantum-Cryptographic-Algorithms (Letöltés ideje: 2024. február 16.)

- *Apple Platform Security*. Apple. 2022. Online: https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf (Letöltés ideje: 2023. április 11.)
- *Az uniós kiberbiztonsági tanúsítási keret*. Európai Bizottság. Online: https://digital-strategy.ec.europa.eu/hu/policies/cybersecurity-certification-framework (Letöltés ideje: 2024. február 17.)
- BENE ZOLTÁNNÉ PUSZTAI Virág: *Médiaelmélet.* Online: www.jgypk.hu/mentorhalo/tananyag/MediaelmeletV2/index.html (Letöltés ideje: 2023. december 19.)
- BERTA Sándor (2006): *Online házkutatásokat indítanának Németországban*. SG.hu Online:http://sg.hu/cikkek/49079/online_hazkutatasokat_inditananak_nemetorszagban (Letöltés ideje: 2024. február 15.);
- BERTA Sándor (2016): *Német-francia javaslat az üzenetküldő programok lehallgatására*. Sg.hu. Online: https://sg.hu/cikkek/it-tech/120885/nemet-francia-javaslat-az-uzenetkuldo-programoklehallgatasara (Letöltés ideje: 2024. február 28.)
- BEST, Shivali (2022): *Mark Zuckerberg takes a dig at Apple: Meta CEO says WhatsApp is 'far more private and secure' than iMessage.* DalyMail. Online: https://www.dailymail.co.uk/sciencetech/article-11327023/Mark-Zuckerberg-says-WhatsApp-far-private-secure-iMessage.html (Letöltés ideje: 2023. november 13.)
- BLANCHE, Ed (2017): *The Arab Weekly*. UPI. Online: https://www.upi.com/Top_News/Voices/2017/03/20/Islamic-States-killing-machine-focused-on-sleeper-cells/6291490033456/ (Letöltés ideje: 2023. december 8.)
- BRAUN, Stephen - FLAHERTY, Anne – GILLUM, Jack – APUZZO, Matt (2013): *Secret To Prism Program: Even Bigger Data Seizure.* AP. Online: https://web.archive.org/web/20130910083307/http://bigstory.ap.org/article/secret-prism-success-even-bigger-data-seizure (Letöltés ideje: 2024. február 28.)
- CALDWELL Serenity (2011): *Up close with iOS 5: iMessage*. Mac World. Online: https://www.macworld.com/article/214747/ios-5-imessage.html (Letöltés ideje: 2023. november 13.)

- CALDWELL, Serenity (2011): *Up close with iOS 5: iMessage*. Mac World. Online: https://www.macworld.com/article/214747/ios-5-imessage.html (Letöltés ideje: 2023. november 13.)
- CAMPBELL, Scott (2016): *ISIS warn London 'next to be attacked' as UK churches put on terror alert after French priest murder*. Daily Mirror. Online: https://www.mirror.co.uk/news/world-news/isis-warn-london-next-attacked-8500399 (Letöltés ideje: 2023. július 8.)
- ÇEKINMEZ, Fethi (2023): *Radio Access Network (RAN)*. Medium. Online: https://medium.com/@fthcknmz/radio-access-network-ran-1fb033b708f1 (Letöltés ideje: 2024. február 23.)
- CHAFFEY, Dave (2023): *Global social media statistics research summary 2023*. Smart Insights.
  Online: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/ (Letöltés ideje: 2023. március 24.)
- *Commission puts forward declaration on digital rights and principles for everyone in the* EU. Europea, Commission. 2022.
  Online: https://ec.europa.eu/commission/presscorner/detail/hu/IP_22_452 (Letöltés ideje: 2023. július 9.)
- *Connecting Police For a Safer World*. Interpol. Online: https://www.interpol.int/content/download/624/file/GI-01_2020-01_EN_LR.pdf (Letöltés ideje: 2024. február 28.)
- CONSTINE, Josh (2014): *Facebook Is Forcing All Users To Download Messenger By Ripping Chat Out Of Its Main Apps*. TechCrunch.
  Online: https://techcrunch.com/2014/04/09/facebook-messenger-or-the-highway/ (Letöltés ideje: 2023. november 13.)
- CRISAN, Loredana (2023): *Launching Default End-to-End Encryption on Messenger*. Meta.
  Online: https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/ (Letöltés ideje: 2024. február 26.)
- CURRY, David (2023): *Messaging App Revenue and Usage Statistics (2023)*. Business of Apps.
  Online: https://www.businessofapps.com/data/messaging-app-market/ (Letöltés ideje: 2023. november 18.)

- CURRY, David (2024a): *Messaging App Revenue and Usage Statistics (2024)*. BusinessofApps.
  Online: https://www.businessofapps.com/data/messaging-app-market/# (Letöltés ideje: 2024. február 26.)
- CURRY, David (2024b): *Signal Revenue & Usage Statistics (2024)*. BusinessofApps. Online: https://www.businessofapps.com/data/signal-statistics/ (Letöltés ideje: 2024. február 26.)
- DAJKÓ Pál (2011): *Lebukott az állami kémprogram*. ITCoffe.hu. Online: http://itcafe.hu/hir/chaos_computer_club_nemetorszag_bundestrojaner.html (Letöltés ideje: 2024. február 15.)
- DALY, Andrew (2022): T*he Digital Markets Act proposes messaginginteroperability, but this is easier said than done*. Analysys Mason. Online:https://www.analysysmason.com/contentassets/dbe8d6f83e7f4b9489b3783601ee6d45/analysys_mason_dma_messaging_interoperability_apr2022.pdf (Letöltés ideje: 2024. február 17.)
- DANIEL, Ch (2023a): *iMessage Revenue and Growth Statistics (2023).* SignHouse. Online: https://www.usesignhouse.com/blog/imessage-stats (Letöltés ideje: 2023. november 18.)
- DANIEL, Ch (2023b): *Viber Revenue and Growth Statistics (2023).* SignHouse. Online: https://www.usesignhouse.com/blog/viber-stats Letöltés ideje: 2023. november 18.)
- DE, Rajesh – CHRISTIAN, Marcus A. – KOURINIAN, Arsen at al. (2022): *President Biden Signs Executive Order on U.S. Intelligence Activities to Implement EU-U.S. Data Privacy Framework*. MayerBrown.
  Online: https://www.mayerbrown.com/en/perspectives-events/publications/2022/10/president-biden-signs-executive-order-on-us-intelligence-activities-to-implement-eu-us-data-privacy-framework (Letöltés ideje: 2024. február 27.)
- *Déclaration sur les droits et principes numériques: les valeurs et les citoyens de l'UE au cœur de la transition numérique*. Conseil de l'UE. 2022. Online: https://www.consilium.europa.eu/fr/press/press-releases/2022/12/15/declaration-on-digital-rights-and-principles-eu-values-and-citizens-at-the-centre-of-digital-transformation/ (Letöltés ideje: 2024. február 19.)

- *Digital Single Market: EU negotiators reach a political agreement to update the EU's telecoms rules*. Európai Bizottság. 2018.
  Online: https://ec.europa.eu/commission/presscorner/detail/hu/IP_18_4070 (Letöltés ideje: 2024. február 17.)
- *Digital Single Market: Political agreement on the rules shaping the telecommunication markets in the 5G era*. European Commission. 2018. Online:https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_18_4084/MEMO_18_4084_EN.pdf (Letöltés ideje: 2024. február 18.)
- DÖMÖS Zsuzsanna (2022): *Megvan, mikor végez a Telekom a 3G kivezetésével*. HWSW. Online: https://www.hwsw.hu/hirek/64508/magyartelekom-3g-halozat-lekapcsolas-datum.html (Letöltés ideje: 2024. február 21.)
- DR. BENCSIK Balázs (2023): *Az SZTFH szerepe a kiberbiztonságban*. SZTFH. Online:https://www.fogalomtar.hte.hu/documents/10180/4737479/C_3_Dr_Bencsik_Balazs_Szabalyozott_Tevekenysegek_Felugyeleti_Hatosag_szerepe_a_kiberbiztonsagban.pdf (Letöltés ideje: 2024. február 17.)
- DR. GYÖMBÉR Béla (2022): *Poszt-kvantumtitkosítást vezetnek be Magyarországon*; Jogalap.
  Online: https://jogalappal.hu/poszt-kvantumtitkositast-vezetnek-be-magyarorszagon/ (Letöltés ideje: 2024. február 16.)
- DR. IFJ. LOMNICI Zoltán (2024): K*ormányzati szivárogtatások és következményeik az Egyesült Államokban*. AlaptörvényBlog.
  Online:https://alaptorvenyblog.hu/kormanyzati_szivarogtatasok_es_kovetkezmenyeik_az_egyesult_allamokban.html Letöltés ideje: 2024. július 7.)
- DR. SONNEVEND-VALLE Anna (2023): *NIS 2 és a GDPR – A kiberbiztonsági és az adatvédelmi előírások összefüggései.* Jogi Fórum. Online: https://www.jogiforum.hu/hir/2023/09/04/nis-2-es-a-gdpr-a-kiberbiztonsagi-es-az-adatvedelmi-eloirasok-osszefuggesei/ (Letöltés ideje: 2024. február 17.)
- DR. SZALAI Anita (2023): *Már hatályos a DSA, a digitális szolgáltatásokról szóló rendelet*. SzalaiLegal.
  Online: https://www.szalailegal.hu/mar-hatalyos-a-dsa-a-digitalis-szolgaltatasokrol-szolo-rendelet/ (Letöltés ideje: 2024. február 17.)

- E*gyre jobban terjed az internethasználat hazánkban*. KSH. 2021. Online: https://www.ksh.hu/infografika/2021/internethasznalat_2021.pdf (Letöltés ideje: 2023. július 29.)
- *Ericsson Mobility Report*. Ericcson. 2023. Online: https://www.ericsson.com/4ae12c/assets/local/reports-papers/mobility-report/documents/2023/ericsson-mobility-report-november-2023.pdf (Letöltés ideje: 2024. február 23.)
- *Ericsson Mobility Report.* Ericsson. 2022. Online: https://www.ericsson.com/4ae28d/assets/local/reports-papers/mobility-report/documents/2022/ericsson-mobility-report-november-2022.pdf (Letöltés ideje: 2024. november 2.)
- *EU Elektronikus Hírközlési Kódex. Európai Bizottság*. 2020. Online: https://digital-strategy.ec.europa.eu/hu/policies/eu-electronic-communications-code (Letöltés ideje: 2024. február 18.)
- *European Union Serious and Organised Crime Threat Assessment* (SOCTA) 2021. Europol, 32. Online:https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf (Letöltés ideje: 2023. július 8.)
- *EVE Explains: 5G and Lawful Interception*. Hága: EVE. Online: https://www.lawfulinterception.com/explains/5g-and-lawful-interception/ (Letöltés ideje: 2024. február 23.)
- *Façonner l'avenir numérique de l'Europe - Conclusions du Conseil* (9 juin 2020) Bruxelles. 2020. Online: https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/fr/pdf (Letöltés ideje: 2024. február 18.)
- *FBI Targets Encrypted Platforms Used by Criminal Groups - Global partners announce results of innovative Operation Trojan Shield.* FBI. 2021. Online: https://www.fbi.gov/news/stories/fbi-global-partners-announce-results-of-operation-trojan-shield-060821 (Letöltés ideje: 2024. február 15.)
- *FBI Targets Encrypted Platforms Used by Criminal Groups - Global partners announce results of innovative Operation Trojan Shield.* FBI. 2021. Online: https://www.fbi.gov/news/stories/fbi-global-partners-announce-results-of-operation-trojan-shield-060821 (Letöltés ideje: 2024. február 15.)

- *FBI Targets Encrypted Platforms Used by Criminal Groups - Global partners announce results of innovative Operation Trojan Shield.* FBI. 2021.*; 800 criminals arrested in biggest ever law enforcement operation against encrypted communication.* Europol. 2021.
  Online: https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication (Letöltés ideje: 2024. február 15.)
- *FBI-EUROPOL-KR NNI – ANOM adatok alapján számolták fel a hálózatot*. Police.hu. Online: https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/fbi-europol-kr-nni-anom-adatok-alapjan-szamoltak (Letöltés ideje: 2024. február 15.)
- *FBI-EUROPOL-KR NNI – ANOM adatok alapján számolták fel a hálózatot*. Police.hu. Online: https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/fbi-europol-kr-nni-anom-adatok-alapjan-szamoltak (Letöltés ideje: 2024. február 15.)
- FEKŐ Ádám (2024): *Rekordszámú személyes adatot kért ki a magyar kormány a Facebook felhasználóiról*. Media1.
  Online: https://media1.hu/2024/01/09/rekordszamu-szemelyes-adatot-kert-ki-a-magyar-kormany-a-facebook-felhasznaloirol/ (Letöltés ideje: 2024. február 27.)
- FLACHNER Balázs (2023): *Tényleg itt a minden titkosítást feltörő kvantumszámítógép?*. Telex.
  Online: https://telex.hu/tudomany/2023/02/11/kvantumtechnologia-kvantumszamitogep-rsa-eljaras-titkositas-kriptografia (Letöltés ideje: 2024. február 18.)
- *Gazdasági és társadalmi változások az 1990-es években és a 2000-es évek első felében*. NKP.
  Online: https://okostankonyv.nkp.uni-eszterhazy.hu/tankonyv/tortenelem_12/lecke_05_035 (Letöltés ideje: 2023. július 27.)
- *Global ICT market share 2013-2022, by selected country*. Statista Research Department. 2023.
  Online: https://www.statista.com/statistics/263801/global-market-share-held-by-selected-countries-in-the-ict-market/ (Letöltés ideje: 2023. november 2.)

- *Global ICT market share 2013-2022, by selected country*. Statista Research Department. 2023.
  Online: https://www.statista.com/statistics/263801/global-market-share-held-by-selected-countries-in-the-ict-market/ (Letöltés ideje: 2023. július 8.)
- GOLOVANOV, Sergey (2013): *Spyware. HackingTeam*. SecureList.
  Online: http://securelist.com/analysis/publications/37064/spyware-hackingteam (Letöltés ideje: 2024. február 15.)
- GOODIN, Dan (2023): *Messenger billed as better than Signal is riddled with vulnerabilities*. ArsTechnica.
  Online: https://arstechnica.com/information-technology/2023/01/messenger-billed-as-better-than-signal-is-riddled-with-vulnerabilities/ (Letöltés ideje: 2023. április 8.)
- HADDAD, Margot - HUME, Tim (2016): *Killers of French priest met 4 days before attack.* CNN.
  Online: http://edition.cnn.com/2016/08/01/europe/france-church-attack-telegram/index.html (Letöltés ideje: 2023. december 8.)
- HARDWICK, Tim (2024): *iOS 17.4 to Add This 'Groundbreaking' New Messaging Feature*. MacRumors. Online: https://www.macrumors.com/2024/02/23/ios-17-4-adds-groundbreaking-imessage-feature/ (Letöltés ideje: 2024. február 28.)
- HASSAN, Mohammad (2022): *Az IoT-felhő: Microsoft Azure vs. AWS vs. Google Cloud.* IoT Analtics.
  Online: https://iot-analytics.com/iot-cloud/ (Letöltés ideje: 2024. február 23.)
- *Havonta 20 személy titkos megfigyelésére adtak bírói engedélyt idén*. HVG.hu. 2023.
  Online:https://hvg.hu/itthon/20230613_Havonta_20_szemely_titkos_megfigyelesre_adtak_biroi_engedelyt_iden (Leöltési ideje: 2024. február 18.)
- HORTEN, Monica (2012): *The ITU's DPI standard - that's something to be afraid of!* IPTegrity.
  Online: https://www.iptegrity.com/index.php/telecoms-package/net-neutrality/827-the-itus-dpi-standard-thats-something-to-be-afraid-of (Letöltés ideje: 2024. február 15.)
- HURST, Luke (2023): *How will 6G change the world? This is what experts at Mobile World Congress think*. Euronews.next.
  Online: https://www.euronews.com/next/2023/02/28/how-will-6g-change-the-world-this-is-what-experts-at-mobile-world-congress-think (Letöltés ideje: 2024. február 22.)

- *ICT (Global Market).* TAdviser. 2023.
  Online: https://tadviser.com/index.php/Article:ICT_(Global_Market) (Letöltés ideje: 2023. november 2.)
- *Idén tavaszig már 440 titkos megfigyelési igény került Varga Judit elé, de már azt is titkosították, hogy ebből hányat engedélyeztek* HVG.hu. 2023. Online:https://hvg.hu/itthon/20230604_Titkos_megfigyelesek_Varga_Judit_titkositas_nemzetbiztonsag_igazsagugyi_miniszterium_engedely (Leöltési ideje: 2024. február 18.)
- *Infokommunikációs És Információtechnológiai Nemzeti Laboratórium (InfoLab).*
- *Interdiszciplináris "űrképzés" indul 17 hazai egyetem együttműködésében*. NKE. 2021.
  Online: https://vtkm.uni-nke.hu/hirek/2021/12/19/interdiszciplinaris-urkepzes-indul-17-hazai-egyetem-egyuttmukodeseben (Letöltés ideje: 2024. február 25.)
- *Irányelv az egész Unióban egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS2 irányelv).* Európai Bizottság.
  Online: https://digital-strategy.ec.europa.eu/hu/policies/nis2-directive (Letöltés ideje: 2024. február 17.)
- JACKIEWICZ, Magdalena (2023): *Chat app development trends that will shape the industry in 2023.* RST.
  Online: https://www.rst.software/blog/chat-app-development-trends-that-will-shape-the-industry-in-2023 (Letöltés ideje: 2023. március 25.)
- JAIN, Puneet (2023): Rel-18 Status and Rel-19 Progress in TSG SA. *Highlights*, 3(7), 4-5.
  Online: https://www.3gpp.org/newsletter-issue-07-nov-2023 (Letöltés ideje: 2024. február 21.)
- JELINEK Anna (2024): *Rekordszámú személyes adatot kért ki a magyar kormány a Facebooktól*. 444.
  Online: https://444.hu/2024/01/09/rekordszamu-szemelyes-adatot-kert-ki-a-magyar-kormany-a-facebooktol (Letöltés ideje: 2024. február 27.)
- *Közlekedési, Távközlési és Energiaügyi Tanács, 2015.6.11–12*. Európai Unió Tanácsa. 2015.
  Online: https://www.consilium.europa.eu/hu/meetings/tte/2015/06/11-12/ Letöltés ideje: 2024. február 17.)

- LAI, Richard (2010): *3G GSM encryption cracked in less than two hours*. Engadget. Online: https://www.engadget.com/2010-01-15-3g-gsm-encryption-cracked-in-less-than-two-hours.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAALBTMnOk12PZGvXoKxD4BbP5rBK7GxrdAmBAQrudtQ4QvbrqmrWwrDcDZj4CIhtgHQSCD2nU0Ih8i4IXPaUN7745YYiIi6y4Op5jE0myIJgMUkygjkbGuM9xfN2BRL2GLriURK5d3g-Yz5YScK20sxevexbdmmzhLJAAad0aLErc (Letöltés ideje: 2024. április 1.)
- *Lawful Intercept Standards.* National Domestic Communications Assistance Center. Online: https://ndcac.fbi.gov/calea/lawful-intercept-standards (Letöltés ideje: 2023. július 31.)
- LIAO, Shannon (2019): *Over 300 million Chinese private messages were left exposed online*. The Verge. Online: https://www.theverge.com/2019/3/4/18250474/chinese-messages-millions-wechat-qq-yy-data-breach-police (Letöltés ideje: 2024. február 19.)
- LONG, Heinrich (2023): *Signal Review 2023: Secure Messenger (Pros and Cons)*. Restore Privacy. Online: https://restoreprivacy.com/secure-encrypted-messaging-apps/signal/ (Letöltés ideje: 2023. november 12.)
- LONG, Heinrich (2023): *Telegram Review 2023: NOT as Private as You Think*. Restore Privacy. Online: https://restoreprivacy.com/secure-encrypted-messaging-apps/telegram/ (Letöltés ideje: 2023. november 15.)
- LUTKEVICH, Ben – BACON, Madelyn (2021): End-to-End Encryption (E2EE). TechTarget. Online: https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE (Letöltés ideje: 2024. február 20.)
- MARCH, Liz (2023): *Most Popular Messaging Apps Worldwide 2023*. SimilarWeb. Online: https://www.similarweb.com/blog/research/market-research/worldwide-messaging-apps/ (Letöltés ideje: 2024. február 26.)
- *Messenger Súgóközpont*. Meta. 2024. Online: https://www.facebook.com/help/messenger-app/1084673321594605 (Letöltés ideje: 2024. február 27.)

- *Mesterséges Intelligencia Nemzeti Laboratórium (MiLab)*. Online: https://mi.nemzetilabor.hu/hu/partnerek/nemzetbiztonsagi-szakszolgalat (Letöltés ideje: 2023. november 08.)
- *Metaverzum*. Lexiq.hu. Online: https://lexiq.hu/metaverzum (Letöltés ideje: 2024. június 22.)
- MIHINDUKULASURIYA, Regina (2019): *Rape videos, child porn, terror — Telegram anonymity is giving criminals a free run - The end-to-end encryption provided by social media app Telegram has paved the way for a host of illegal activities*. The Print. Online: https://theprint.in/tech/rape-videos-child-porn-terror-telegram-anonymity-is-giving-criminals-a-free-run/307959/ (Letöltés ideje: 2023. december 26.)
- MORA, Justino (2017): *Demystifying the Signal Protocol for End-to-End Encryption (E2EE)*. Medium. Online: https://medium.com/@justinomora/demystifying-the-signal-protocol-for-end-to-end-encryption-e2ee-ad6a567e6cb4 (Letöltés ideje: 2023. november 12.)
- MOXIE, Marlinspike (2016): *Signal on the outside, Signal on the inside*. Signal Online: https://signal.org/blog/signal-inside-and-out/ (Letöltés ideje: 2023. április 10.)
- *MTProto Mobile Protocol*. Telegram. Online: https://core.telegram.org/mtproto (Letöltés ideje: 2023. november 15.)
- MU-HYUN, Cho (2020): *Samsung expects 6G to launch as early as 2028*. ZDNET. Online: https://www.zdnet.com/article/samsung-expects-6g-to-launch-as-early-as-2028/ (Letöltés ideje: 2024. február 22.)
- *NAIH: a Nemzetbiztonsági Szakszolgálat alkotmányos módon működik*. NBSZ. 2017. Online: https://nbsz.gov.hu/tevekenyseg-mukodes/kulso-vizsgalatok-ellenorzesek/naih (Letöltés ideje: 2024. február 20.)
- NEMES Tamás (2022): *Rekordösszegű bírságot kell fizetnie a Facebook anyacégének*. Világgazdaság. Online: https://www.vg.hu/nemzetkozi-gazdasag/2022/12/rekordosszegu-birsagot-kell-fizetnie-a-facebook-anyacegenek (Letöltés ideje: 2023. november 24.)
- *Next-Generation Deep Packet Inspection*. Leipzig: Rohde &Schwarz GmbH. 2023. Online: https://www.ipoque.com/media/brochures/Solution_guide_en_DPI_3608-7309-62_v0200_144dpi.pdf (Letöltés ideje: 2024. február 15.)

- *NSA slides explain the PRISM data-collection program.* Washington Post. 2013. Online: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (Letöltés ideje: 2024. február 28.)
- Online: https://infolab.nemzetilabor.hu/hu/infokommunikacios-es-informaciotechnologiai-nemzeti-laboratorium-infolab (Letöltés ideje: 2023. november 08.)
- PAHWA, Aashish (2023): *The History Of WhatsApp*. Feedough. Online: https://www.feedough.com/history-of-whatsapp/ (Letöltés ideje: 2023. november 11.)
- PFEIFFER Szilárd (2023): *Már ma is törhető az RSA titkosítás*?. HSWS. Online: https://www.hwsw.hu/hirek/65635/rsa-titkositas-kvantumszamitogep-feltores-kod-algoritmus.html (Letöltés ideje: 2024. február 16.)
- *Phil Zimmermann*. The Center for Internet and Society at Stanford Law School. Online: https://cyberlaw.stanford.edu/about/people/phil-zimmermann (Letöltés ideje: 2024. február 19.)
- *PRISM logo*. NSA, US federal Government; original (C) Adam Hart-Davis © 1998-04-08.
  Online:
  https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/
  (Letöltés ideje: 2024. február 28.)
- *Protección de datos: la Comisión Europea adopta una nueva decisión de adecuación para la circulación de datos UE-EE.UU. con seguridad y confianza.* Comisión Europea. 2023.
  Online: https://ec.europa.eu/commission/presscorner/detail/es/ip_23_3721 (Letöltés ideje: 2024. február 27.)
- *Proud Boys celebrate Trump's 'stand by' remark about them at the debate* New York Times. 2020.
  Online: https://www.nytimes.com/2020/09/29/us/trump-proud-boys-biden.html
  (Letöltés ideje: 2023. december 25.)
- *Regarding CLOUD Act Executive Agreements*. U.S. Department of Justice Criminal Division.
  Online: https://www.justice.gov/criminal/criminal-oia/regarding-cloud-act-executive-agreements (Letöltés ideje: 2024. február 28.)

- *Roads to Mobile 2030: 10 Wireless Industry Trends*. Huawei. 2021. Online: https://www.huawei.com/en/huaweitech/industry-insights/outlook/mobile-2030-10-wireless-industry-trends (Letöltés ideje: 2024. február 23.)
- RUBY, Daniel (2023): *86+ Telegram Statistics In 2023 (Usage, Revenue & Facts)*. DemandSage.
  Online: https://www.demandsage.com/telegram-statistics/ (Letöltés ideje: 2023. november 18.)
- SANGER, David - PERLROTH, Nicole (2015). *Encrypted Messaging Apps Face New Scrutiny Over Possible Role in Paris Attacks*. The New York Times. Online: https://www.nytimes.com/2015/11/17/world/europe/encrypted-messaging-apps-face-new-scrutiny-over-possible-role-in-paris-attacks.html (Letöltés ideje: 2023. július 8.)
- *Secretariat General of the Gulf Cooperation Council.* Online: https://www.gcc-sg.org/en-us/Pages/default.aspx (Letöltés ideje: 2024. február 23.)
- SINGH, Manish (2021): *Signal's Brian Acton talks about exploding growth, monetization and WhatsApp data-sharing outrage*. TechCrunch. Online: https://techcrunch.com/2021/01/12/signal-brian-acton-talks-about-exploding-growth-monetization-and-whatsapp-data-sharing-outrage/?guccounter=1&guce_referrer=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnLw&guce_referrer_sig=AQAAAKuXSptQLR0v5sWMdP23kyAo_s3_3n69hKRC4SbVL1WfB3L5BHumIJ19r_y-tLRsUReS8o-lKBJ0NQbdqgA_jB3uBtw_0rFws8u_Z5PCkWET5H7Kbt9JA0tWIdTphhP1EFjVUje1E-Jma9kBHbhS9TrWRR5ViyPGxsG9GHrBwJJg (Letöltés ideje: 2024. február 26.)
- SMITH, Brad: *Best Messaging Apps to Keep Your Data Private and Secure*. Cyber Protection Magazine.
  Online: https://cyberprotection-magazine.com/best-messaging-apps-to-keep-your-data-private-and-secure (Letöltés ideje: 2023. november 15.)
- *Solutons for Next Generation Networks.* SafeSoft. Online: http://www.safesoft.eu/safelims_ngn.htm (Letöltés ideje: 2024. február 23.)
- *State of IoT – Spring 2023. - Market Report*. IoT Analtics. 2023. Online: https://iot-analytics.com/number-connected-iot-devices/ (Letöltés ideje: 2024. február 23.)

- SUNGHYUN, Choi (2022): *6G - Spectrum Expanding the Frontier* IEEE International Conference on Communications 2022.
  Online: https://news.samsung.com/global/samsung-unveils-6g-spectrum-white-paper-and-6g-research-findings (Letöltés ideje: 2024. február 22.)
- TAMÁSI Dávid (2024): Sajtóközlemény: *A 4iG csoport önálló vállalatba szervezi űr- és technológiai portfólióját*. SpaceJunkie.
  Online: https://spacejunkie.hu/sajtokozlemeny-a-4ig-csoport-onallo-vallalatba-szervezi-ur-es-technologiai-portfoliojat/ (Letöltés ideje: 2024. február 25.)
- *Telefónia – A távközlés története*. T-Com. 15.
  Online: https://docplayer.hu/2271237-Telefonia-a-tavkozles-tortenete.html (Letöltés ideje: 2023. július 26.)
- *Telefonos csapdával csípett nyakon az FBI több száz bűnözőt*. NBSZ NKI. 2021.
  Online: https://nki.gov.hu/it-biztonsag/hirek/anom-az-fbi-telefonos-csapdaja-ami-nagyot-szolt/ (Letöltés ideje: 2024. február 15.)
- *Teljessé vált az Európai elektronikus hírközlési kódex magyarországi átültetése.* NMHH. 2021.
  Online:https://nmhh.hu/cikk/216959/Teljesse_valt_az_Europai_elektronikus_hirkozlesi_kodex_magyarorszagi_atultetese (Letöltés ideje: 2024. február 18.)
- *Tematikus tájékoztató – A személyes adatok védelme*. Európai Unió Bírósága, 2021.
  Online: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_hu.pdf (Letöltés ideje: 2024. február 14.)
- *The CLOUD Act*. Eurojust. 2022.
  Online: https://www.eurojust.europa.eu/sites/default/files/assets/the-cloud-act.pdf (Letöltés ideje: 2024. február 28.)
- *The CLOUD Act*. European Union Agency for Criminal Justice Cooperation. 2022.
  Online: https://www.eurojust.europa.eu/publication/cloud-act (Letöltés ideje: 2024. február 28.)
- *The Most Secure Messaging Apps in 2023*. Avast. 2023.
  Online: https://www.avast.com/c-most-secure-messaging-apps (Letöltés ideje: 2024. február 27.)
- THOMPSON, Arron (2018): *Lawful Interception Basics*. Utimaco. 3.
  Online: https://slideplayer.com/slide/16142658/ (Letöltés ideje: 2024. február 20.)

- *Új elitfegyvernem született.* Magyar Nemzet. 2021. Online: https://magyarnemzet.hu/belfold/2021/05/uj-elitfegyvernem-szuletett (Letöltés ideje: 2024. február 25.)
- USHER, Sebastian (2014): *Tracking Syria fighters now main task for MI5*. BBC News. Online: https://www.bbc.com/news/uk-27947343 (Letöltés ideje: 2023. szeptember 11.).
- *Versenyképességi Tanács, 2015.5.28–29*. Brüsszel. Európai Unió Tanácsa. 2015. Online: https://www.consilium.europa.eu/hu/meetings/compet/2015/05/28-29/ (Letöltés ideje: 2024. február 17.)
- *Viber Encryption Overview.* Rakuten Viber. Online: https://www.viber.com/app/uploads/viber-encryption-overview.pdf (Letöltés ideje: 2023. november 15.)
- *What are the challenges of 5G for Lawful Interception?*. Utimaco. Online: https://utimaco.com/service/knowledge-base/lawful-interception/what-are-challenges-5g-lawful-interception (Letöltés ideje: 2024. február 23.)
- *WhatsApp Security Whitepaper*. Version 6 Updated January 24, 2023 Version. 2023. Online: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf (Letöltés ideje: 2023. november 12.)
- *Why we're taking the UK government to court over mass spying*. Amensty International. 2020. Online: https://www.amnesty.org.uk/why-taking-government-court-mass-spying-gchq-nsa-tempora-prism-edward-snowden (Letöltés ideje: 2024. február 28.)
- ZHANG, XING (2020): *New Retail Marketing Strategy Combining Virtual Reality and 5G Mobile Communication.* Mathematical Problems in Engineering. Online: https://www.hindawi.com/journals/mpe/2021/6632701/ (Letöltés ideje: 2024. február 21.)

9. ÁBRÁK JEGYZÉKE

10. PUBLIKÁCIÓK LISTÁJA

1. DOBÁK Imre – TÓTH Tamás (2023). A külső környezet és tendenciák nyomon követésének szükségessége a stratégiaalkotás tükrében. In DOBÁK Imre – RESPERGER István (szerk.): *Stratégiák, stratégiai gondolkodás, nemzetbiztonság*. Budapest: Ludovika Egyetemi Kiadó. 33–50.
   ISBN: 978-963-531-85-1-3

2. TÓTH Tamás (2023): Actualities of certain security aspects of cryptography with regard to information societies. *National Security Review*, 9(1), 107-118. ISSN 2416-3732
   Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2023_1_NSR.pdf#page=107

3. TÓTH Tamás (2022): Magyarország Nemzeti Biztonsági Stratégiájának nemzetbiztonsági aspektusú elemzése. *Szakmai Szemle,* 20(3), 69-99. ISSN 1785-1181
   Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_3_szam.pdf

4. TÓTH Tamás (2022): Az információgyűjtés új típusú kihívásai a mobil hírközlési hálózatok technológiai fejlődésének aspektusából. In SZELEI Ildikó (szerk.): *A hadtudomány aktuális kérdései napjainkban II*. Budapest: Ludovika Egyetemi Kiadó. 105-122.
   ISBN: 978-963-531-61-6-8
   Online: https://webshop.ludovika.hu/termek/konyvek/hadtudomany/a-hadtudomany-aktualis-kerdesei-napjainkban-ii/

5. TÓTH Tamás (2022): Magyarország nemzeti biztonsági stratégiai evolúciója, annak aktualitásai és főbb nemzetbiztonsági vetületei. *Szakmai Szemle*, 20(2), 58-73.
   ISSN 1785-1181
   Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_2_szam.pdf#page=58.

6. DOBÁK Imre – TÓTH Tamás (2022): Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering). *Belügyi Szemle*, 69(2), 195-212. ISSN 2677-1632
   Online: https://ojs.mtak.hu/index.php/belugyiszemle/article/view/5345/4209

7. TÓTH Tamás (2020): A mobilhálózatok technológiai fejlődéstörténete: Az analóg hangátviteltől az 5G-hálózatokig. *Nemzetbiztonsági Szemle*, 7(4), 44-60.
ISSN 2064-3756
Online: https://doi.org/10.1007/s11276-015-1165-z

8. TÓTH Tamás (2020): Az információgyűjtő szervezetek technikai képességeire ható külső közvetett tényezők. *Felderítő Szemle*, 19(2), 43-57. ISSN 1588-242X
ISSN 1588-242X
Online: https://www.knbsz.gov.hu/hu/letoltes/fsz/2020-2.pdf#page=43

9. TÓTH Tamás (2020): Az egyes social engeneering módszerek elhatárolása és rendszerezése. *Szakmai Szemle*, 18(1), 87-110.
ISSN 1785-1181
Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2020_1_szam.pdf#page=87

10. TÓTH Tamás (2020): New challenges of recruiting personnel for the national security services in light of the information society. *Belügyi Szemle*, 68(2 – Special Issue), 125-139.
ISSN 2677-1632
Online: http://doi.org/10.38146/BSZ.SPEC.2020.2.9

11. TÓTH Tamás (2019). A Nemzetbiztonsági Szakszolgálat felvételi eljárási rendszere. *Belügyi Szemle*, 57(1), 53-67.
ISSN 2677-1632
Online: http://doi.org/10.38146/BSZ.2019.1.4

12. TÓTH Tamás (2019): General description of social engineering and its place in information warfare. *National Security Review*, 5(1), 42-55.
ISSN 2416-3732
Online: https://doi.org/10.38146/BSZ.SPEC.2020.2.9

13. TÓTH Tamás (2019): Az Európai Unió tervezett kiberbiztonsági tanúsítási keretrendszerének bemutatása *Szakmai Szemle*, 17(1), 97-115.
ISSN 1785-1181
Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2019_1_szam.pdf

14. TÓTH Tamás (2019): A digitális alapú, integritás centrikus közszolgálati szervezetek személyi integritását sértő tényezőinek kialakulása, valamint kihívásaik az információs társadalom tükrében. *Rendvédelem*, 8(1), 50–132.
ISSN 2560-2349
Online:
https://epa.oszk.hu/03300/03353/00014/pdf/EPA03353_rendvedelem_2019_1_050-132.pdf

15. TÓTH Tamás (2018): A NATO Kibervédelmi Kiválósági Központ bemutatása. *Nemzetbiztonsági Szemle*, 6(4), 48–62.
ISSN 2064-3756
Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1485/804

16. TÓTH Tamás (2018): Humán kockázatok a kritikus információs infrastruktúrában. *Rendvédelem,* 7(1), 149–176.
ISSN 2560-2349
Online:
https://epa.oszk.hu/03300/03353/00012/pdf/EPA03353_rendvedelem_2018_1_150-177.pdf

17. TÓTH Tamás (2018). Az üzleti információszerzés új kihívásai a szervezett bűnözés XXI. századi paradigmaváltásának következtében. *Szakmai Szemle*, (1), 102–122.
ISSN 1785-1181
Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2018_1_szam.pdf

11. MELLÉKLETEK JEGYZÉKE

1. számú melléklet: Főbb kriptográfiai protokollok, algoritmusok, eljárások általános ismertetése

2. számú melléklet: Az értekezés során vizsgált alkalmazásszolgáltatások kriptográfiai jellemzői

3. számú melléklet: A 3.2.2. részfejezet ábráinak forrásadattáblái

4. számú melléklet: A 4. fejezet ábráinak forrásadattáblái

1. számú melléklet: Főbb kriptográfiai protokollok, algoritmusok, eljárások általános ismertetése

Szimmetrikus kulcsú rejtjelezés[653]***:***

A hagyományos rejtjelező eljárások szimmetrikus, azaz konvencionális kulcsú kriptográfiai algoritmust alkalmaznak, így a rejtjelező és visszafejtő eljárás során azonos kulcsot használnak. „*Feltörésük leggyakrabban csak kimerítő kulcskereséses módszerrel lehetséges, amely a ma használatos algoritmusoknál végtelenül hosszú időt vehet igénybe. Az idő exponenciálisan nő a kulcs hosszának függvényében, és ez adja a biztonság zálogát.*”[654]. A szimmetrikus kulcsú rejtjelezők két nagy osztálya a blokkrejtjelezők és az adatfolyam, vagy kulcsfolyam rejtjelezők. A blokkrejtjelezők, mint például az AES[655]-256 tetszőleges hosszúságú üzeneteket szeletelnek fel előre meghatározott bit hosszúságú blokkokra, majd ezeket a blokkokat titkosítják, azaz helyettesítik, vagy felcserélik. Az adatfolyam rejtjelezők, mint például a ChaCha20, az eredeti szövegben szereplő szimbólumokat egyesével, azokat folyamatában rejtjelezik, szimbólumonként változó kulccsal.[656] Az adatfolyam rejtjelezők könnyen összekeverhetőek a véletlenszám generátorokkal, mivel hasonló elven működnek.

Aszimmetrikus kulcsú rejtjelezés[657]*:*

A rejtjelezéshez és a visszafejtéshez két különböző, egy nyilvános titkosító és egy attól eltérő titkos privát kulcsra van szükség. Előbbit a küldő alkalmazza a rejtjelezésre, utóbbit pedig a fogadó fél a visszafejtéshez. A két kulcs gyakorlatilag nem kivitelezhető számítási idő alatt következtethető ki egymásból. A titkos kulcs védelme szükséges, hiszen az összetartozó párt alkot a nyilvános kulccsal,[658] éppen ezért lényeges a kulcsgenerálás és -csere biztonsága, melyet kulcskezelő algoritmusok biztosítanak. Aszimmetrikus kulcsú titkosítási algoritmus például az

---

[653] AUMASSON, Jean-Philippe (2018): *Serious Cryptography - A Practical Introduction to Modern Encryption*. San Francisco: No Starch Press, Inc. 99-170. Online: https://theswissbay.ch/pdf/Books/Computer%20science/Cryptography/SeriousCryptography.pdf (Letöltés ideje: 2023. július 17.)

[654] PÓSERNÉ OLÁH Valéria (2008): Rejtjelező módszerek vizsgálata. *Hadtudományi Szemle*, 1(1), 46-47. Online: https://www.epa.hu/02400/02463/00001/pdf/EPA02463_hadtudomanyi_szemle_2008_1_043-052.pdf (Letöltés ideje: 2024. február 16.)

[655] AES: Advanced Encryption Standard - Fejlett titkosítási szabvány [U.S. FIPS PUB 197 (FIPS 197)]

[656] ERDÉLYI Áron (2021): *Cryptography vizsgajegyzet*. Budapest: PPKE ITK. Online: https://users.itk.ppke.hu/~erdar2/wp-content/uploads/2021/09/Cryprography.pdf (Letöltés ideje: 2024. február 20.)

[657] Lásd: KAHATE, Atul (2013): *Cryptography and Network Security*. Delhi: Tata McGraw Hill Education Private Limited. 153-204. Online: https://nayakuch.files.wordpress.com/2015/08/cryptography-network-security-atul-kahate.pdf (Letöltés ideje: 2024. február 20.)

[658] TAKÁCS Péter (2009): *Kriptográfiai protokollok formális vizsgálata a CSN logikai rendszer bővítésével*. Doktori (PhD) értekezés. Debrecen: DE ITDI. 7-8. Online: https://dea.lib.unideb.hu/server/api/core/bitstreams/7eca2ade-7dfa-4d4f-9360-c12c8f592019/content (Letöltés ideje: 2024. február 20.)

RSA[659]-2048.[660] A kulcsgenerálás és kulcscsere biztonságos folyamatát különböző kulcskezelő algoritmusok, eljárások biztosítanak, mint például a Diffie-Hellman kulcscsere algoritmus.

Elliptikus görbekriptográfia:

Victor Miller és Neil Koblitz 1985-ben alkotta meg az aszimmetrikus kulcs alapú elliptikus görbe kriptográfia (a továbbiakban: ECC[661]) elméletét, amely a Diffie-Hellman kulcscserére épül. Az ECC egy olyan algoritmus, amely az elliptikus görbe geometriai tulajdonságait használja fel a rejtjelezésre és a kulcsok generálására. Az RSA-nál kevesebb erőforrást igényel a kulcsok generálásához, ezáltal hatékonyabb az erőforrások szempontjából. Az ECC alkalmazása a mobil eszközökön és az IoT eszközökön különösen előnyös, ahol az erőforrások korlátozottak. Az algoritmus biztonsága azon alapul, hogy a titkos privát kulcs megtalálása az elliptikus görbén történő vándorlással nagyon nagy számítási igényű feladat egy támadó számára, amelyet a jelenlegi számítógépek nem tudnak hatékonyan megoldani.[662] Az ECC alkalmazása az utóbbi években elterjedt, a legnépszerűbb algoritmusok P-256 és a Curve25519.

Lenyomatképző (hash) kriptográfiai függvények[663]:

A kriptográfiai protokollok elemeként a lenyomatképző hash egy olyan matematikai függvény, amely tetszőleges hosszúságú bemeneti üzenetből egy rögzített hosszúságú karakterláncot („lenyomatot") hoz létre. A függvény alkalmas az üzenetek integritásának, hitelességének biztosítására, a kulcsvédelemre, a digitális aláírások során is alkalmazzák. *„Egy üzenetet tömörítenek, ami így egy rövidebb, adott hosszú bitsztring lesz. Úgy is tekinthetünk rájuk, mint az üzenet egy lenyomatára. Lényeges részt képeznek különböző aláíró sémákban, üzenet hitelesítéseknél, jelszó tárolásnál és kulcs képzésnél.*"[664]

---

[659] RSA: az algoritmus feltalálói Ron Rivest, Adi Shamir és Leonard Adleman nevének kezdőbetűiből származik.

[660] Az RSA nem helyettesíti a szimmetrikus algoritmusokat, mivel nagy számítási kapacitásigénye okán jóval lassabb. A gyakorlatban az RSA-t gyakran használják szimmetrikus algoritmusokkal, például AES-sel ötvözve, ahol a szimmetrikus algoritmus végzi el az adatok rejtjelezését, míg az RSA a biztonságos kulcscseréért felelős. Az RSA-2048 rendkívül erős biztonsági szintet nyújt, mivel a 2048 bites kulcsokat gyakorlatilag lehetetlen feltörni, de egyre inkább terjed a 3072 és a 4096 bitméret is.

[661] ECC: Elliptic Curve Cryptography - elliptikus görbe kriptográfia

[662] AL SAADI, Maiya – KUMAR, Basant (2020): A Review on Elliptic Curve Cryptography. *International Journal of Future Generation Communication and Networking,* 13(3), 1597-1598. Online: https://www.researchgate.net/publication/350048546_A_Review_on_Elliptic_Curve_Cryptography (Letöltés ideje: 2024. február 18.)

[663] Lásd: FERGUSON, Niels – SCHNEIER, Bruce – KOHNO, Tadayoshi (2010): *Cryptography Engineering: Design Principles and Practical Applications.* Indianapolis: Wiley Publishing, Inc. 77-88. Online: https://zlibrary.to/pdfs/cryptography-engineering-pdf (Letöltés ideje: 2024. február 18.)

[664] SZABÓ Zsuzsanna (2017): *Kriptográfiai protokollok*. Budapest: Eötvös József Tudományegyetem. 7. Online: https://web.cs.elte.hu/blobs/diplomamunkak/bsc_matelem/2018/szabo_zsuzsanna.pdf (Letöltés ideje: 2024. február 16.)

Üzenet-hitelesítő kódok, digitális aláírás:

Az egyes protokollok az üzenetek hitelesítése érdekében alkalmaznak üzenet-hitelesítő kódokat[665](a továbbiakban: MAC[666]), mechanizmusokat is, továbbá az identifikáció érdekében digitális aláírást. A MAC olyan kriptográfiai algoritmus, amely lehetővé teszi egy üzenet hitelességének, sértetlenségének ellenőrzését, észleli az üzenetek manipulálását. A rejtjelező algoritmusok megakadályozzák, hogy a támadó visszafejtse az üzeneteket, a MAC pedig az üzenetek és a forrás eredetének manipulálását. Általában egy titkos kulcsot használnak, amelyet csak a küldő és a címzett fél ismer, és amelyet a hitelesítő algoritmus a hitelesség, sértetlenség ellenőrzésekor használ. Az üzenet-hitelesítő algoritmusok az egyirányú MAC (például a HMAC[667]), valamint a blokklánc titkosítás alapú hitelesítő kód, azaz a CBC-MAC[668].[669]

[665] Lásd: PAAR, Christof – PELZ, Jan (2010): *Understanding Cryptography*. New York: Springer Publishing Company.319-330. Online: https://link.springer.com/book/10.1007/978-3-642-04101-3 (Letöltés ideje: 2024. február 20.)
[666] MAC: Message Authentication Code – üzenethitelesítő kód
[667] HMAC: Hash-based Message Authentication Code – hash alapú üzenethitelesítő kód
[668] CBC-MAC: Cipher Block Chaining Message Authentication Code – blokklánc titkosító üzenethitelesítő kód
[669] FERGUSON at al. 2010: 89

2. számú melléklet: Az értekezés során vizsgált alkalmazásszolgáltatások kriptográfiai jellemzői[670]

Alapértelmezett E2EE-t biztosító alkalmazásszolgáltatások

Signal alkalmazásszolgáltatás kriptográfiai környezete:

A Signal egy az USA székhelyű Signal Messenger LLC által üzemeltett, 2014. július 29-én piacra vezetett nyílt forráskódú alkalmazásszolgáltatás. E2EE-t 2014-es megjelenés óta biztosít, jelenleg alapértelmezetten. Kriptográfiai védelemre a Signal Protocol-t alkalmazza. Az IP címeket nem naplózza.[671] A protokoll szimmetrikus AES-256 titkosító algoritmust, Curve25519 elliptikus görbét, HMAC-SHA256 üzenet-hitelesítő kódot, valamint a Double Ratchet kulcskezelő algoritmust alkalmazza, mely része az Extended Triple Diffie-Hellman (a továbbiakban: X3DH[672]) kulcscsere.[673] A Signal Protocol-t a WhatsApp és a Messenger is alkalmazza.

WhatsApp alkalmazásszolgáltatás kriptográfiai környezete:

A WhatsApp egy az USA székhelyű Meta Platforms LLC által üzemeltett, 2009 óta piacra vezetett alkalmazásszolgáltatás. Az EU területére irányuló szolgáltatásnyújtásért és adatkezelésért az írországi székhelyű Meta Platforms Ireland Ltd. a felelős. E2EE-t 2016 óta biztosít jelenleg alapértelmezetten. Kriptográfiai védelemre a Signal Protocol-t alkalmazza.[674] Az alkalmazás kriptográfiai környezetét a Signal Protocol általános leírásán túl, a WhatsApp 6. verziószámú Biztonsági Fehérkönyve részletezi.[675]

---

[670] A melléklet az alábbi dokumentum felülvizsgált, aktualizált megállapításán alapul: TÓTH Tamás (2023): *A kibervédelem és a nemzetbiztonsági célú törvényes kommunikációellenőrzés viszonyrendszere*. Diplomamunka. Budapest: NKE. 39-41.

[671] LONG, Heinrich (2023a): *Signal Review 2023: Secure Messenger (Pros and Cons)*. Restore Privacy. Online: https://restoreprivacy.com/secure-encrypted-messaging-apps/signal/ (Letöltés ideje: 2023. november 12.)

[672] X3DH: Extended Triple Diffie-Hellman – kiterjesztett hármas Diffie-Hellman

[673] MORA, Justino (2017): *Demystifying the Signal Protocol for End-to-End Encryption (E2EE)*. Medium. Online: https://medium.com/@justinomora/demystifying-the-signal-protocol-for-end-to-end-encryption-e2ee-ad6a567e6cb4 (Letöltés ideje: 2023. november 12.)

[674] PAHWA, Aashish (2023): *The History Of WhatsApp*. Feedough. Online: https://www.feedough.com/history-of-whatsapp/ (Letöltés ideje: 2023. november 11.)

[675] *WhatsApp Security Whitepaper*. Version 6 Updated January 24, 2023 Version. 2023. Online: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf (Letöltés ideje: 2023. november 12.)

Messenger alkalmazásszolgáltatás kriptográfiai környezete:

A Messenger szintén az USA székhelyű Meta Platforms LLC által üzemeltett, 2011 óta önálló termékként piacra vezetett alkalmazásszolgáltatás. Az EU területére irányuló szolgáltatásnyújtásért és adatkezelésért szintén a Meta Platforms Ireland Ltd. a felelős. E2EE-t 2016 óta nem alapértelmezetten, hanem csak a „titkos csevegés" funkció bekapcsolása esetén, funkcionálisan biztosította, azonban 2023. decemberétől ez megváltozott és alapértelmezetté vált az E2EE a peer-to-peer Messenger kommunikáció során.[676] Kriptográfiai védelemre a Signal Protocol-t alkalmazza.[677]

iMessage alkalmazásszolgáltatás kriptográfiai környezete:

A iMessage egy az USA székhelyű Apple Inc. által üzemeltett, 2011 óta az iOS 5-ös verziójával piacra vezetett szöveges és multimédiás adatmegosztást biztosító alkalmazásszolgáltatás – VoIP és élő stream kommunikációt az Apple FaceTime alkalmazása biztosít. Az EU területére irányuló szolgáltatásnyújtásért és adatkezelésért az Egyesült Királyság székhelyű Apple Europe Limited a felelős.[678] E2EE-t 2016 óta, az iOS 9.3/10-es verziójának bevezetését követően biztosít jelenleg alapértelmezetten két kommunikáló fél között.[679] Az iMessage az Apple által fejlesztett, saját kriptográfiai protokollt használ, amely szimmetrikus AES-256 és aszimmetrikus RSA kriptográfiai algoritmusokra épül.[680] Ezeken kívül alkalmazza az SHA-1 hash-t, P-256 elliptikus görbe algoritmust. Az iMessage az üzenetekkel kapcsolatos metaadatokat a csatornán TLS protokollal titkosítja.[681]

---

[676] CRISAN, Loredana (2023): *Launching Default End-to-End Encryption on Messenger*. Meta. Online: https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/ (Letöltés ideje: 2024. február 26.)

[677] CONSTINE, Josh (2014): *Facebook Is Forcing All Users To Download Messenger By Ripping Chat Out Of Its Main Apps*. TechCrunch. Online: https://techcrunch.com/2014/04/09/facebook-messenger-or-the-highway/ (Letöltés ideje: 2023. november 13.)

[678] CALDWELL, Serenity (2011): *Up close with iOS 5: iMessage*. Mac World. Online: https://www.macworld.com/article/214747/ios-5-imessage.html (Letöltés ideje: 2023. november 13.)

[679] XIAOYU, Shi (2016): *Breaking Down iMessage's End-to-End Encryption, and How It Got Hacked in iOS 9.3*. Medford: Tufts University. Online: http://www.cs.tufts.edu/comp/116/archive/fall2016/xshi.pdf (Letöltés ideje: 2023. november 13.); BEST, Shivali (2022): Mark Zuckerberg takes a dig at Apple: Meta CEO says WhatsApp is 'far more private and secure' than iMessage. DalyMail. Online: https://www.dailymail.co.uk/sciencetech/article-11327023/Mark-Zuckerberg-says-WhatsApp-far-private-secure-iMessage.html (Letöltés ideje: 2023. november 13.)

[680] CALDWELL, Serenity (2011): *Up close with iOS 5: iMessage*. Mac World. Online: https://www.macworld.com/article/214747/ios-5-imessage.html (Letöltés ideje: 2023. november 13.)

[681] *Apple Platform Security*. Apple. 2022. 167, 170-171 Online: https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf (Letöltés ideje: 2023. április 11.)

Viber alkalmazásszolgáltatás kriptográfiai környezete:

A Viber egy a Luxemburgban bejegyzett Viber Media Inc. által üzemeltett, 2010-ben piacra vezetett alkalmazásszolgáltatás.[682] E2EE-t 2014 óta biztosít jelenleg alapértelmezetten. Kriptográfiai védelemre a Viber Protocol-t alkalmazza. A protokoll szimmetrikus AES-256 titkosító algoritmust,[683] aszimmetrikus Curve25519 algoritmust, SHA256 hash-t, HMAC-SHA256 üzenet-hitelesítő kódot, valamint Diffie-Hellman kulcsgenerálást/-cserét alkalmaz. „*A Viber protokollja ugyanazokat a koncepciókat használja, mint a nyílt forráskódú Signal alkalmazásban használt Double Ratchet, azonban a Viber megvalósítását a semmiből fejlesztették ki, és nem osztozik a Signal [Protocol] forráskódján.*” [684]

Nem alapértelmezett E2EE-t biztosító alkalmazásszolgáltatások

Telegram alkalmazásszolgáltatás kriptográfiai környezete:

A Telegram egy a Brit Virgin szigeteken bejegyzett Telegram Messenger Inc. által üzemeltett, 2013 márciusában piacra vezetett alkalmazásszolgáltatás. E2EE-t a szöveges üzenetek tekintetében 2013 óta biztosít, de nem alapértelmezetten, hanem csak a „titkos csevegés” bekapcsolása esetén. Jelenleg kriptográfiai védelemre az MTProto 2.0. protokollt alkalmazza.[685] Az MTProto 2.0 az E2EE során szimmetrikus AES-256, aszimmetrikus RSA-2048 algoritmust, Diffie-Hellman kulcskezelést, HMAC-SHA256 üzenet-hitelesítő kódot és SHA-256 hasht alkalmaz.[686]

[682] AGAOUA, Djamel (2020): *Viber is 10*! Rakuten Viber. Online: https://www.viber.com/en/blog/2020-12-02/viber-is-10/ (Letöltés ideje: 2023. november 13.)

[683] SMITH, Brad: *Best Messaging Apps to Keep Your Data Private and Secure*. Cyber Protection Magazine. Online: https://cyberprotection-magazine.com/best-messaging-apps-to-keep-your-data-private-and-secure (Letöltés ideje: 2023. november 15.)

[684] *Viber Encryption Overview.* Rakuten Viber. Online: https://www.viber.com/app/uploads/viber-encryption-overview.pdf (Letöltés ideje: 2023. november 15.)

[685] LONG, Heinrich (2023b): *Telegram Review 2023: NOT as Private as You Think*. Restore Privacy. Online: https://restoreprivacy.com/secure-encrypted-messaging-apps/telegram/ (Letöltés ideje: 2023. november 15.)

[686] *MTProto Mobile Protocol*. Telegram. Online: https://core.telegram.org/mtproto (Letöltés ideje: 2023. november 15.)

3. számú melléklet: A 3.2.2. részfejezet ábráinak forrásadattáblái

20. ábra: Vezetékes és mobil előfizetések/ kiinduló hívások számának/ időtartamának hazai összesített alakulása 1990-2023. között

Év	Vezetékes fővonalak száma (millió darab)	Mobil előfizetések száma(millió darab)	Vezetékes hálózatból kiinduló hívások (millió darab)	Mobilhálózatból kiinduló hívások (millió darab)	Vezetékes hálózatból kiinduló hívások (millió perc)	Mobilhálózatból kiinduló hívás (millió perc)
1990	0,996	..	1 301	..		
1991	1,129	0,005	1 456	3		
1992	1,292	0,023	1 638	16		
1993	1,498	0,070	1 839	54		
1994	1,785	0,142	2 350	123		
1995	2,157	0,267	2 922	294		
1996	2,651	0,473	3 433	532		
1997	3,095	0,706	3 788	714		
1998	3,385	1,034	4 144	949	9 593	1221
1999	3,609	1,620	4 250	1 279	10 037	1667
2000	3,799	3,076	4 223	2 258	11 861	2766
2001	3,746	4,967	3 921	3 780	12 089	4055
2002	3,670	6,886	3 728	4 399	12 323	5080
2003	3,607	7,945	3 537	4 700	11 056	6169
2004	3,570	8,727	3 258	5 124	10 576	7492
2005	3,453	9,320	2 999	5 995	9 905	9496
2006	3,365	9,966	2 636	6 759	8 558	11904
2007	3,282	11,030	2 200	7 173	7 276	13653
2008	3,115	12,224	1 981	7 777	6 291	15765
2009	3,110	11,792	1 784	7 789	5 661	16666
2010	2,933	12,012	1 678	8 071	5 261	17462
2011	2,908	11,690	1 599	8 368	5 412	17860
2012	2,927	11,579	1 426	8 045	5 235	18001
2013	2,919	11,676	1 344	8 080	5 141	18310
2014	3,012	11,796	1 188	8 149	4 673	19346
2015	3,082	11,865	1 061	8 140	4 433	20586
2016	3,155	11,793	946	7 949	4 220	21468
2017	3,171	11,738	857	7 898	4 006	22377
2018	3,230	11,831	761	7 945	3 700	23232
2019	3,183	12,532	662	7 972	3 383	24028
2020	3,085	12,710	603	7 851	3 633	26632
2021	2,956	13,314	529	8 495	3 239	28785
2022	2,845	13,607	441	8 577	2 384	28426
2023 (becs.)	2,708	14,037	363	7 958	2184	26922
Forrás:	KSH 2024. 12.1.1.2.tábla 12.2.1.2. tábla	KSH 2024. 12.1.1.5. tábla 12.2.1.4. tábla	KSH 2024. 12.1.1.2.tábla 12.2.1.2. tábla	KSH 2024. 12.1.1.5. tábla 12.2.1.4. tábla	KSH 2024 12.2.1.2. tábla; NMHH 2024. 8. tábla; NMHH EHMMSA 2023.	KSH 2024. 12.1.1.5. tábla; NMHH 2024. 8. tábla; NMHH EHMMSA 2023.

21. ábra: Belföldi mobilinternet forgalom megoszlásának alakulása hálózat típusonként 2015-2022.

Időszak	2G hálózat	3G hálózat	4G/ 5G hálózat
2015Q4	1,8%	43,5%	54,7%
2016Q1	1,7%	38,1%	60,2%
2016Q2	1,9%	31,8%	66,4%
2016Q3	1,8%	26,1%	72,0%
2016Q4	1,6%	22,2%	76,2%
2017Q1	0,9%	19,8%	79,2%
2017Q2	1,0%	15,8%	83,2%
2017Q3	1,7%	12,2%	86,1%
2017Q4	1,3%	9,9%	88,8%
2018Q1	1,1%	8,3%	90,5%
2018Q2	1,0%	7,5%	91,5%
2018Q3	1,3%	6,2%	92,5%
2018Q4	1,1%	5,5%	93,4%
2019Q1	1,1%	4,7%	94,1%
2019Q2	0,9%	4,2%	94,9%
2019Q3	1,2%	3,9%	94,9%
2019Q4	0,8%	3,2%	96,0%
2020Q1	0,9%	2,9%	96,2%
2020Q2	1,0%	4,4%	94,6%
2020Q3	0,7%	3,7%	95,6%
2020Q4	1,1%	3,3%	95,6%
2021Q1	1,2%	3,0%	95,8%
2021Q2	1,1%	2,8%	96,1%
2021Q3	0,0%	3,2%	96,7%
2021Q4	0,1%	4,1%	95,9%
2022Q1	0,0%	2,3%	97,6%
2022Q2	0,0%	1,9%	98,1%
2022Q3	0,0%	1,2%	98,7%
2022Q4	0,0%	1,0%	99,0%
Forrás	NMHH 2023. 22. ábra	NMHH 2023. 22. ábra	NMHH 2023. 22. ábra

22. ábra: Mobilinternetre csatlakozott mobiltelefonok és táblagépek alakulása hálózat típusonként 2021.Q1. – 2023.Q2.

Időszak	2G hálózat	3G hálózat	4Ghálózat	5G hálózat
2021Q1	15,0%	6,0%	77,0%	2,0%
2021Q2	15,0%	6,0%	77,0%	3,0%
2021Q3	13,0%	6,0%	75,0%	6,0%
2021Q4	14,0%	4,0%	74,0%	8,0%
2022Q1	10,0%	4,0%	77,0%	9,0%
2022Q2	8,0%	3,0%	75,0%	13,0%
2022Q3	7,0%	3,0%	73,0%	17,0%
2022Q4	7,0%	3,0%	70,0%	20,0%
2023 Q1	7,0%	3,0%	67,0%	23,0%
2023 Q2	6,0%	2,0%	65,0%	26,0%
Forrás:	NMHH 2024. 28. ábra	NMHH 2024. 28. ábra	NMHH 2024. 28. ábra	NMHH 2024. 28. ábra

23. ábra: Indított mobil hívás-, küldött SMS és mobil (okostelefon) internetfogalom hazai alakulása 2002-2023 között

Időszak	Mobilhálózatból kiinduló hívás (millió	Mobilhálózatból kiinduló hívás (millió	Küldött SMS/MMS (millió darab)	Okostelefon internetforgalom (Petabyte)
2002	4399	5080		
2003	4700	6169		
2004	5124	7492		
2005	5995	9496		
2006	6759	11904		
2007	7173	13653		
2008	7777	15765		
2009	7789	16666		
2010	8071	17462	1963	14
2011	8368	17860	1972	17
2012	8045	18001	1967	26
2013	8080	18310	1842	30
2014	8149	19346	1800	38
2015	8140	20586	1737	57
2016	7949	21468	1801	45
2017	7898	22377	1898	85
2018	7945	23232	1992	176
2019	7972	24028	1949	295
2020	7851	26632	1761	479
2021	8495	28785	1739	654
2022	8557	28426	1640	888
2023 (becs	7 958	26922	1934	1134
Forrás:	KSH 2024. 12.1.1.5. tábla 12.2.1.4. tábla	KSH 2024 12.2.1.4. tábla; NMHH 2024. 8. tábla; NMHH EHMMSA 2023.	KSH 2024. 12.1.1.5. tábla 12.2.1.4. tábla; NMHH 2023. 14. tábla	KSH 2016. 12. tábla; NMHH 2023. 16. tábla; NMHH 2024. 2. tábla

24. ábra: Internetforgalmat bonyolított okostelefonos SIM-kártyák számának és fajlagos forgalmának alakulása 2016-2023 között

Időszak	Internetforgalmat bonyolító okostelefon SIM kártya	Egy SIM-kártyára jutó havi adatforgalom (Gbyte)
2015 Q4	4353730	1,2
2016Q1	4403704	1,1
2016Q2	4606948	1,3
2016Q3	4817240	1,5
2016Q4	4920097	1,7
2017Q1	4967981	1,7
2017Q2	5179147	1,9
2017 Q3	5409702	2,5
2017Q4	5412394	2,7
2018Q1	5476524	3,1
2018Q2	5675292	3,5
2018Q3	5912060	4,1
2018Q4	6102643	4,5
2019Q1	6178414	4,6
2019Q2	6316161	5,1
2019Q3	6462156	6,0
2019Q4	6597142	7,0
2020Q1	6807457	7,9
2020Q2	6787570	10,0
2020Q3	6934054	8,8
2020Q4	6961643	9,8
2021Q1	6917284	10,0
2021Q2	7048891	10,8
2021Q3	7685030	13,2
2021Q4	7536708	12,4
2022Q1	7404283	12,5
2022Q2	7556080	13,8
2022Q3	7650007	15,4
2022Q4	7698143	17,0
2023Q1	7673000	20,5
2023 Q2	7760000	23,1
Forrás:	NMHH 2019 16. tábal; NMHH 2023. 17. tábla NMHH 2024. 20. tábla	NMHH 2019. 16. tábala; NMHH 2023. 17. tábla; NMHH 2024. 22. tábla

25. ábra: A mobil elektronikus hírközlés tendenciái és összefüggése a hazai LI evolúciójával napjainkig

Időszak	Vezetékes hálózatból kiinduló hívások (millió darab)	Mobilhálózatból kiinduló hívások (millió darab)	Vezetékes hálózatból kiinduló hívások (millió perc)	Mobilhálózatból kiinduló hívás (millió perc)	Küldött SMS/MMS (millió darab)	Okostelefon internetforgalom (Petabyte)
1990	1 301	..				
1991	1 456	3				
1992	1 638	16				
1993	1 839	54				
1994	2 350	123				
1995	2 922	294				
1996	3 433	532				
1997	3 788	714				
1998	4 144	949	9 593	1221		
1999	4 250	1 279	10 037	1667		
2000	4 223	2 258	11 861	2766		
2001	3 921	3 780	12 089	4055		
2002	3 728	4 399	12 323	5080		
2003	3 537	4 700	11 056	6169		
2004	3 258	5 124	10 576	7492		
2005	2 999	5 995	9 905	9496		
2006	2 636	6 759	8 558	11904		
2007	2 200	7 173	7 276	13653		
2008	1 981	7 777	6 291	15765		
2009	1 784	7 789	5 661	16666		
2010	1 678	8 071	5 261	17462	1963	14
2011	1 599	8 368	5 412	17860	1972	17
2012	1 426	8 045	5 235	18001	1967	26
2013	1 344	8 080	5 141	18310	1842	30
2014	1 188	8 149	4 673	19346	1800	38
2015	1 061	8 140	4 433	20586	1737	57
2016	946	7 949	4 220	21468	1801	45
2017	857	7 898	4 006	22377	1898	85
2018	761	7 945	3 700	23232	1992	176
2019	662	7 972	3 383	24028	1949	295
2020	603	7 851	3 633	26632	1761	479
2021	529	8 495	3 239	28785	1739	654
2022	441	8 577	2 384	28426	1640	888
2023 (becs.)	363	7 958	2184	26922,0	1 934,0	1 134,0
Forrás:	KSH 2024. 12.1.1.2.tábla 12.2.1.2. tábla	KSH 2024. 12.1.1.5. tábla 12.2.1.4. tábla	KSH 2024 12.2.1.2. tábla; NMHH 2024. 8. tábla; NMHH EHMMSA 2023.	KSH 2024. 12.1.1.5. tábla; NMHH 2024. 8. tábla; NMHH EHMMSA 2023.	KSH 2024. 12.1.1.5. tábla 12.2.1.4. tábla; NMHH 2023. 14. tábla	KSH 2016. 12. tábla; NMHH 2023. 16. tábla; NMHH 2024. 2. tábla

4. számú melléklet: A 4. fejezet ábráinak forrásadattáblái

29. ábra: Vizsgált alkalmazásszolgáltatások letöltésének éves megoszlása 2019-2021 között (millió felhasználó/ év)

	2019	2020	2021	2022	Forrás:
Signal	10	22	125	155	CURRY 2024a; CURRY 2024b
WhatsApp	643	669	437	1221	MARCH 2023; CURRY 2024b
Messenger	505	571	238	405	MARCH 2023; CURRY 2024b
Telegram	119	296	359	196	MARCH 2023; CURRY 2024b
Viber	66	60	44	25	MARCH 2023; CURRY 2024b

30. ábra: Vizsgált alkalmazásszolgáltatások letöltésének 2023. január havi megoszlása

	2023. január havi letöltések
Signal	2,96
WhatsApp	51,19
Messenger	21,31
Telegram	36,7
Viber	3,54
Forrás:	CECI 2024

31. ábra: Vizsgált alkalmazásszolgáltatások és az E2EE bevezetésének összehasonlítása

	Megjelenés éve	E2EE bevezetés éve	Források:
WhatsApp	2009	2016	PAHWA 2023
Viber	2010	2014	AGAOUA 2020
Messenger	2011	2016	COUSTINE 2017
iMessage	2011	2016	CALDWELL 2011; XIAYOU 2016
Telegram	2013	2013	LONG 2023b
Signal	2014	2014	LONG 2023a

33. ábra: Vizsgált alkalmazásszolgáltatások és az E2EE bevezetésének és a Snowden-incidens időpontjának összehasonlítása

	Megjelenés éve	E2EE bevezetés éve	2013 Snowden-incidens	Források:
WhatsApp	2009	2016	2013	PAHWA 2023
Viber	2010	2014	2013	AGAOUA 2020
Messenger	2011	2016	2013	COUSTINE 2017
iMessage	2011	2016	2013	CALDWELL 2011; XIAYOU 2016
Telegram	2013	2013	2013	LONG 2023b
Signal	2014	2014	2013	LONG 2023a

34. ábra: Vizsgált alkalmazásszolgáltatások és az E2EE bevezetésének, a Snowden-incidens időpontjának és a GDPR alkalmazandóságának összehasonlítása

	Megjelenés éve	E2EE bevezetés éve	2013 Snowden-incidens	2018 GDPR alk.	Források:
WhatsApp	2009	2016	2013	2018	PAHWA 2023
Viber	2010	2014	2013	2018	AGAOUA 2020
Messenger	2011	2016	2013	2018	COUSTINE 2017
iMessage	2011	2016	2013	2018	CALDWELL 2011; XIAYOU 2016
Telegram	2013	2013	2013	2018	LONG 2023b
Signal	2014	2014	2013	2018	LONG 2023a

35. ábra: Vizsgált alkalmazásszolgáltatások és az E2EE bevezetésének, a Snowden-incidens időpontjának, a GDPR alkalmazandóságával és a 2015-től kezdődő Európai terrortámadások kezdőidőpontjának összehasonlítása

	Megjelenés éve	E2EE bevezetés éve	2013 Snowden-incidens	2018 GDPR alk.	2015 EU terrortámadások	Források:
WhatsApp	2009	2016	2013	2018	2015	PAHWA 2023
Viber	2010	2014	2013	2018	2015	AGAOUA 2020
Messenger	2011	2016	2013	2018	2015	COUSTINE 2017
iMessage	2011	2016	2013	2018	2015	CALDWELL 2011; XIAYOU 2016
Telegram	2013	2013	2013	2018	2015	LONG 2023b
Signal	2014	2014	2013	2018	2015	LONG 2023a