A KIBERTÉR SZABÁLYOZÁSI MODELLJEI EURÓPÁBAN

DORNFELD LÁSZLÓ[1]

ABSZTRAKT

Cyberspace has become a new contest ground for national interest. Although lacking borders in a traditional sense, the physical infrastructure and the intermediaries are located in individual countries. This new stage of geopolitics is about controlling data as information is the most precious thing in the digital world. Two competing models have been developed: the now dominant multi-stakeholder model and the cyber sovereignty model challenging its positions. The first one was adopted at a time of Western international supremacy and is supported by Western democracies, mainly the USA and the EU, while the second is spearheaded by Russia and China. Then there is a wide third group who are undecided on the matter and there are huge efforts to convince them, leading to the birth of cyber diplomacy. Now there are important changes undergoing in the relations of the nations involved: the US-Chinese trade war, the animosity between Russia and the EU due to the Crimean annexation, which all effect their stance on cyber governance. As US is now losing its leading position in the area, the EU and China is trying to fill in the gaps.

Keywords: cyberspace, cyber diplomacy, multi-stakeholder, cyber sovereignty, regulation

BEVEZETÉS

Az emberiség az elmúlt pár évtizedben rohamos sebességgel tette magáévá az új digitális technológiai vívmányokat, amelyek jelentősen megváltoztatták mindennapjainkat. Az előző évszázad közepétől egyre jelentősebbé vált a harmadik ipari forradalomként is nevezett információtechnológiai fejlődés, és napjainkban sokan már negyedik ipari forradalomról beszélnek, amely ennek vívmányain alapul (Schwab, 2016). Az új fejlemények közé sorolhatók az egymással folyamatos kapcsolatban álló rendszerek (pl. dolgok internete, önvezető autók), a 3D nyomtatás, az új virtuális fizetőeszközök (pl. Bitcoin), vagyis az életünk egyre nagyobb részének digitalizálása.

Ezek a változások a geopolitikában is éreztetik a hatásukat, hiszen az új vívmányok nemcsak újabb és újabb kihívások elé állítják az országokat, de egyúttal új lehetőségeket is teremtenek az államok közötti versengésben. Az új technológiák átvétele, szabályozásának megalkotása előnyhöz juttattja azokat, akik elsők között teszik ezt meg: az innováció, a tehetség és a rugalmasság kiemelkedően fontossá váltak a 21. század elején (Engelke, 2018). Az államoknak az új technológiák alkalmazása mellett azok biztonságosságáról is gondoskodniuk kell (Douzet, 2016, 29-30. o.).

A korábbi, viszonylag szabályozatlan időszakhoz képest az államok egyre inkább próbálják befolyásuk alá vonni a kiberteret. Ennek egyik fontos eszköze a szabályozás kialakítása, amivel kapcsolatban beszélhetünk normaalkotó és normakövető államokról. Publikációmban a két kialakult szabályozási modell helyzetét vizsgálom: az Európai Unió által elfogadott több érdekelt fél bevonásával zajlót, illetve az Oroszország által alkalmazott nemzeti

[1] dr. Dornfeld László, Mádl Ferenc Összehasonlító Jogi Intézet, laszlo.dornfeld@mfi.gov.hu

szuverenitás talaján állót (Dornfeld, 2016, 78. o.), és mindemellett egy jelentős harmadik csoport is található, az egyik iránt sem elkötelezett országoké. A tényleges szabályozáson túl vizsgálom a különböző nemzetközi fórumok előtti megjelenéseket, illetve az állami politikai törekvéseket is.

EURÓPAI UNIÓ

Az Európai Unió hamar meglátta az internetben és az új infokommunikációs technológiák terjesztésében rejlő hasznot. A technológia gazdasági célú felhasználásának elősegítése már régóta fontos célként szerepel, és manapság már a digitális egységes piac megteremtése a kitűzött cél. A 2010-ben elfogadott Európa 2020 stratégia (COM/2010/2020 final) egyik fontos kiemelt kezdeményezése volt a digitális menetrend kialakítása. Ennek részeként az Európai Bizottság 2015-ben megalkotta az európai digitális egységes piaci stratégiát (SWD(2015) 100 final), amely leszögezi, hogy a megvalósítás mintegy 400 milliárd eurós gazdasági növekedést eredményezne.

Az EU számos fontos rendelkezést fogadott el a digitális egységes piac megteremtése érdekében. Így például kiállt az internetsemlegesség mellett (COM(2011) 222 final), eltörölte a roaming díjakat (531/2012/EU rendelet), valamint javaslatot tett egy rendeletre az az elektronikus hírközlés egységes európai piacáról (COM/2013/0627 final), és elfogadták az új szerzői jogi irányelvet (2019/790 irányelv a digitális egységes piacon a szerzői és szomszédos jogokról).

Sokkal inkább elvi alapokra helyezve a kérdést, egészen más indokot lát az EU-s szabályozás kialakulása mögött a kanadai központú Nemzetközi Kormányzati Innovációs Központ, amelynek egyik tanulmánya szerint a brüsszeli döntéshozók a „polgári internet" megvalósítását tűzték ki célul. A tanulmány szerzői szerint ez az európai történelmi gyökerekhez visszanyúló felfogás, amelynek célja, hogy egyfajta erényes polgári térnek megőrizze az internetet (O'Hara – Hall 2018, 6. o.)

Az okot tehát már ismerjük, ám a bevezetőben már említett biztonság dimenziója igen fontos szerepet játszik az elért eredmények biztosításában. Az Európai Unió kiberbiztonsági stratégiája (JOIN/2013/01) szerint ugyanis „az új internetalapú technológiák elterjedéséhez bizalomra van szükség az emberek részéről". Ez a bizalom pedig csak úgy teremthető meg, ha nem kell a felhasználóknak adataik sérülésétől, illetve különböző bűncselekményektől (pl. csalástól) tartaniuk az interneten. A kérdés fontosságát az is mutatja, hogy az európai biztonsági stratégia (COM(2015) 185) a három fő prioritás közé sorolta a kiberbűnözést, amely így olyan problémákkal került hasonló fontossági szintre, mint a terrorizmus és a határokon átnyúló szervezett bűnözés.

Az Uniós szabályozás és politika átalakulása

Az európai kiberszabályozás kezdetei nem az EU-hoz, hanem az attól több taggal rendelkező Európa Tanácshoz köthetők. Az első vonatkozó ajánlás 1989-re datálható, amelyben a számítógépekkel kapcsolatos bűncselekmények felsorolása történt meg (Dornfeld, 2016, 61). A legfontosabb hozzájárulása az Európa Tanácsnak ugyanakkor a gyakran Budapesti Egyezmény néven emlegetett számítástechnikai bűnözésről szóló egyezmény létrehozása volt, amely 2001-es elfogadása óta a legfontosabb alapegyezmény a kibertér minden érdekelt fél bevonásával történő szabályozásával összefüggésben. 2001-ben 35 ország írta alá, köztük olyan Európa Tanácson kívül államok, mint az Egyesült Államok, Kanada, Japán és Dél-Afrika

(Buono 2012, 336. o.). Az egyezményt 2018-ig az ENSZ tagállamainak több mint harmada, 71 ország ratifikálta, írta alá vagy került meghívásra (Schulman 2018). Számos regionális szervezetben (így például a Brit Nemzetközösségben, a Karib-tengeri Közösségben és a Délkelet-ázsiai Nemzetek Szövetségében) a dokumentum a saját szabályozás modelljévé is vált (Dornfeld 2016, 61. o.).

Az Európai Unió számos területen épít az Európa Tanács vívmányaira (például Az Emberi Jogok Európai Egyezményére az alapjogvédelemnél) és ez a terület sem kivétel. Az EU számos alkalommal elismerte a Budapesti Egyezmény jelentőségét, arra buzdítva a még nem részes tagállamait, hogy mihamarabb csatlakozzanak hozzá (Buono 2012, 336. o.). Az Uniós szintű kiberszabályozás azonban sokáig igen mostoha helyzetű terület volt, mivel a biztonságot érintő területek a harmadik pillér részei voltak, ahol csak a közvetlen hatállyal nem bíró kerethatározatok elfogadására volt lehetőség (Dornfeld 2016, 62. o). A Lisszaboni Szerződés 2009-es elfogadása változást hozott, ugyanis most már nem volt szükség egyhangúságra a jogalkotáshoz, és a kerethatározatokat is felváltották a közvetlen hatállyal bíró (vagyis az átültetéstől függetlenül alkalmazható) másodlagos jogforrások. Ezt követően megindult a fennálló uniós kiberbiztonsági rezsim felülvizsgálata jogi, politikai és intézményi szinten egyaránt (Buono 2012, 338. o.)

Az Unió több esetben is igyekezett a hatékonyságot növelni, még ha ez esetleg az alapvető jogok sérülésével is járt. Ilyen volt például a 2006/24/EK irányelv, amely bizonyos adatok megőrzésére kötelezte a szolgáltatókat, hogy azok elérhetők legyenek a büntetőeljárás során. Maga az elfogadás körülményei is meglehetősen sajátosak voltak: mivel bizonyosnak tűnt, hogy Németország nem szavazza azt meg, az egyhangúságot megkívánó harmadik pillér helyett az első pillér részeként fogadták azt el. 2014-ben végül az Európai Bíróság érvénytelennek mondta ki az irányelvet az arányosság és az Európai Alapjogi Charta megsértése miatt (Dornfeld 2017, 250-251. o.) Hasonlóan nagy aggodalmat okozott az EU 2018-as e-bizonyíték javaslatcsomagja (Warken 2019, 427-431. o.), amelynek lényege, hogy a bűnüldöző hatóságok a más tagállami hatóságok igénybevétele nélkül, közvetlenül igényelhetnek adatot a szolgáltatóktól. Ez jelentősen gyorsítja a bizonyítékok határon átnyúló beszerzését, és egyszerűsíti az eljárást, ugyanakkor a javaslat ellenzői szerint igazságügyi hatóságokká transzformálja a szolgáltatókat, és mivel rájuk nem vonatkoznak a büntetőeljárási garanciák, ez jelentősen sértheti az állampolgárok jogait (EDRi, 2018).

Az EU a nemzetközi színtéren: normakövetőből normaalkotó

Az Európai Unió a kibertér szabályozásával kapcsolatban igyekszik minél aktívabb külpolitikát folytatni, és aktívan részt venni a kiberbiztonsággal kapcsolatos nemzetközi diskurzusban. A 2012-es ITU nemzetközi távközlési világkonferencián való részvétel kapcsán a Tanács COM(2012) 430 határozatában úgy fogalmazott, hogy a nemzetközi távközlési szabályozás (ITR) bármely módosítása összhangban kell, hogy legyen az uniós vívmányokkal, és segítenie kell az Unió céljainak elérését. 2014-ben a Tanács következtetései a kiberdiplomáciáról című 9967/4/14. számú dokumentumban sor került a kibetérrel kapcsolatos nemzetközi politika hat uniós pillérének meghatározására. (Dancă 2015, 95. o.) A dokumentumban olyan EU-s értékek jelennek meg, mint az emberi jogok védelme a kibertérben, a hatályos nemzetközi jog alkalmazása a nemzetközi biztonság területén és a minden érdekelt bevonásával működő szabályozási modell támogatása. A Tanács számos célt is megfogalmaz ebben, mint például az EU versenyképességének és jólétének fokozása, a kiberkapacitás-építés és -fejlesztés, valamint a nemzetközi partnerekkel való szorosabb együttműködés.

Az Európai Unió igen sokáig csak normakövető állam volt, normaalkotóként csak korlátozottan lépett fel. Így például a fentebb említett 2012-es nemzetközi távközlési világkonferencia kapcsán az EU már régóta a globális szabályozás megszüntetése mellett kardoskodott, ám végül az Egyesült Államokat követve mégsem szorgalmazta annak megszüntetését, ami komoly diplomáciai kudarcot eredményezett, amikor az USA kivonult a tárgyalásokról (Mueller 2012). 2014-ben került sor az EU-USA kiberpárbeszédre, amely a kiberdiplomáciai kérdéseket érintette. Napjainkban az EU Japánnal, Dél-Koreával és Indiával is megbeszéléseket folytat, valamint kiemelt figyelmet fordít a Nyugat-Balkánra.

Az elmúlt években változni látszik az eddigi Amerika központú tendencia, és ahogy az USA egyre inkább háttérbe vonul a világpolitikában, úgy Kína mellett az EU lépett színre, mint új globális normaalkotó. A két szereplő már régóta folytat gazdasági együttműködést, ám digitális téren az EU az, amely inkább rászorul Kínára és nem fordítva. Mivel a tagállamok külön politikákat folytatnak, a digitális terület is az amerikai-kínai kereskedelmi háború egyik színterévé vált (Bendiek – Godehart – Schulze 2019). Az ezen kérdésben egységet nélkülöző EU esetén a legfontosabb tényező az, hogy túlságosan is nagy piacot jelent ahhoz, hogy az óriás amerikai techcégek figyelmen kívül hagyják az új szabályozást (O'Hara – Hall 2018, 7. o). Politikai szinten fontos fejlemény volt 2015-ben az orosz „dezinformációs narratívákat" célzó akcióterv, valamint a 2016-os uniós globális stratégia, amely a kiberkérdéseket az európai külpolitika egyik sarokkövének tette meg, és az EU magára, mint „előre tekintő globális kiberjátékosra" tekint, amely megvédi kritikus eszközeit és érdekeit a digitális térben is (Barrinha 2018, 32. o). Az egyik globális hatású uniós normaalkotás az 2016/679. sz. európai általános adatvédelmi rendelet (GDPR) volt, amely az adatvédelem terén vált meghatározóvá. De ugyanilyen jelentős hatással bír a korábban már említett e-bizonyíték javaslatcsomag és az új szerzői jogi irányelv is. Jelenleg úgy tűnik, hogy belső problémái és a nagy techcégek hatalmas befolyása miatt az Egyesült Államok még jó ideig nem lesz képes visszanyerni sokáig élvezett vezető szerepét (Geller 2018).

OROSZORSZÁG

Oroszország a nemzeti szuverenitást a kibertérre kiterjeszteni kívánó országok egyik vezető hatalma Kínával közösen. A javasolt modell lényegileg a „vesztfáliai szuverenitás" digitális térre történő kiterjesztését szorgalmazza, vagyis a jelenlegi minden érdekelt fél bevonásával működő modellel szemben az államoknak biztosítana kizárólagosságot. Oroszország viszonylag hamar, 1998-ban érdeklődést mutatott a globális szabályozás iránt, és orosz javaslatra fogadta el az ENSZ Közgyűlése az 53/70. határozatot, amely a kiberteret érő új fenyegetésekkel kapcsolatban fogalmazott meg ajánlást a tagállamok számára.

2011 szeptemberében a sanghaji együttműködés országai: Oroszország, Kína, Kazahsztán, Kirgizisztán, Tádzsikisztán és Üzbegisztán nemzetközi magatartási kódexet javasoltak az ENSZ Közgyűlésének a kiberbiztonság megteremtése érdekében, amelyben hangsúlyos szerepet kapott a szerintük a nemzeti szuverenitás részét képező kiberszuverenitás, vagyis a kormányok azon joga, hogy határaikon belül korlátok nélkül ellenőrizhessék az adatforgalmat (Dornfeld 2016, 48. o). A dokumentum sok mindenben tekinthető inkább egyszerű retorikai fogásnak, valamint egy könnyen felmutatható válasznak, ha bárki a részes államok kiberbiztonság iránti eltökéltségét vitatja. Kína és Oroszország a nemzetközi szervezeteken keresztül igyekszik a korábban, a nyugati erőfölény idején kialakult szabályozást (így pl. a Budapesti Egyezményt) felülírni (Lewis 2013, 8. o.). Az ITU 2012-es világkonfereniciáját megelőzően, 2011 júniusában Vlagyimir Putyin miniszterelnök például

kijelentette, hogy országának célja az, hogy a szervezeten keresztül nemzetközi irányítás alá vonja az internetet (Barrinha 2018, 37. o.).

A sanghaji országok képviselői közös levélben kérték az ENSZ főtitkárát, hogy az általuk elfogadott nemzetközi magatartási kódexet a Közgyűlés 66. ülésszakán hivatalos dokumentumként terjessze a megjelentek között (Zhang 2013, 126. o.). Változtatásokat követően Oroszország és Kína 2015 januárjában ismét benyújtotta a magatartási kódexet a főtitkárnak. A változtatások megerősítették, hogy az államok szuverén joga politikai döntéseket hozni az internettel kapcsolatos közpolitikai kérdésekben. Egyúttal előírták, hogy minden részes állam köteles más államok szuverenitását, területi integritását és politikai függetlenségét tiszteletben tartani (Dornfeld 2016, 75-76. o).

Az oroszok más téren is digitális úttörőnek bizonyultak: a világon először orosz hackerek voltak képesek megbénítani egy állam digitális működését, amikor összehangolt kibertámadás érte Észtországot 2007-ben (Barrinha 2018, 34. o.). Ugyan az orosz állami érintettség mind a mai napig nem nyert bizonyítást, az incidens Oroszország és az EU kiberteret illető felfogását jelentősen befolyásolta. A későbbi események, így például az USA 2016-os elnökválasztásába történő beavatkozás, a krími annexiónál alkalmazott hibrid hadviselés és más választási beavatkozási kísérletek oda vezettek, hogy 13 EU tagállam tartott attól, hogy az oroszok digitális úton beavatkoznak belpolitikájába (Barrinha 2018, 34. o). Hasonlóan komoly helyzet alakult ki, amikor két zsarolóvírus, a WannaCry és a NotPetya jelentős pusztítást végzett a világ információs rendszereiben. Ezeket sokak szerint az oroszok fejlesztettek ki – az orosz kiberbűnözési piac mintegy 2,3 milliárd dollárra rúg, így az EU-t érő sok kiberfenyegetés innen indul ki (Barrinha 2018, 36. o).

Az orosz-kínai viszonyt érintő számos feszültség ellenére látszólag teljes összhang mutatkozik a kibertérrel kapcsolatos politikai törekvéseket illetően. 2015-ben a két ország bilaterális egyezményt is kötött, amely azonban nem sok újdonságot tartalmazott a korábbi dokumentumokhoz képest, így inkább csak az eddigi szándékok megerősítését jelzi. Ugyanakkor az egyéb geopolitikai feszültségek korántsem teszik olyan egyértelművé a hosszútávú együttműködést, ahogy a tényleges célok sem feltétlenül azonosak. Míg a pekingi vezetés politikájának legfőbb célja az internet uralása, addig az orosz motivációkat illetően akad olyan vélemény, amely szerint csupán eszköznek tekintik azt a nyugattal szemben. Az érvelés szerint az oroszok nem azért támadják a fennálló szabályozási status quot, mert új rendszert szeretnének, hanem, hogy a kialakuló káoszt és szabályozatlanságot saját dezinformációs tevékenységükre használhassák ki (O'Hara – Hall 2018, 11. o.).

ÖSSZEGZÉS

Mint a fentiekből látható, a globális kiberszabályozás kialakult modellje minden érdekelt fél bevonásával valósul meg, elsősorban Amerika központú rendszerként. A geopolitikai érdekek mentén három tábor alakult ki: a status quot támogató, elsősorban nyugati demokráciák, a nemzeti szuverenitás alapjára helyezkedő autoriter államok, amelyek a fennálló rezsim megváltoztatásában érdekeltek, valamint a legnépesebb csoport, az egyik irányba sem elkötelezett államok. Ez a harmadik csoport a legszélesebb, akik nem feltétlenül érzik magukénak a fennálló szabályozást, ugyanakkor annak teljes eltörlését sem támogatják.

A helyzet a másik két tábornál sem olyan egyszerű, mint az elsőre tűnik. A status quot támogatók között egyre inkább az Európai Unió tesz szert nagy szerepre, mivel következetesen tud megfelelő szabályozást alkotni, ám így az Egyesült Államok által írt rendszerben gyakran sérülnek az USA érdekei (például a techcégek vonatkozásában). A változást kívánó államok

esetén a fő összetartó erő a jelenlegi rendszer elvetése jelenti, ám annak felváltására csak homályos terveik vannak. Kína bizonyosan jóval szigorúbban szabályozott internetet szeretne, mint Oroszország, amely geopolitikai céljainak egy lazán szabályozott rendszer felel meg igazán.

Ahogy a párosból Kína és az Egyesült Államok viszonya ellentmondásos, úgy igaz ez az EU-ra és Oroszországra is. Kapcsolatuk régóta konfliktusoktól terhelt, és az EU töredezett rendszere, a tagállamok bizonytalansága, illetve a fellépést szorgalmazó nagyobb államok és a kiegyezésben érdekelt kisebb államok közötti érdektelentét miatt viszonyuk ritkán egyértelmű. Barrinha amellett érvel, hogy bizonyos kérdésekben partnerként kell kezelni Oroszországot, ugyanakkor koherens fellépésre és megfelelő elrettentő erőre van szükség más esetekben (Barrinha 2018, 39. o.). Bizonyosnak tűnik, hogy a jelenlegi kiberszabályozási rendszer nem fog egyhamar változni, ugyanakkor ezt olyan korban alakították ki, amikor a kereskedelmi internet még csak gyerekcipőben járt. Át kell gondolni a jelenlegi szabályozási modellt, több szemléletmód beépítésével, és az új rendszernek egyensúlyt kell találnia számos kérdésben. Amíg ez nem történik meg, addig a konkuráló rendszerek fennállása biztosra vehető.

IRODALOMJEGYZÉK

- Barrinha, A. (2018): *Virtual Neighbors: Russia and the EU in Cyberspace* in Insight Turkey, 20. évf. 3. sz. 29-42. o.
- Bendiek, A. – Godehardt, N. – Schulze, D. (2019): The age of digital geopolitics Europe may well become the scene of a technological proxy war between the US and China. Interneten elérhető: https://www.ips-journal.eu/in-focus/chinas-new-power/article/show/the-age-of-digital-geopolitics-3593/
- Buono, L.(2012): *Gearing Up the Fight Again Cybercrime in the European Union: A New Set of Rules and Establishment of the European Cybercrime Centre (EC3)* in New Journal of European Criminal Law, 4. évf. 3. sz. 332–343. o.
- Dancă, D. (2015): *Cyber Diplomacy – A New Component of Foreign Policy* in Journal of Law and Administrative Sciences, 2. évf. 3. sz. 91–97. o.
- Douzet, F. (2016): *Geopolitika a kibertér megértéséhez* in Pintér, I. (szerk.) Műhelymunkák: A virtuális tér geopolitikája. Budapest: Geopolitikai Tanács Közhasznú Alapítvány, 21-42. o.
- Dornfeld, L. (2016): *A kibertér főbb nemzetközi és nemzeti szabályozásai* in Pintér, I. (szerk.) Műhelymunkák: A virtuális tér geopolitikája. Budapest: Geopolitikai Tanács Közhasznú Alapítvány, 43-88. o.
- Dornfeld, L. (2017): *Az elektronikus bizonyítékszerzés aktuális kérdései* in Kriminológiai Közlemények 77., 241-256. o.
- EDRi: *EU "e-evidence" proposals turn service providers into judicial authorities*. Interneten elérhető: https://edri.org/eu-e-evidence-proposals-turn-service-providers-into-judicial-authorities/ (Elérés dátuma: 2019.09.12.)
- Engelke, P. (2018): *Three ways the Fourth Industrial Revolution is shaping geopolitics*. Interneten elérhető: https://www.weforum.org/agenda/2018/08/three-ways-the-fourth-industrial-revolution-is-shaping-geopolitics/ (Elérés dátuma: 2019.09.12.)
- Geller, E. (2018): *China, EU seize control of the world's cyber agenda*. Interneten elérhető: https://www.politico.com/story/2018/07/22/china-europeglobal-cyber-agenda-us-internet-735083 (Elérés dátuma: 2019.09.12.)
- Lewis, J. A.. (2013): *Internet Governance: Inevitable Transitions*. Interneten elérhető: https://www.cigionline.org/sites/default/files/no4.pdf (Elérés dátuma: 2019.09.12.)

- Mueller, M. (2012): ITU Phobia: Why WCIT was derailed. Interneten elérhető: https://www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/ (Elérés dátuma: 2019.09.12.)
- O'Hara, K.– Hall, W. (2018) *Four Internets:The Geopolitics of Digital Governance*. Interneten elérhető: https://www.cigionline.org/sites/default/files/documents/Paper%20no.206web.pdf (Elérés dátuma: 2019.09.12.)
- Schulman, Cristina: *Legislation and legal frameworks on cybercrime and electronic evidence: Some comments on developments 2013–2018.* Interneten elérhető: http://www.unodc.org/documents/organized-crime/cybercrime/cybercrime-april-2018/SCHULMAN_Item_2.pdf (Elérés dátuma: 2019.09.12.)
- Schwab, K. (2016): *The Fourth Industrial Revolution: what it means, how to respond*. Interneten elérhető: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ (Elérés dátuma: 2019.09.12.)
- Warken, C (2019): *A kiberbűnözés elleni küzdelem új fejleményei az Európai Unióban* in Farkas, Á.– Dannecker, G. – Jacsó, J. (szerk.): Az Európai Unió pénzügyi érdekei védelmének büntetőjogi aspektusa - különös tekintettel az adócsalás, a korrupció, a pénzmosás és a büntetőjogi compliance nemzeti szabályozására, valamint a kiberbűnözésre, Budapest: Wolters Kluwer, 2019. 427-431. o.
- Zhang, X, (2013) *Establishing Common International Rules to Strengthen the Co-Operation of Cyber Information Security* in China Legal Science, 12. évf. 1. sz. 121–139. o.