DOI: 10.59851/imr.13.1.12 IN MEDIAS RES 2024/1. • 12, 222–235

Egyes német internetszabályozási megoldások védelmi és biztonsági szempontú áttekintése

VIKMAN LÁSZLÓ*

A tanulmány áttekintést ad a Németországban az interneten felmerülő fenyegetésekkel szemben alkalmazott, széles körben értelmezett biztonsági igazgatási jogkörökről és tevékenységekről. Az online terrorista tartalmakra, az ifjúságvédelemre, a tiltott szerencsejátékra, a közösségi médiára és a dezinformációra vonatkozó tematikus szabályozás mellett a hagyományosan védelmi-biztonságinak tekinthető szervezetek – rendészet, nemzetbiztonság és hadsereg – internetes fenyegetésekkel szembeni tevékenységére is kitérve veszi sorra a különböző szervezeti és szabályozási megoldásokat, megközelítési irányokat és kezelési stratégiákat. Zárásként ezek elméleti alkalmazási lehetőségeit elemezve jut arra a következtetésre, hogy a kibertér kihívásai egy korszerű államszervezettől magas szintű és rugalmas alkalmazkodást követelnek meg, és az egyes biztonsági fenyegetéseket differenciáltan, a puhább megközelítésektől a keményebb, bírságolási és büntetőjogi megoldásokig terjedő széles eszközrendszerrel érdemes kezelni.

Kulcsszavak: internetszabályozás, médiaigazgatás, közösségi média, dezinformáció, hatósági hatáskörök

Some German internet governance solutions from a defence and security perspective overview

The study provides an overview of the broadly understood security management powers and activities applied in Germany against threats arising on the Internet. In addition to the thematic regulation on online terrorist content, youth protection, illegal online gambling, social media and disinformation, it also addresses the activities of organizations traditionally considered to be defense and security – police, national security and army – against internet threats, and takes a turn at various organizational and regulatory solutions, approaches and treatment strategies. Finally, by analyzing their theoretical application possibilities, he comes to the conclusion that the challenges of the cyberspace require a high-level and flexible adaptation from a modern state organization, and it is worth handling individual security threats in a differentiated manner, with a wide range of tools ranging from softer approaches to harsher fines and criminal law solutions.

Keywords: internet regulation, media governance, social media, disinformation, responsibilities of authorities

* Tudományos segédmunkatárs, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar.

1. Bevezetés

A kibertér a számtalan szereplője által nyújtott, egyre sokszínűbb szolgáltatásával egyre dominánsabb szerepet tölt be a gazdasági és kereskedelmi folyamatokban, a hétköznapi kapcsolattartásban, a munkavégzésben (különösen a koronavírus-járvány által is katalizált távmunkában), a szórakozásban, a tanulásban, az általános tájékoztatásban és tájékozódásban, valamint a közvélemény és a közbeszéd formálásában. E tevékenységek gyorsan és több platformon, több terjesztési csatornán keresztül zajlanak – ezek tere az egyszerű közvetítő közegtől a fórumon át a csak a kibertérben értelmezhető innovációkig terjed (lásd például a *non-fungible token*eket). A kibertérben zajló valós értékű gazdasági tranzakciók és személyi interakciók, az azokat megjelenítő és hordozó információk, az adatok vagy akár egyszerűen az elérhető és manipulálható figyelem ugyanannyira célpontja ártó szándékú, kriminális, ellenséges, szervezett vagy alkalomszerűen fellépő állami és nem állami szereplőknek, mint a hagyományos, valós térben.

Ez a közeg olyan szabályozási feladatokat támaszt a polgárait és a társadalmi rendet védeni kívánó, alkotmányos szerepét betöltő államokkal szemben, amelyekre a magas szintű komplexitás, a nemzetközi elemek és a különböző alapjogok érintettsége kiemelten jellemző. Az is kihívást jelent, hogy a hagyományos igazgatási eszközrendszerekkel adott válaszok eddig ritkán látott gyorsasággal avulnak el. Az elmúlt két-három évtizedben – párhuzamosan az információs és kommunikációs technológiai szektor teljes spektrumának robbanásszerű evolúciójával – folyamatosan látjuk, hogy új innovációk, diszruptív technológiák gyorsan képesek lehetnek bármely szofisztikált szabályozási rend meghaladására, ezzel újabb lépésekre kényszerítve a jogalkotókat.[1]

Az internet egyes védelmi és biztonsági szabályozási kérdéseinek szomorú felértékelődését részben e szerepnövekedés, a mindenhol jelenlévőség és jelentős részben a geopolitikai rend stabilitásának megbomlása hozta magával. Az orosz–ukrán háború kapcsán is mára mindennapi valósággá vált hibrid hadviselés, a tájékoztatás tényszerűségét és objektivitását kikezdő propaganda és dezinformáció, a nemzetközi terrorszervezetek nyomásgyakorló törekvései és a szervezett bűnözés térnyerése az internet és a tágabb értelemben vett média minden zugában tetten érhető, nemcsak a közösségi oldalakon, hanem a hagyományosnak tekinthető tévécsatornákon is.[2] Ezek a biztonsági kihívások együtt járnak az állami szervek kontrollálási lehetőségeinek csökkenésével, hiszen összevetve az akár a kora 20. századi nyomtatott sajtó- és postaellenőrzés

---

1 A téma védelmi-biztonsági vonatkozásaihoz magyar nyelven lásd például Kelemen Roland – Farkas Ádám: A közösségimédia-platformok és a hibrid konfliktusok kapcsolata. *In Medias Res,* 2022/1., 96–108.; Farkas Ádám: A multidiszciplinaritás helye, szerepe a védelem és biztonság szabályozásának és szervezésének komplex kutatásaiban. *Közjogi Szemle,* 2021/4., 22–28.; Farkas Ádám: Kibertér művelet: hírszerző, rendészeti és katonai műveletek elegye? Gondolatok az angol National Cyber Force kapcsán. *Military and Intelligence CyberSecurity Research Paper,* 2021/1., 1–8.; Farkas Ádám – Spitzer Jenő: Az információs korszak és az állami reziliencia egyes kérdései. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2021/18., 1–27.; Kelemen Roland – Mihály Laura Dominika: A kibertér és a psziché ütközéspontjai mint a 21. századi reziliencia kulcskérdése. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/14., 1–31.; Kelemen Roland: A közösségimédia-platformok tartalomszűrő tevékenységének árnyoldalai. In Glavanits Judit – Papp Nikolett (szerk.): *A fogyasztóvédelem egyes aktuális kérdései: a békés vitarendezés lehetőségei a 21. század technológia-intenzív közegében.* Budapest, Gondolat, 2022, 65–81.

2 Például a Russia Today német nyelvű adásának németországi betiltása kapcsán lásd Deutsche Welle und RT DE – Auslandsrundfunk im Medienkrieg. *Deutsche Welle,* 2022. február 5., https://bit.ly/4bEt3RW.

módszereivel, az interneten található globális és fragmentált médiakínálat, kommunikációs platform és csatorna, az anonimitás megőrzésének számos lehetősége (a jog oldaláról adott esetben az attribúció nehézsége) és az internet alaparchitektúrájából fakadó decentralizált jelleg mind ellene hat egy koncentrált és mindenható cenzúrának vagy tartalomellenőrzésnek.[3]

Németország az Európai Unió egyik vezető államaként és gazdasági motorjaként meghatározó szerepet tölt be a 21. században már elsődleges fontosságú kibertér gazdasági, kereskedelmi és médiaszabályozásában is. A német jogalkotónak – történelméből is fakadóan – a média szervezése és igazgatása vonatkozásában a liberális és a totalitárius elemeket is ismerve kell adekvát megoldásokat találnia arra,[4] hogy egy jogállami elveken, az emberi szabadságjogok tiszteletben tartásán, piacgazdaságon és innováción alapuló társadalom hogyan küzdhet meg a technológiai fejlődés hozta újfajta problémákkal. A jelen tanulmányban – annak relatíve szűk terjedelmi keretei miatt – arra keresünk példákat, hogy a meglehetősen kiterjedt és szerteágazó hatályos német szabályozás és államszervezet milyen sajátos megoldásokat alkalmaz kifejezetten az interneten felmerülő egyes védelmi és biztonsági válaszokat is megkövetelő kockázatokkal kapcsolatban, így különösen a terrorista tartalmak, a médiaigazgatás terén az ifjúságvédelem, a tiltott szerencsejátékok, a közösségi média és a dezinformáció tárgyában.[5]

2. A német médiaigazgatás tematikus szervezeti és szabályozási háttere

A német alaptörvény (Grundgesetz) alapvető jogként tételezi a sajtó- és a véleménynyilvánítás szabadságát, a cenzúrát pedig kifejezetten tiltja. A törvény 5. cikk (1) bekezdése kimondja: „Mindenkinek joga van véleményét szóban, írásban és képi formában szabadon kifejezni és terjeszteni, valamint az általánosan hozzáférhető információforrásokból tájékozódni. A sajtószabadság, valamint a rádión és a filmen keresztüli tudósítás szabadsága biztosított. Nincs cenzúra." Azaz a tartalom – így az online is – alapvetően szabadnak számít. Ebből fakad a főszabály szerint nem korlátozható véleménynyilvánítással kapcsolatos összes rendelkezés. Fontos, hogy az 5. cikk (1) bekezdése kiterjed az információszabadságra is, amely szerint mindenkinek lehetősége kell legyen arra, hogy szabadon tájékozódjon általánosan hozzáférhető forrásokból. E két alkotmányos rendelkezés eredményeként az internet bizonyos tartalmaihoz való hozzáférés korlátozása, megakadályozása alapvető jogok sérelmét jelentheti, ugyanakkor az 5. cikk (2) bekezdése szerint ezek a jogok törvényben korlátozhatók, például az ifjúság és a személyhez fűződő jogok védelme érdekében.

---

3 Eltekintve természetesen az autoriter államok saját nemzeti hálói vagy azok leválasztási lehetőségétől, lásd Kína és Oroszország példáját.

4 A témához lásd Victor Klemperer: *A Harmadik Birodalom nyelve – egy filológus feljegyzései* (ford. Lukáts János). Budapest, Ampersand, 2021.

5 Háttérként lásd többek között Udo Branahl: *Medienrecht – Eine Einführung.* Wiesbaden, Springer, 2019, https://doi.org/10.1007/978-3-658-27381-1; Jan Krone (szerk.): *Medienwandel kompakt 2017–2019 – Schlaglichter der Veränderung in Kommunikation, Medienwirtschaft, Medienpolitik und Medienrecht. Ausgewählte Netzveröffentlichunge.* Wiesbaden, Springer, 2019, https://doi.org/10.1007/978-3-658-27319-4; Peter Bühler – Patrick Schlaich – Dominik Sinner: *Medienrecht – Urheberrecht, Markenrecht, Internetrecht*. Berlin, Springer Vieweg, 2017, https://doi.org/10.1007/978-3-662-53920-0.

A médiaszabályozás mint szabályozási tárgykör a köz- és a magánjog számos területéről megközelíthető, meglehetősen szerteágazó terület. A közjogi alapoktól, például a sajtó- és az információszabadságtól, a személyes adatok védelmétől kezdve a frekvenciagazdálkodás szabályain át a verseny- vagy a büntetőjogig, a magánjogi témákban pedig a személyhez fűződő jogoktól a szerzői jogig olyan mértékben összetett, hogy gondozására és felügyeletére minden államban jellemzően több szervezet kap feladat- és hatáskört. A német államszervezetben sem találunk egyetlen, minden felügyeleti lehetőséget koncentráló és az online médiát is ellenőrző sajtóigazgatási szervet – szét vannak osztva a szükség esetén alkalmazandó, egy korszerű jogállami közegben és a 21. századi médiapiaci környezetben a társadalom és a közösség védelméhez elengedhetetlen intézkedési jogkörök. Ezek és újabb változataik – jelentős részben az internet generálta nyomás miatt egyre gyorsabban, az EU jogalkotása miatt pedig egyre sztenderdizáltabban – jelennek meg, ami a védelmi és biztonsági szempontokra is igaz. A következőkben ennek apropóján lesz szó a német államszervezet néhány jelentős szervének szerepéről és a kapcsolódó jogszabályokról.

2.1. Online terrorista tartalmak[6]

A szövetségi hálózati ügynökség mellett a szövetségi bűnügyi rendőrség (Bundeskriminalamt) is felelős az online terrorista tartalmak elleni küzdelemről szóló szabályozás végrehajtásáért – a két hatóság közötti feladatmegosztást törvény határozza meg.[7] Ennek megfelelően a szövetségi bűnügyi rendőrség rendeli el és ellenőrzi a terrorista tartalmak eltávolítását. A német megközelítés szerint, mivel a terrorista tartalom büntetőjogilag releváns, csak a szövetségi bűnügyi rendőrség rendelheti el annak eltávolítását.

A szövetségi hálózati ügynökség (Bundesnetzagentur) bonni székhelyű, szabályozási feladatokkal is felruházott hivatal, a szövetségi gazdasági tárcához tartozik, és az elsődlegesnek tekinthető versenyjogi és fogyasztóvédelmi szempontok mellett igazgatásiak alapján is felügyeli a kiemelt hálózatos szolgáltatásokat. Hatásköre kiterjed az elektromos hálózatra, a földgázvezeték-rendszerre, a telekommunikációra, a postára és a vasutakra. Biztonsági szempontból az egyik kiemelt feladata az online terrorizmus elleni küzdelem. A szövetségi hálózati ügynökség kompetenciája – az online terrorista tartalom terjesztésével szembeni fellépésről szóló, egységesített szabályokat tartalmazó uniós rendelet 5. cikke alapján[8] – a szolgáltatók intézkedéseinek nyomon követésére és szükség esetén azok módosíttatására terjed ki.

---

6 A témához lásd Andrea Keller et al.: *Die Attraktion des Extremen Radikalisierungsprävention im Netz.* Frankfurt, Wochenschau, 2021, https://doi.org/10.46499/1649; Sally Hohnstein – Maruta Herding: *Digitale Medien und politisch-weltanschaulicher Extremismus im Jugendalter. Erkenntnisse aus Wissenschaft und Praxis*. München, Deutsches Jugendinstitut, 2017; Josephine B. Schmitt et al.: *Propaganda und Prävention.* Wiesbaden, Springer, 2020, https://doi.org/10.1007/978-3-658-28538-8; Mahmud El-Wereny: *Radikalisierung im Cyberspace. Die virtuelle Welt des Salafismus im deutschsprachigen Internet.* Bielefeld, Transcript, 2020, https://doi.org/10.1515/9783839452066.

7 Gesetz zur Durchführung der Verordnung (EU) 2021/784 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte.

8 Az Európai Parlament és a Tanács (EU) 2021/784 rendelete (2021. április 29.) az online terrorista tartalom terjesztésével szembeni fellépésről.

A rendelet az EU területén tárhelyszolgáltatást nyújtó cégekre vonatkozik, függetlenül attól, hogy azok fő üzleti tevékenysége a tagállamokban folyik-e. Az 5. cikk alapján a szolgáltatóknak gondoskodniuk kell saját tárhelyükön a tiltott tartalmak terjesztésének megakadályozásáról. A szolgáltatók maguk dönthetik el, hogy milyen intézkedéseket vezetnek be, de körültekintően és diszkriminációmentesen kell eljárniuk, figyelembe kell venniük a felhasználók jogait és jogos érdekeit, így különösen a véleménynyilvánításhoz, a tájékozódás szabadságához, a magánélethez és a személyes adatok védelméhez való jogot, intézkedéseiknek pedig hatékonyaknak, célzottaknak és arányosaknak kell lenniük. Ha az illetékes hatóságok tudomást szereznek terrorista tartalom internetes közzétételéről,[9] elrendelik annak eltávolítását vagy hozzáférhetetlenné tételét, amit a szolgáltatóknak egy órán belül el kell végezniük. Ha a szolgáltatók ezt elmulasztják vagy rendszeresen megsértik az előírásokat, akkor pénzbírsággal sújthatók. Az uniós rendelet 18. cikke, valamint az online terrorista tartalmak elleni küzdelemről szóló német törvény 6. cikke szerinti szankciók kiszabása a szövetségi hálózati ügynökség feladata – ha a szolgáltatók nem tesznek eleget kötelezettségeiknek, akár ötmillió eurós bírságot is kaphatnak. A világszinten 125 millió eurót meghaladó éves forgalmú jogi személyek esetében az előző pénzügyi év forgalmának négy százalékáig terjedő szankció is lehetséges.

2.2. Médiaigazgatás és ifjúságvédelem

Németországban 14 tagállami médiahatóság működik, mivel a médiaszabályozás tagállami kompetencia. Ezek a hatóságok a Medienanstalten elnevezésű ernyőszervezetben egy államközi médiaszerződés égisze alatt hangolják össze tevékenységüket,[10] és a szövetségi államok nevében közösen dolgoznak központi feladatokon és projekteken, négy központi bizottságban hozva meg a döntéseket. Ez biztosítja, hogy az országos magánrádió- és televízióadók, valamint a felhasználói felületek, médiaplatformok és médiaközvetítők szolgáltatói azonos előírások szerint működjenek, és a médiahatóságok egységes álláspontot képviseljenek az európai médiapolitikában.

Az engedélyezési és felügyeleti bizottság (Kommission für Zulassung und Aufsicht)[11] központilag dönt a műsoraikat országosan sugározni kívánó magántévé- és rádióadók engedélykérelmeiről, ideértve a teljesen új műsorszolgáltatók jóváhagyását, de a meglévő engedélyek meghosszabbítását is. Dönt továbbá a műsorszolgáltatási engedéllyel rendelkező társaságok ügyvezetőinek, valamint tulajdonosi szerkezetének változásáról is. Azt is szabályozza, hogyan kezeljék a szolgáltatók jogsértéseit, ezért a bizottság értékeli a műsorelvek, az újságírói gondossági kötelezettség és a reklámszabályok esetleges megsértését. Az eljárásokat szakbizottságokban folytatják le, a bizottság határozatait az illetékes állami médiahatóságok készítik elő és hajtják végre, a szükséges koordinációt pedig a berlini közös iroda végzi. Az internethez már közvetve kapcsolódó feladatként a platformszabályozás is a bizottság portfóliójába tartozik. Ezen a terü-

9 Hazánkban a Nemzeti Média- és Hírközlési Hatóság feladatköre, lásd 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről 12/B. §.

10 Staatsvertrag zur Modernisierung der Medienordnung in Deutschland (Medienstaatsvertrag, MStV).

11 A bizottság feladatkörét részletesen az MStV 105. §-a tartalmazza.

leten a cél a nyílt hozzáférés biztosítása a tartalmakhoz (programokhoz), valamint a szolgáltatók közötti tisztességes verseny és a bejutási feltételek megteremtése. Klasszikus médiaigazgatási feladatként a bizottság bonyolítja le a sugárzott digitális rádió- és televíziópályázatokat is.

Az európai jog, különösen az audiovizuális médiaszolgáltatásokról szóló irányelv[12] tartalmaz előírásokat a kiskorúak védelmének biztosítására a televízióban és a lekérhető szolgáltatásokban. Németországban a tematikus szabályozás az ifjúságvédelmi törvényen (Jugendschutzgesetz) és az államközi ifjúságvédelmi szerződésen (Jugendmedienschutz-Staatsvertrag) alapul. Az ifjúságvédelmi feladatokhoz sorolható a médiatartalmak kockázati potenciáljának felmérése és nyilvános terjesztésének szabályozása. Az ifjúságvédelmi bizottság (Kommission für Jugendmedienschutz) a jogi kritériumok mellett pedagógiai, pszichológiai és más társadalomtudományi kutatások eredményei alapján ellenőrzi (az interneten is), hogy megfelelnek-e a médiatartalmak a társadalmilag elvárt értékeknek és normáknak. A prevenció mellett a fiatalok médiához kapcsolódó készségeinek, kompetenciáinak fejlesztése is egyre nagyobb figyelmet kap, ami a tájékozottságuk növelésével a védelmükben tett lépésként is értékelhető.[13]

2.3. Tiltott szerencsejáték

Az online szerencsejáték-szolgáltatókkal szemben alkalmazható intézkedéseket az ilyen szolgáltatások szövetségi szabályozására létrehozott, a szerencsejátékról szóló államközi szerződés tartalmazza (Glücksspielstaatsvertrag). A törvény 9. § (1) bekezdés 3. pontja szerint az illetékes tagállami hatóság adhat engedélyt az online kaszinó, póker és sportfogadási szolgáltatások nyújtására. Részben a több szövetségi államban is reklámoztató, szolgáltatásokat nyújtó szervezetek miatt a tagállami szerencsejáték-felügyeleti hatóságok létrehoztak egy szövetségi szintű közös hatóságot is. A törvény 4a és 4b §-a tartalmazza az online játékok feltételeit, engedélyezési rendjét és a szolgáltatók különös kötelezettségeit. A törvény szabályozza a kiskorúak szerencsejátékokhoz való hozzáférését, a megszervezhető játékok típusait, a szervezők bejelentési kötelezettségeit, valamint a reklámozás szabályait (például tilosak a szenvedélybetegek kihasználását célzó, a túlzottan figyelemfelkeltő és a további játékra csábító felhívások). A 6. § alapján a szolgáltatóknak a fiatalok és a szenvedélybetegek védelmét célzó társadalmi koncepciót is ki kell dolgozniuk.

A törvény 6e §-a további, az ifjúságot és a szerencsejátékoktól eltiltottakat védő szabályokat ad meg. A kiskorúak és az eltiltott játékosok kizárását az azonosítás és a hitelesítés megfelelő technikai eljárásaival kell biztosítani. A szervezési engedély előírhat az azonosítás és a hitelesítés végrehajtására vonatkozó követelményeket, különös tekintettel arra, hogy az abban megjelölendő rendszeres időközönként a szokásos hitelesítési módtól eltérőket kell alkalmazni.

---

12 Az Európai Parlament és a Tanács 2010/13/EU irányelve (2010. március 10.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról.

13 Lásd például a *medienanstalten* tematikus jelentését az ifjúságvédelem, a médiakonpetencia és a dezinformáció vonatkozásában tett intézkedésekről, *Fakt oder Fake? Jugendschutz, Medienkompetenz und Desinformation Maßnahmen, Projekte und Forderungen aus Sicht der Landesmedienanstalten.* Berlin, Medienanstalten, 2022, https://bit.ly/3wRPT9S.

Az internetes szerencsejátékokban használt véletlenszerű generátorok megfelelő működését az első használat előtt, majd azt követően évente legalább egyszer, az engedélyes költségére, egy később kijelölendő, független szakértői testületnek kell ellenőriznie, az eredményt pedig közölni kell az illetékes engedélyező hatósággal.

A nyilvános internetes szerencsejátékokat olyan internetes domén alatt kell kínálni, amelynek legfelső szintű, országspecifikus doménje a *.de.* Az engedélyezett doménnév alatt elérhető honlap kezdőlapján jól látható helyen el kell helyezni, hogy a szerencsejátékban 18 éven aluliak nem vehetnek részt, és hogy az engedélyes rendelkezik az illetékes szerencsejáték-felügyeleti hatóság engedélyével és annak felügyelete alatt áll. Minden információnak, amelyet az engedélyesnek a játékosok rendelkezésére kell bocsátania, német nyelven elérhetőnek kell lennie a játékajánlatot tartalmazó internetes doménjén, és elérhetőnek kell lennie a domén minden oldaláról. A játékban való részvételkor a játékosokat haladéktalanul tájékoztatni kell a szerencsejáték kockázatairól és esetleges negatív társadalmi következményeiről.

2.4. Közösségi média

A közösségi hálózatokon történő jogérvényesítés javításáról szóló hálózati végrehajtási törvény (Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, NetzDG) a közösségi hálózatokat célozza és az értesítési és eltávolítási eljárással kapcsolatos tapasztalatokra épít. Ahogyan az a törvény tervezetének indokolásában olvasható, a szövetségi kormány gyűlöletbeszéddel és más illegális tartalommal szembeni munkacsoportja által 2015-ben végzett vizsgálatok egyik eredménye az volt, hogy a legtöbb közösségi hálózat nem teljesítette megfelelően a (törlési) kötelezettségeit. Az illegális tartalmak többnyire a közösségi platformokon maradnak. Az iparág két vezető vállalata, a Facebook és a Twitter, a tiltott tartalmak mindössze 39 és 1%-át távolította el, míg a YouTube 90%-os arányt ért el. A közösségi hálózatokon megjelenő illegális tartalmak kezelésében az átláthatóság problémáját is azonosították. Ennek javítása érdekében röviddel a 2017-es szövetségi választások előtt elfogadták a NetzDG-t és 2018 januárjában hatályba léptették. A világosan felépített törvény négy területre oszlik: az alkalmazására, a közösségi hálózatok bejelentési kötelezettségére, az illegális tartalommal kapcsolatos panaszok kezelésére és a közigazgatási szankciókra.[14]

A „lex Facebooknak" aposztrofált törvény legfontosabb szabálya, hogy kötelezi a Németországban több mint kétmillió felhasználót számláló közösségimédia-platformokat, hogy a közzétételt követő 24 órán belül távolítsák el az „egyértelműen illegális" tartalmat és hét napon belül minden jogsértő tartalmat – ellenkező esetben 50 millió euróig terjedő bírságot szabhatnak ki rájuk. A törölt tartalmat ezt követően legalább tíz hétig meg kell őrizni. A NetzDG alapján azok a szolgáltatók, amelyekhez egy naptári évben több mint száz panasz érkezik illegális tartalommal kapcsolatban, kötelesek félévente jelentést készíteni arról, hogy miként kezelik az

[14] Yunfei Zha: *Die Regulierung rechtswiedriger Infromationen im Internet unter besonderer Berücksichtigung von Sperrmassnahmen gegen Access-Provider – Vergleich zwischen Deutschland und China.* Doktori értekezés, Münster, Universität Münster, 2019, 85.

ilyen panaszokat, és azt a szövetségi közlönyben és a saját honlapjukon legkésőbb a félév lejárta után egy hónappal közzé kell tenniük.

A szolgáltatóknak hatékony és átlátható eljárással kell rendelkezniük az illegális tartalommal kapcsolatos panaszok kezelésére. Az ilyen panaszok benyújtására könnyen felismerhető, közvetlenül elérhető és használható, valamint a tartalom megtekintésekor folyamatosan hozzáférhető eljárásokat kell biztosítaniuk a felhasználóknak. A közösségi hálózatok szolgáltatói kötelesek értesíteni a szövetségi bűnügyi hivatalt az esetleges bűncselekmények üldözésének lehetővé tétele érdekében, ha a bejelentést illegális tartalommal kapcsolatban tették, ha a szolgáltató illegális tartalmat távolított el vagy letiltotta az ahhoz való hozzáférést, valamint az olyan tartalmakról is, amelyeknél arra utaló jelek vannak, hogy súlyos büntetőjogi tényállások valamelyik elemét valósíthatják meg.[15] Az értesítésnek tartalmaznia kell a tartalmat és – ha elérhető – azt az időpontot, amikor a tartalmat megosztották vagy nyilvánosan hozzáférhetővé tették, megadva az alapul szolgáló időzónát, a tartalmat megosztó vagy nyilvánossá tevő felhasználó nevét és, ha rendelkezésre áll, az IP-címét, a portszámot és az utolsó hozzáférés időpontját, feltüntetve az alapul szolgáló időzónát.

2.5. Dezinformáció

A dezinformáció, azaz a *fake news,* az összeesküvés-elméletek és a célzott befolyásoló propaganda terjesztése a hibrid konfliktusok és a multipolaritás felé mozduló nemzetközi kapcsolatokban egyre inkább jelen lévő, globális jelenség, és olyan kihívás, amelyre minden államnak meg kell találnia a saját válaszait. Ezeknek az üzeneteknek az egyik legfontosabb csatornája – nem utolsósorban a cenzúra teljes hiánya és az anonimitás lehetősége miatt –a kibertér, benne főként a közösségi média. Emiatt a dezinformáció egyes jelenségeinek kezeléséhez eszközöket ad a NetzDG, azonban a meghamisított, részben elhallgatott vagy kriminális szempontból nem értékelhető, de elferdített információk terjesztését nem gátolhatja meg. Németország is nagy figyelmet szentel ennek a nem csekély védelmi és biztonsági kockázatokkal járó fenyegetésnek. Az egészségügyi tárca számára – akárcsak hazánkban – komoly kihívást jelentett a koronavírus-járvány kapcsán terjedő, sok forrásból és számos témában megjelenő káros tartalom, ami ellen széles körű tájékoztatással igyekeztek fellépni.[16] A téma kormányzati szinten elsősorban a külügyminisztérium (Auswärtiges Amt), a szövetségi sajtóiroda (Bundespresseamt) és a szövetségi belügyminisztérium (Bundesministerium des Innern und für Heimat) számára jelent feladatot. Ezek a tárcák figyelemmel kísérik az információs teret, az ott keringő hamis vagy félrevezető, téves információkat, aktuálisan főként az orosz–ukrán konfliktussal kapcsolatban.[17] Német-

[15] Például alkotmányellenes vagy terrorista propagandát terjesztenek, alkotmányellenes vagy terrorista szimbólumokat használnak, súlyos állam ellenes erőszakos cselekményt készítenek elő, a köznyugalom megzavarása bűncselekményekkel fenyegetnek, szervezett bűnöző vagy terrorista csoportokat szerveznek meg, uszítók, gyermekpornográfiát, az élet, a szexuális önrendelkezés, a testi épség vagy a személyi szabadság elleni fenyegetést tartalmaznak.

[16] Lásd például *Faktenchecks zur Corona-Schutzimpfung. Die Bundesregierung,* https://bit.ly/3QOUYGM.

[17] *Verfassungsschutz informiert* über *Aktivitäten russischer Nachrichtendienste. Die Bundesregierung,* https://bit.ly/3QRBhOB.

ország a kérdésben erősen támaszkodik az uniós és más együttműködésekre:[18] a dezinformáció elleni közös cselekvési terv,[19] az EUvsDisinfo kampány,[20] az online platformok számára készített, 2022-es szigorított viselkedési kódex[21] mind olyan elem, amelynek kidolgozásában és működtetésében fontos szerepet vállalt. További kezdeményezést jelentenek a hamis információk elleni küzdelemben az ún. tényellenőrző vállalkozások, amelyekre szintén van német példa, osztrák együttműködéssel.[22]

3. A német védelmi-biztonsági szervezetrendszer és feladatai a kibertérben

A hírszerzésért felelős Bundesnachrichtendienst a Kancelláriához tartozik, részt vesz a gazdaságvédelemben és a nemzeti kibervédelmi központ (Nationales Cyber-Abwehrzentrum)[23] tevékenységében, valamint veszély észlelése esetén figyelmezteti az érintett belföldi aktorokat, hogy azok megtehessék a megfelelő ellenintézkedéseket. Feladata az, hogy korai előrejelzéseket nyújtson a Németország kritikus infrastruktúráját érintő kockázatok és az az ellen irányuló támadások idejében való azonosításához. Elsősorban a német érdekek elleni külföldi tevékenységek elhárítására törekszik, de a kibertámadások, -kémkedés és -szabotázs felderítése is feladata. Felhatalmazással és technikai lehetőségekkel rendelkezik a nemzetközi adatforgalom stratégiai szempontok szerinti vizsgálatához.

Épp e forgalomfigyelő nemzetbiztonsági tevékenysége került alapjogi viták fókuszába 2020-ban. A frankfurti DE-CIX a világ legforgalmasabb internetcsomópontja,[24] napi 91 terabit feletti globális adatforgalommal, amelyet a hírszerzés is figyelemmel kísért – sokáig lényegi korlátozások nélkül. Azonban a német szövetségi alkotmánybíróság 2020. május 19-i döntésében kimondta, hogy a külföldi állampolgárok külföldi telekommunikációs forgalmát ugyanúgy megilleti a telekommunikációs titok védelme, mint a német állampolgárokét, ezért a hírszerző szolgálatnak le kellett állítania az addig folytatott kiterjedt megfigyelési programját. Emellett az alkotmánybírósági határozat 2021 végéig adott időt a törvényhozásnak az új, alkotmánykonform megfigyelési szabályozás megalkotására.[25]

A szövetségi információtechnikai biztonsági hivatal (Bundesamt für Sicherheit in der Informationstechnik) feladata az ország információtechnikai biztonságának erősítése. A ható-

18 Mint például a G7-ek között együttműködés a témában, https://bit.ly/4ajLYjW.

19 Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: https://bit.ly/3wDfcN0.

20 EUvsDisinfo: https://bit.ly/3wtjaYA.

21 2022. évi megerősített gyakorlati kódex a dezinformáció visszaszorításáról: https://bit.ly/4aoVvGj.

22 German-Austrian Digital Media Observatory: https://bit.ly/4bnqdBd.

23 A központ 2011 óta működik, és a német kiberbiztonságban érintett kormányzati szervezetek együttműködése, információ- és tapasztalatcsere, közös értékelés-elemzés, folyamatos egyeztetések fóruma és központja.

24 Jeder kann einen Cyber-Angriff für weniger als 18 Euro beauftragen. *The European,* 2020. június 6., https://bit.ly/4bJ6Wtw.

25 Ausland-Ausland-Fernmeldeaufklärung nach dem BND-Gesetz verstößt in derzeitiger Form gegen Grundrechte des Grundgesetzes. Bundesverfassungsgericht, 2020. május 19., https://bit.ly/4bouzrA.

ság nagy technikai szakértelemmel ösztönzi az információ- és a kiberbiztonságot a közigazgatásban, a gazdaságban és általában a társadalomban különböző kooperációkon és kezdeményezéseken keresztül. Országszerte rendelkezik kirendeltségekkel a regionális beágyazottság érdekében, emellett 2019-ben kapott egy második központot Drezdában, majd egy kifejezetten a mesterséges intelligenciára összpontosító harmadikat is Saarbrückenben. A hivatal a belügyminisztérium alá tartozik, és többek között otthont ad a számítógépes vészhelyzetekre reagáló csoportnak (CERT-Bund). Amellett, hogy közel nemzetbiztonsági felhatalmazásokkal működik, és többek között az állami elektronikus információbiztonság és kiberbiztonsági tanúsítás központi szereplője, minden évben széles fókuszú részletes jelentést tesz közzé a német kibervédelem helyzetéről.

A szövetségi alkotmányvédelmi hivatal (Bundesamt für Verfassungsschutz) elsősorban arra fókuszál, hogy a szélsőségesek, a terroristák és más államok hírszerzése milyen új technikai lehetőségeket tud kihasználni Németországban kémkedés, politikai dezinformáció vagy számítógépes szabotázs céljából. A hivatal igyekszik felderíteni és elhárítani az állami és a magáncélpontok elleni kibertámadásokat is. A belügy irányítása alatt áll, szerepet vállal a gazdaságvédelemben és részt vesz a nemzeti kibervédelmi központ munkájában.

A szövetségi bűnügyi hivatal (Bundeskriminalamt) szintén a belügyminisztérium irányítása alatt áll, és magasan szervezett, kiemelt jelentőségű bűnügyek kapcsán a kibertérben is tevékeny, sőt a kibertérre specializálódott operatív bűnüldözési részleggel is rendelkezik, ahol az ilyen bűncselekményekkel kapcsolatos kompetenciák és információk összefutnak. Szintén részt vesz a nemzeti kibervédelmi központ munkájában, és képviseli Németországot az Europolban.

Miután 2017 áprilisában a kiberteret a hadsereg legújabb szervezési területeként, doménként azonosították (összhangban a NATO megközelítésével, a szárazföld, a víz, a levegő és az űr mellett), 2021-es határidővel kialakították a szövetségi haderők új feladatának ellátásához szükséges szervezeti hátteret is. A doménfelelősség keretében el kell látni a hadsereg belföldi és missziós információtechnológiai rendszereinek védelmét, biztosítani kell a szükséges felderítést, az üzembiztonságot és a geoinformációs adatokat, valamint a szakterületi kapcsolattartást más szervekkel. A nemzeti szintű védelmi képesség fejlesztése és megóvása szempontjából a szövetségi katonai elhárítás hivatala (Militärischer Abschirmdienst) kulcsfontosságú a haderők támogatásában, védelmében és stabilitásának erősítésében. A hadsereg kiberképességeit egy vezető és két alárendelt parancsnoksághoz osztották be. A kiber- és információs tér parancsnokság (Kommando Cyber- und Informationsraum) háromcsillagos tábornoki vezetési szint, legfőbb feladata a kiber- és az információs tér strukturálása, ennek keretében stratégiai felderítést végez, ellátja a hadsereg geoinformációs tevékenységét és az operatív kommunikációt. Parancsnoka helyetteseként koordinálja a nemzeti kibervédelmi központ működését. Az információtechnikai parancsnokság (Kommando Informationstechnik) hat zászlóaljba szervezve biztosítja a hadsereg műveletei alatt az információtechnológiai eszközök működését, és külön szakértői csoportok rendelkezésre bocsátásával nyújt szükséges reakcióképességet kibertámadás esetén. A stratégiai felderítési parancsnokság (Kommando Strategische Aufklärung) feladata a hadsereg információigényének kielégítése műholdas képalkotással, távérzékeléssel és elektronikai felderítéssel szerzett adatokkal, emellett az elektronikai harc és az objektumanalízis. Folyamatosan fejleszti hálózati műveleti képességeit és üzemelteti a hadsereg kiberműveleti központját.

A fentebb már említett szövetségi katonai elhárítási hivatal Németország katonai nemzetbiztonsági szolgálata és tagja a nemzeti kibervédelmi központnak. 2017-ben rendelték közvet-

lenül a védelmi minisztérium alá, 2019-ben pedig reorganizációt és 400 fős létszámbővítést hajtottak végre benne (az összlétszám mintegy 1200 fő). Központja Kölnben található, de nyolc országos kirendeltsége működik, és külföldön is rendelkezik állomáshelyekkel. A hivatal elsősorban elhárító és alkotmányvédelmi feladatokat lát el, amelyekbe beletartozik a szélsőséges és a terrorista tevékenységek elhárítása mellett a (kiber)kémkedés és a szabotázs elleni küzdelem is. Ezenkívül folyamatosan követi a belföldi támaszpontok és a német missziók biztonsági helyzetét, részt vesz azok védelmében, végrehajtja a szükséges személyi biztonsági ellenőrzéseket, valamint az elektromágneses leárnyékolásért is felel. Elnökét egy nagyobb törzs, valamint egy civil és egy katonai elnökhelyettes támogatja a munkában. A két helyettes saját szakterület felett rendelkezik – a kibertémáért is felelős „T részleg" a katonai ágba tartozik. A „T részleg" több korábbi képesség koncentrálásával jött létre – folyamatosan törekszik az előremutató fejlesztésekre az információtechnológiai menedzsment, a hírszerzési technikák és a leárnyékolás területén.

4. Adaptációs lehetőségek

A fenti médiaigazgatási, szabályozási és védelmi-biztonsági hatásköri áttekintés után vizsgáljuk meg, hogy ezek közül melyik megoldás átvétele fontolandó meg Magyarországon. A közösségi jogharmonizáció egyik fő területe a média, mivel a versenyszabályozástól a kereskedelmi szakkérdéseken át a transzeurópai hálózatokig számos tárgykört érint. A kibertér úgyszintén átível a nemzeti határokon, ezért a hatékony szabályozási megoldásai is általában működőképesek a nemzeti kereteken átlépve (legalábbis az európai államok szintjén), és valamilyen standardizált közös alapból indulnak ki.

Fontos eltérés hazánkhoz képest Németország lényegesen bonyolultabb, föderális állami szerkezete, amire leginkább a médiaszabályozás kapcsán nagyon gyakran előkerülő szövetségi államközi megállapodások hívhatják fel a figyelmünket. Ennek ellenére az egyes online szabályozási megközelítések, szervezeti megoldások és a szervezetek mitigációs stratégiái képet adhatnak arról, hogy milyen szempontok szerint igyekeznek válaszokat adni az internet felől érkező multidimenziós biztonsági fenyegetésekre.

Megfontolandó a NetzDG és az online terrorista tartalmak elleni küzdelemről szóló törvény közelebbi vizsgálata a hasonló magyar szabályozásokhoz viszonyítva. A jogalkotó is jelezte a szövetségi hálózati ügynökség és a szövetségi bűnügyi rendőrségi hivatal együttműködésének az online terrorista tartalmak elleni küzdelemről szóló törvényben való kodifikálásával, hogy az ilyen komplex feladatok esetében akár több igazgatási szervezet közös munkájára is szükség lehet a cél eléréséhez. Ez a gyakorlatban nyilvánvalóan az érintett szakemberek és szervezeti egységek közös munkáján túl az együttes felkészítésükben, egymás képességeinek ismeretében, közös gyakorlatokban és folyamatos továbbképzésekben is meg kell jelenjen. A NetzDG hatékony nemzeti választ adott a közösségi média felől érkező egyes fenyegetésekre, viszont erős felhatalmazásai szinte szükségszerűen kritikát is kiváltottak, többek között a Human Rights Watch részéről,[26] és a belföldi szakértők is arra jutottak, hogy a törvény a közösségi jogba ütközhet. En-

[26] Germany: Flawed Social Media Law. *Human Rights Watch,* 2018. február 14., https://bit.ly/3UJldzz.

nek ellenére az Európai Bizottság egyelőre nem indított eljárást a kérdésben Németország ellen, sőt sajtóértesülések szerint egyes vonatkozó belső dokumentumokat vissza is tartott a „kölcsönös bizalom megőrzése érdekében".[27] A törvény rendelkezéseit már alkalmazzák, és például a Facebookot annak alapján 2,3 millió euróra büntették.[28] Mindez jól jelzi, hogy még alapos előkészítés és jól célzott jogalkotás esetén sem könnyű egy minden alapjogot védő és a köz érdekeit is hatékonyan óvni képes állami fellépés kodifikálása.

Szervezeti oldalról több vonatkozásban is jól láthatók a német jogi kultúrára egyébként is jellemző konzultatív, érdekegyeztető és kompromisszumkereső megoldások. Azon túlmenően, hogy minden szakterületnek külön hatásköre és felelőse van, fennállnak olyan problémák is (például a kibertér kockázatai), amelyek kapcsán a legtöbbször egymás mellé rendelt, mátrix jellegű szerveződésekkel hoznak létre szervezetközi kommunikációs platformokat. Ezek elsődleges szerepe adott esetben nem a konkrét lépések megtétele, hanem az akcióik összehangolása, a tapasztalatok és az információk cseréje.

A kibertér árnyoldalaival, az onnan érkező fenyegetésekkel a stratégia oldaláról megszívlelendő gyakorlat lehet az érintett igazgatási szervezetek közötti együttműködés fokozása, szükség és lehetőség esetén akár közös műveleti központok kialakításával. A jelenségek jobb megismerését, a hatékony fellépést és az adekvát szabályozás korszerűen tartását támogathatja a fokozott szakmai-tudományos tevékenység és együttműködés. Szintén jelentős szerepük van és a szervezetrendszer hitelességét is nagyban emelik a fogyasztóvédelmi tevékenységek, a különböző tudatosságépítő kampányok és a releváns, aktuális, használható és közérthető felvilágosító tartalmak fejlesztése (tájékoztató webtartalmak, podcastok stb.), ami szintén folyamatos tudományos és kutatói háttértevékenységet igényel, amelynek hátterét, kereteit elemi érdek megteremteni és fenntartani.

5. Összegzés

A 21. század biztonsági környezetének első két évtizede egyelőre a korábban megszokott stabil világrend megrendülését, a hibrid konfliktusok felerősödését hozta magával, amihez a kibertér globalitása egyszerre ad közvetítő közeget és értékes célpontokat. A dezinformáción, a szélsőséges vagy ellenérdekelt propagandán vagy a szervezett bűnözés érdekeinek megfelelően célzott tartalmak által megragadott figyelem értéke, a befolyásolás lehetősége, a saját narratívák futtatása, az objektív, kemény valóság felpuhítása, a bizonytalanság és a bizalmatlanság keltése mind akadályozhatja a hatékony, központilag irányított védelmi lépések végrehajtását az állami szervezetekben, éppen akkor, amikor szükség lenne rájuk. Ezért óriási a jelentősége annak, hogy a média igazgatásával megbízott szervezetrendszer a saját szakmai hitelességét és az állampolgárok bizalmát megőrizze, de közben döntései az emberi jogokat, a jogszabályokat és a köz érde-

[27] „Veröffentlichung würde das Klima des gegenseitigen Vertrauens beeinträchtigen". *WirtschaftsWoche,* 2017. november 10., https://bit.ly/44JtgkH.

[28] Facebook fined $2.3 Million by Germany for Providing Incomplete Information about Hate Speech Content. *Packt Hub,* 2019, július 3., https://bit.ly/44Kaycs.

keit tükrözzék és védjék, nyújtson támogatást az állampolgároknak, fogyasztóknak a dezinformációval és az információs közeget érő más támadásokkal szemben.

Kétségtelen, hogy a kibertérben mint folyamatos innovációs közegben állandó értékelést igényel, hogy egy fenyegetés vagy kihívás milyen beavatkozást igényel. Mérlegelendő, hogy az egyes problémák kezelése az érintettek milyen körének bevonását teszi szükségessé. Az áttekintésből jól látható, hogy míg egyes jelenségek *soft* eszközökkel, együttműködéssel, tájékoztatással is kordában tarthatók, addig mások esetében szigorú jogi szabályozásra és hatósági hatáskörök kialakítására van szükség. Szintén az adott probléma dönti el, hogy a megoldás – egyre atipikusabban – egy szereplő eszköztárában megtalálható, vagy szükséges a több szervezet közötti együttműködés, esetleg a közös folyamatos fellépés (akár műveleti központ) kialakítása az ideális megközelítés. Különösen a NetzDG kapcsán az is felvethető, hogy a szabályozás betűje gyakran nem a végső szó, az nem feltétlenül lesz azonnal általánosan elfogadott, és az EU egyik mintaállamának tekintett Németország esetében is előfordulhat, hogy vitatott megoldásokat kodifikál. Ez önmagában nem baj, hiszen az iteratív útkeresés, a folyamatos párbeszéd és adott esetben akár a demokratikus jogállami jogorvoslati megoldások alkalmazása, a jogi viták végigvitele vezethet el kompromisszumos és adekvát válaszhoz – amely válasz akár már pár év elteltével is meghaladottá válhat, mert egy új technikai fejlesztés és annak alkalmazásai ismét újraindíthatják az egész folyamatot.

Irodalomjegyzék

Branahl, Udo: *Medienrecht – Eine Einführung.* Wiesbaden, Springer, 2019. https://doi.org/10.1007/978-3-658-27381-1

Bühler, Peter – Schlaich, Patrick – Sinner, Dominik: *Medienrecht – Urheberrecht, Markenrecht, Internetrecht*. Berlin, Springer Vieweg, 2017. https://doi.org/10.1007/978-3-662-53920-0

El-Wereny, Mahmud: *Radikalisierung im Cyberspace. Die virtuelle Welt des Salafismus im deutschsprachigen Internet.* Bielefeld, Transcript, 2020. https://doi.org/10.1515/9783839452066

Farkas Ádám: Kibertér művelet: hírszerző, rendészeti és katonai műveletek elegye? Gondolatok az angol National Cyber Force kapcsán. *Military and Intelligence CyberSecurity Research Paper,* 2021/1., 1–8.

Farkas Ádám: A multidiszciplinaritás helye, szerepe a védelem és biztonság szabályozásának és szervezésének komplex kutatásaiban. *Közjogi Szemle,* 2021/4., 22–28.

Farkas Ádám – Spitzer Jenő: Az információs korszak és az állami reziliencia egyes kérdései. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2021/18., 1–27.

Hohnstein, Sally – Herding, Maruta: *Digitale Medien und politisch-weltanschaulicher Extremismus im Jugendalter. Erkenntnisse aus Wissenschaft und Praxis.* München, Deutsches Jugendinstitut, 2017.

Kelemen Roland: A közösségimédia-platformok tartalomszűrő tevékenységének árnyoldalai. In Glavanits Judit – Papp Nikolett (szerk.): *A fogyasztóvédelem egyes aktuális kérdései: a békés vitarendezés lehetőségei a 21. század technológia-intenzív közegében.* Budapest, Gondolat, 2022, 65–81.

Kelemen Roland – Farkas Ádám: A közösségimédia-platformok és a hibrid konfliktusok kapcsolata. *In Medias Res,* 2022/1., 96–108.
Kelemen Roland – Mihály Laura Dominika: A kibertér és a psziché ütközéspontjai mint a 21. századi reziliencia kulcskérdése. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/14., 1–31.
Keller, Andrea et al.: *Die Attraktion des Extremen Radikalisierungsprävention im Netz*. Frankfurt, Wochenschau, 2021.
https://doi.org/10.46499/1649
Klemperer, Victor: *A Harmadik Birodalom nyelve – egy filológus feljegyzései* (ford. Lukáts János). Budapest, Ampersand, 2021.
Krone, Jan (szerk.): *Medienwandel kompakt 2017–2019 – Schlaglichter der Veränderung in Kommunikation, Medienwirtschaft, Medienpolitik und Medienrecht. Ausgewählte Netzveröffentlichunge.* Wiesbaden, Springer, 2019.
https://doi.org/10.1007/978-3-658-27319-4
Schmitt, Josephine B. et al.: *Propaganda und Prävention.* Wiesbaden, Springer, 2020.
https://doi.org/10.1007/978-3-658-28538-8
Zha, Yunfei: *Die Regulierung rechtswiedriger Infromationen im Internet unter besonderer Berücksichtigung von Sperrmassnahmen gegen Access-Provider – Vergleich zwischen Deutschland und China.* Doktori értekezés, Münster, Universität Münster, 2019.