

Pázmány Péter Katolikus Egyetem
Jog- és Államtudományi Doktori Iskola

Habilitációs tézisek

**Méltóság, demokrácia, szuverenitás:
a digitalizáció felforgató hatása az alkotmányjogban**

Török Bernát

Budapest
2026

A habilitációs eljárás hivatalos és teljes tézisgyűjteménye a *Méltóság, demokrácia, szuverenitás: a digitalizáció felforgató hatása az alkotmányjogban* c. egy szerzős, kiadás alatt álló monográfia kézírata, amely a doktori iskolában teljes terjedelmében megtekinthető. Az alábbi összefoglaló csupán a kézirat következtetéseinek kivonata.

A) A MONOGRÁFIA TARTALOMJEGYZÉKE

Előszó

Bevezetés

I. Felforgatott szuverenitás: az állami szabályozás mozgástere és korlátai a digitális térben

1. A digitális szuverenitás elemzésének megalapozása: a szuverenitás fogalma

1.1. A szuverenitás eszme kifejlődése és fogalmi változatossága

1.2. A szuverenitás az alkotmányjogban

1.2.1. A szuverenitás alanya(i)

1.2.2. Az állam belső szuverenitásának tartalma

1.3. Szuverenitás az ezredfordulón

2. Az állam szuverenitása a digitális technológiák között

2.1. A digitális szuverenitás fogalma

2.2. A digitális szuverenitás területisége: a kibertér immunitásának kérdése

2.3. A digitális szuverenitás gyakorlati kerete: kódok és architektúra

2.4. A digitális szuverenitás gyakorlásának fő kihívásai

2.4.1. Magánszereplők kulcspozícióban

2.4.2. A hagyományos jogi eszközök elgyengülése

2.4.3. Társadalmi és gazdasági előnyök

3. Szabályozási csomópontok a digitális szuverenitás érvényesítésekor

3.1. Nemzeti vagy uniós szint

3.2. „Extraterritorialitás”

3.3. Kiszervezett szabályozás

3.3.1. Az alkotmányjog horizontális hatálya

3.3.2. Proxy szabályozók

3.3.3. „Önkéntes” magatartási kódexek

II. Felforgatott demokrácia: a közösségi média szabályozása a demokrácia védelmében

1. A közösségi média és a demokrácia

2. A közvélemény formálódásának demokratikus értékei

2.1. Önkormányzó közösség

2.2. Részvétel

2.3. Tanácskozás

2.4. Pluralizmus

2.5. Informált nyilvánosság

2.6. Átláthatóság

3. Az állam szerepe a demokratikus közvélemény védelmében

3.1. Alapjogok horizontális hatálya

3.2. Objektív intézményvédelem

3.3. A nyilvánosság szerkezete

4. Demokrácia-kihívások a közösségi média működésében

4.1. Új részvételi lehetőségek elvesztése

- 4.2. Kozmopolitizmus
 - 4.3. A nyilvánosság szélsőséges fragmentációja
 - 4.4. Törzsi hajlamok felerősítése
 - 4.5. Dezinformáció
 - 4.6. Manipuláció, választások integritása
 - 5. Európai eszköztár a demokrácia megerősítésére
 - 5.1. Felhasználói szólásszabadság a platformokon
 - 5.2. Átláthatósági követelmények – és amit láthatóvá tettek
 - 5.3. Kockázatértékelés és -csökkentés
 - 5.3.1. A platformok jelentései
 - 5.3.2. A kockázatcsökkentő törekvések értékelése
 - 5.4. További lehetséges jogi lépések
 - 5.4.1. A perszonalizáció áttörése
 - 5.4.2. Változtatások az architektúrában
 - 5.4.3. Hitelesítés
 - 6. Hamvukba holt szabályozási kísérletek az Egyesült Államokban
 - 6.1. A tartalommoderálás szabályozása
 - 6.2. Deepfake-szabályozások
 - 6.3. Politikai hirdetések átláthatósága a platformokon
 - 7. Túl a jogon
- III. Felforgatott méltóság: az egyén alkotmányjogi pozíciója a digitális valóságban
- 1. Az emberi méltóság jogi fogalmának új elemei
 - 1.1. Az emberi méltóság jogi fogalmának alapvető kihívása
 - 1.2. Az MI és a méltóság: empirián innen és túl
 - 1.2.1. Profilalkotás
 - 1.2.2. Prediktív algoritmusok
 - 1.2.3. Elgépiesedés: az emberi beavatkozás kérdése
 - 1.2.4. Manipuláció
 - 1.2.5. Utópia: jog a megfigyeléssel szemben
 - 1.2.6. Deepfake: régi-új veszély a méltóságra
 - 2. Az információs önrendelkezés délibábja
 - 2.1. Az információs önrendelkezés koncepciója
 - 2.2. Az információs önrendelkezés kihívásai a digitális térben
 - 2.3. Alkotmányjogi helyzetértékelés és „hogyan tovább”
 - 2.3.1. Az adatvédelem horizontális hatálya
 - 2.3.2. Új megoldások felé tekintve

Zárszó

Irodalomjegyzék

B) A MONOGRÁFIA KIVONATOLT TÉZISGYŰJTEMÉNYE

Bevezetés

1. Nem túlzás azt állítani, hogy a digitális vívmányok az alkotmányjogot is felforgatták. Elég csak rápillantanunk a kibertér szereplőit célzó, számunkra legfontosabb regulációkra – az adatvédelmet (GDPR), az internetes platformokat (DSA) vagy a mesterséges intelligenciát (AIA) szabályozó európai uniós rendelethez –, rögtön szembeötlő, milyen mértékben itatják át őket az alkotmányjogi fogalmak és elvárások. A szabályozások fokozatos egymásra épülése oda vezetett, hogy az európai jogalkotó ma már szinte teljessé vált alapjogi katalógust szegez szembe a digitális szféra magánszereplőivel, és tőlük (is) várja alkotmányos értékeink megvédését az online térben.

2. A célom annak a sajátosan európai megközelítésnek a bemutatása, amelyet az utóbbi évek egyéb feszítő vitái közepette is látványos konszenzus övezett az uniós jogalkotásban. Az új technológiák szabályozása a közelmúlt európai kodifikációs munkájának legaktívabb területévé vált, és felpörgetett ütemben elfogadott rendeletek hosszú sora jelzi: a tagállamok egyhangúan készen állnak arra, hogy egy jellegzetesen európai felfogást szegezzenek szembe a technológiai fejlődés társadalmi hatásaival. Ennek a felfogásnak jellemzője egyrészt a védendő alkotmányos értékek elegye (az emberi méltóságtól kezdve a demokratikus jogállamiságon át az alapjogok katalógusáig), másrészt a védelmükre felsorakoztatott jogi doktrínák (az alapjogok már említett horizontális hatályától kezdve az állam tevőleges védelmi kötelezettségein át az újszerű kockázatcsökkentési megoldásokig).

3. A digitalizáció egyre terebélyesedő társadalmi kihívásaival kapcsolatos diskurzusban hamar megmutatkozott, hogy e kihívások az öreg kontinensen alkotmányos problémaként is konceptualizálódnak. Ezek után nem volt meglepő, hogy az említett uniós rendeletek oly mértékben nyúltak az alkotmányjog fogalmi készletéhez és eszköztárához, hogy a felépített szabályozási rezsimet nem túlzás összefoglalóan Európa „digitális alkotmányosságának” (*digital constitutionalism*) hívni. Csakhogy amennyire hangzatos és – mint látni fogjuk – logikájában érthető ez a jogfejlődés, annyira sok nyitott kérdés övezi jelenleg. Mostanra már nem elég, hogy az új technológiák szabályozásában felismerjük az alkotmányjog megfontolásait és intézményeit, hanem a pontos tartalmukról is mondanunk kell valamit az új környezetben való értelmes alkalmazásuk érdekében.

4. Az elmúlt évek kutatómunkájában a magam részéről olyan metszéspontokat kerestem, amelyek egyrészt fundamentális jelentőségű alkotmányos fogalmakra mutatnak, másrészt az átlagosnál is nagyobb intenzitással vetnek fel újszerű kérdéseket a digitális környezetben, harmadrészt pedig – nyilván az előző szemponttal szoros összefüggésben – a legjobban szemléltetik az új technológiák körében megjelenő sajátos alkotmányjogi logikákat.

5. Célom kettős: egyfelől közelebb hozni az Olvasóhoz az öreg kontinens alkotmányos értékeit óvó jogalkotói megközelítését, másfelől érzékelteni e szabályozási törekvések

korlátozottságát is. A következőkben elemzett három fogalom, a szuverenitás, a demokratikus közvélemény és az emberi méltóság doktrínája kiváló példák arra, hogy az európai alkotmányjog szükség esetén készen áll új korszakok körülményeihez történő adaptálódásra. Ezzel azonban legfeljebb csak „helyzetbe hozhatjuk” magunkat, de hogy ténylegesen előrébb lépünk-e, az valójában már nem az alkotmányjogon vagy dogmatikai újításokon múlik, hanem rajtunk, mindannyiunkon.

I. Felforgatott szuverenitás: az állami szabályozás mozgástere és korlátai a digitális térben

1. A digitális szuverenitás elemzésének megalapozása: a szuverenitás fogalma

6. Míg a szuverenitás eredeti koncepciója a korlátozhatatlanságra és a bináris logikára (vagy van, vagy nincs) épült, addig később az eszme megszelídítésére és bináris tartalmának lazítására helyeződött a hangsúly: egy szuverén számára is hol nagyobb, hol kisebb mozgástér adódhat akaratának érvényesítésére.

7. A szuverenitás alkotmányjogi fogalmában árnyalja egymást a nép-, a jog- és az államszuverenitás eszméje: ezek nem egymással, hanem a kizárólagos alanyiség és a korlátlan hatalom gondolataival állnak kibékíthetetlen viszonyban.

8. A digitális szuverenitás körében különösen az állam szuverenitásának két jellemzője igényel elemzést. Az egyik a belső szuverenitás egyetemessége (általánossága): az állam hatalma kiterjed a teljes területére (területi felségjog) és a területen élő lakosság egészére (személyi felségjog). A másik jellemző a kizárólagosság: az állam a hatalma gyakorlásához nem igényli az érintettek beleegyezését vagy közreműködését. Az állam belső szuverenitása abban a lehetőségben és tényben fejeződik ki, hogy a társadalmi viszonyokat rendezni és alakítani képes, a társadalmi együttélést irányító funkciója van. A szuverenitás az ehhez szükséges felségjogok és hatáskörök összességéként is felfogható.

9. Az egyetemes és kizárólagos belső szuverenitás érvényesülése két lényegi elemre támaszkodik: autoritásra és kontrollra. Az autoritás az állam elismert joga arra, hogy hatalmát gyakorolja, irányítson és parancsát kövessék. A kontroll pedig az állam tényleges képessége arra, hogy a területén folyó cselekményeket és fejleményeket befolyásolja, meghatározza.

10. A digitális világban kiéleződik a kérdés, hogy kiszervezheti-e vagy átengedheti-e az állam a főhatalom gyakorlásának körébe tartozó egyes hatásköreit nem állami szervnek. Az állam ezt megteheti, de mindez akkor lesz összhangban a szuverenitásából fakadó követelményekkel, ha az átengedés a saját döntése alapján, vagyis tipikus esetben előzetes jogalkotás keretében történik.

11. Átengedés, kiszervezés esetén tisztázni kell, hogy adott helyzetben a nem állami szerv cselekvése valóban az állami szuverenitás felségjogait érinti-e. Demokratikus viszonyok között ezt a tisztázást a különféle magánautonómiák határainak tiszteletben tartásával kell elvégezni.

Előfordulhat ugyanis, hogy ami első pillantásra a szuverenitás körébe tartozónak tűnik, valójában a magánautonómia által védett aktus.

12. A globális világgazdaságban a saját területe és népessége fölött szuverenitással bíró nemzetállam olyan nem állami erőközpontokkal szembesül, amelyek nem területi logikában gyakorolnak jelentős hatást a gazdaság és a társadalom működésére, és amelyek már hatalmi értelemben is kihívást jelentenek az állam pozíciója, különösképpen gazdasági mozgástere és befolyásoló képessége számára. Az állam munkamegosztásra kényszerülhet, ugyanakkor nem mindegy, hogy milyen megfontolások alapján, milyen célok elérése érdekében, milyen feltételekkel fogadja el ezt a munkamegosztást. A nemzetállamoknak megkerülhetetlen szerepe marad a nemzetek feletti és alatti hatalmi mechanizmusok legitimálásában (vagy nem legitimálásában), valamint e mechanizmusok elszámoltatásában.

13. Mindez önmagában véve csupán akkor jelentené az államszuverenitás végét, ha azt még mindig totális autonómiaként szeretnénk felfogni. A szuverenitás eszme fejlődése azonban nem ebbe az irányba mutat, így sokkal inkább azt mondhatjuk, hogy az államhatalom gyakorlásának környezete nagy mértékben átalakult, és az állam felségjogai érvényesítésekor nem hagyhatja figyelmen kívül az új peremfeltételeket.

14. Még ha adott körülmények között nem is mutatkozik vagy mutatkozhat meg a demokratikus állam ereje a maga teljességében, ez távolról sem jelenti cselekvőképességének elvesztését. A dolgok végkimenetele rajta múlik.

2. Az állam szuverenitása a digitális technológiák között

15. Le kell választanunk a digitális szuverenitás problémájáról az egyének jogi státuszát érintő kérdéseket. Egyes szerzők ugyanis a digitális szuverenitás problematikájába keverik a felhasználók autonómiáját és önrendelkezését érintő súlyos kérdéseket is, „személyes digitális szuverenitásként” („*personal digital sovereignty*”) vagy „egyéni adat szuverenitásként” konceptualizálva őket. Értve a logikát, amely közös szálra igyekszik felfűzni a digitális folyamatok feletti kontroll kérdéseit, az alkotmányjogi dogmatika felől nézve feloldhatatlan zavart jelentene az egyén és az állam pozíciójának azonos fogalmi keretben történő tisztázása.

16. A technológiai szuverenitás fogalma azt vizsgálja, hogy egy nemzetállam vagy az Európai Unió milyen mértékben képes önállóan fejleszteni és birtokolni a digitális folyamatokhoz szükséges technológiai infrastruktúráját. A túlzott függőség olyan kiszolgáltatottságot jelent, ami alááshatja az állam cselekvőképességét. Az alkotmányjogi elemzésnek ugyanakkor ennek konstatálásán és a kiszolgáltatottság elkerülésére irányuló politikák jelentőségének hangsúlyozásán túl nem sok dolga van a technológiai szuverenitás problémájával, az sokkal inkább gazdaság- és geopolitikai természetű értékelést és cselekvést igényel.

17. Az alkotmányjog fókuszába a digitális szuverenitás diskurzusának az az iránya tartozik, amely arról szól, hogy milyen sajátos kihívások érik az állam felségjogainak, különösen szabályozói hatalmának gyakorlását a kibertérben, és mit jelent ez az állam cselekvőképessége számára.

18. A digitális szuverenitás fogalma kiegészíti az államszuverenitás hagyományos koncepcióját, és azon online aktivitások feletti autoritásra és kontrollra vonatkozik, amelyek vagy egy állam területéről erednek, vagy az állam területén található személyeket, szervezeteket és infrastruktúrákat érintenek. A kibertér feletti kontroll mindenekelőtt az állam területén belüli, illetve onnan induló vagy oda érkező digitális adatforgalom feletti kontrollt jelenti, ezért az adatszuverenitás a digitális szuverenitás legfontosabb aspektusa.

19. Az államoknak az a törekvése, hogy az adatáramlásokat nemzeti joghatóságuk alá vonják, a gyenge és az erős adatszuverenitás két pólusa közti skála adott pontjára helyezi őket. A gyenge adatszuverenitás a magánszektor által vállalt adatvédelmi kezdeményezéseket részesíti előnyben, míg az erős adatszuverenitás az állam által irányított megoldásokban hisz. Az államnak azt a döntését, hogy az erős vagy a gyenge szuverenitás megoldásaira támaszkodjon, jelentős mértékben befolyásolja az alkotmányjogi doktrína, illetve a gazdaság működésére vonatkozó elvek és a gazdasági realitás.

20. Az állam ambíciója nem a kibertér „mint olyan” szabályozására vonatkozik, hanem adott területen élő emberek életének befolyásolására. Az adott területen élő társadalom fölött hatalmat gyakorló állam ambíciója és autoritása ennek a társadalomnak a kontrolljára irányul, függetlenül attól, hogy mely „térből” érkeznek a társadalomformáló hatások. Az állam digitális szabályozási ambíciója a virtuális tér adott területre gyakorolt valós hatásainak befolyásolására irányul.

21. Politikai értelemben nem látszik meginogni a (nemzet)államok alapvető pozíciója, nem látszik valós kihívója a társadalmak jelenlegi állami keretekbe rendeződésének. Az állami szuverenitás számára nem az az elsődleges kérdés, hogy tudja-e az állam a globális kibertérben uralni a digitális technológiákat, hanem az, hogy tudja-e kontrollálni e technológiák lokális társadalmi hatását.

22. Ha az állam a kibertér digitális vívmányainak társadalmi hatásait a teljesség igényével és a hatékonyságot minden esetben elsődleges prioritásként kezelve kívánja kontrollálni, akkor olyan technikai megoldásokhoz kell fordulnia, amelyek a világháló végét jelentenék. A nyugati alkotmányos kultúra államai számára nem az a mérlegelés tárgya, hogy tudnak-e élni a szuverenitásukkal az online tér vonatkozásában, hanem az, hogy hogyan érdemes ezt megtenniük.

23. A digitális világ sajátossága, hogy architektúrájának köszönhetően kódokon és algoritmusokon keresztül tetszőlegesen alakítható meghatározott értékek mentén. Nem kérdés, hogy valaki, valamilyen értékek mentén kódolni fogja az online szférát, csak az a kérdés, hogy ki és milyen értékek mentén tesz ezt meg.

24. A kibertér szabályozási architektúrája, vagyis a kódok és algoritmusok központi szerepe nem pusztán arra nyújt lehetőséget, hogy a szuverenitás tradicionális gyakorlását „átmentsük” az online szférába, hanem egy minden korábbinál erősebb kontroll lehetőségét teremti meg, végső soron az állam számára is. A szuverenitás esztétörténeti fejlődése ugyanakkor azt mutatta, hogy demokratikus viszonyok között a szuverenitás csak korlátok közé terelt cselekvőképességet biztosít az állam számára. Nem lehet ez másképp a digitális szférában sem:

egyszerre feladat az állam cselekvőképességének megteremtése, illetve fellépése határainak kijelölése.

25. Kihívás a digitális szuverenitás számára egyrészt az, hogy magánszereplők kezében vannak a kódok és az architektúra, amelyek a kibertér szabályozásának lényegi eszközei, másrészt funkcionális értelemben is ezek a magánszereplők váltak a digitális világ fő koordinátoraivá. Szerepük nem csupán statikus (ami már önmagában véve is megkerülhetetlenné tenné őket), hanem irányító jellegű is. Mindez azonban – helyes értelmezés szerint – nem eszköztelenné tette az államot, hanem eszközeinek „kibertérre szabását” várja el tőle.

26. Az állam a magáncégek központi szerepe mellett sem veszítette el szabályozói hatalmát. A szuverenitás felségjogai közé tartozó jogalkotás jogát senki nem vitatja el tőle. A mégoly befolyásos magánszereplőknek sincs más fontos céljuk, mint hogy minél jobban monetizálják az online térben kiépített pozícióikat. Kereskedelmi logikában működnek, és szabályaikat is kereskedelmi logikában alakítják.

27. Újszerű helyzet, hogy az államnak minden fontos digitális szabályozói lépésénél számításba kell vennie az infrastruktúrát kézben tartó piaci szereplőket. A digitális architektúra és az online forgalom irányítóiként megkerülhetetlenek az állami célok eléréséhez, ezért olyan új szabályozói megoldásokra van szükség, amelyek „számolnak velük” a közpolitikai lépések megtételekor. Ezek a megoldások egyfelől sajátos korlátokkal bírnak az államhatalom számára, másfelől viszont akár veszélyesen ki is tágíthatják mozgásterét a társadalom kontrollálásában.

28. Demokratikus viszonyok között a magánszereplők kulcspozíciói korlátokat jelentenek abban a tekintetben, hogy az államnak tiszteletben kell tartania autonómiájukat. Az állami szuverenitás a digitális térben sem a korlátlanságban nyeri el értelmét, hanem abban, hogy ott is megmarad az érdekeinek érvényesítésére szolgáló közhatalmi ereje és eszközrendszere. Való igaz, hogy ebben az eszközrendszerben új megoldásokat (is) ki kell dolgozni, de ez egy természetes munkamegosztás következménye: az államnak nem feladata – és a kapitalizmus egyik alaptézise szerint nem is végezné el ezt a munkát a magánérdekek által motivált szereplők hatékonysági szintjén –, hogy a technológia fejlesztésében rejlő újabb és újabb lehetőségek kreatív kiaknázására fordítsa minden figyelmét. Az állam feladata az, hogy szuverenitásával, szabályozói közhatalmával élve a társadalom számára valóban lényeges pontokon beavatkozzon, és határt szabjon a magánautonómiáknak.

29. Az új szabályozói megoldások egyszerre szükségszerűek az állami szuverenitás és a társadalmi érdekek érvényesítése számára, illetve kockázatosak a polgárok szabadsága szempontjából. A kormányok különféle ösztönzők és szankciók célirányos kombinációjával jó eséllyel vehetik rá a magáncégeket, hogy autonómiájukkal a kormányzat elképzelései mentén éljenek, és akár olyan magatartásokat is kontroll alatt tartsanak, amelyek egyébként kívül esnének az állam szabályozói hatókörén.

30. További kihívás a digitális szuverenitás számára, hogy az állam szuverenitását érvényesítő korábbi jogi eszközök bizonyos körben eleve nem képesek hatékonyan kézben tartani az interneten zajló folyamatokat. Az internet forradalmi újdonságot jelent a kommunikáció tömegessége és globális terjedési sebessége terén. A sebesség ráadásul nemcsak az egyedi

„digitális cselekmények” speciális terjedési potenciáljaként jelent kihívást, hanem abban az értelemben is, hogy a kibertér intézményei és folyamatai – vagyis a szabályozás tárgyai – állandó és gyors változásban vannak. Megint csak az architektúra ereje mutatkozik itt meg: mivel a digitális világban kódok szabják meg, mit és hogyan lehet vagy nem lehet, a kódok átprogramozása egyetlen pillanat alatt teljesen új működési mechanizmusokat léptethet életbe.

31. Alapvető szabályozási kihívás az is, hogy az internet, illetve a rá épülő online szolgáltatások és digitális eszközök a szabályozási dilemmákat okozó problémák mellett, sőt azokkal nagyon szorosan összenőve olyan előnyöket hoztak az egyének, a társadalom és a gazdaság életébe, amelyek elvesztése vagy veszélyeztetése vállalhatatlan kockázatot jelent a jogalkotó számára. Ha a szabályozó nem jól méri fel a helyzetet, és kizárólag a problémákra tekintve nem kellőképpen megfontolt megoldást választ a kezelésükre, könnyen úgy járhat, hogy a fürdővízzel együtt a gyereket is kiönti, amelynek a társadalmi és gazdasági költségei jóval jelentősebbek lehetnek, mint az eredeti nehézségek.

32. Ebben a mérlegelésben két körülmény tovább nehezíti az európai jogalkotás eredményességét. Egyrészt az öreg kontinens országainak azzal kell számolniuk szabályozói lépéseik megválasztásánál, hogy az említett társadalmi és gazdasági előnyök realizálását elsősorban külföldi techcégek teszik lehetővé. Másrészt az új technológiák nyújtotta előnyök sokszor magukat a politikai szereplőket is ellenérdekeltté teszik a szabályozási lépések megtételében.

3. Szabályozási csomópontok a digitális szuverenitás érvényesítésekor

33. Az új technológiák szabályozása az egyik, ha nem a legalkalmasabb kérdéskör annak szemléltetésére, hogy az Európai Unió miként tud egy nagy jelentőségű, a társadalmat átfogóan érintő területen, tagállamainak erős támogatása mellett, az állami szuverenitás szempontjából fontos kérdésekben közösen lépni. Az emberi méltóság, a szabadságjogok érzékeny összehangolása, a jogállamiság vagy a demokrácia mind olyan alapértékek, amelyek úgy alkotják a közös európai jogi örökség központi magját, hogy online védelmük eltérő okból ugyan, de egyik más globális befolyással bíró hatalomtól – sem az Egyesült Államoktól, sem Kínától, sem más aktortól – nem várható.

34. Az európai államok helyesen látták be, hogy a szuverenitás digitális környezetben való gyakorlása olyan nyomások alá helyeződik, amelyek között a közös cselekvés jóval nagyobb eséllyel találhatja meg a megfelelő utat. Globális techóriások egyfelől, a világháló nyújtotta előnyök másfelől: ha az állami szuverenitás anélkül szeretné kontroll alatt tartani, sőt céljainak közvetítőiként használni a digitális szereplőket, hogy drasztikus lépésekkel elzárna magát és társadalmát az internet nemzetközi forgatagától, akkor a jogi autoritáson túl politikai-gazdasági erőt és ösztönzőket is fel kell tudni mutatnia. Márpedig az európai államok számára az egyesek által „digitális szuverenizmusnak” vagy „digitális etatizmusnak” hívott bezárkózás mind kulturálisan, mind gazdaságilag idegen, anakronisztikus hozzáállás lenne.

35. Túlzás lenne azonban azt állítani, hogy a digitális szféra szabályozásában meglévő egységes európai szándék és jogalkotási lendület mindenestül eltörölte volna az uniós és a tagállami

szempontok különbözősége közti feszültségeket. Nagyon fontos, hogy eljárásukban az uniós szervek nagy érzékenységgel forduljanak a tagállamokból érkező jelzések felé. A fellépés hatékonyságát érintő belátás nem változtatott azon a helyzeten, hogy a társadalmi problémák megjelenését és sajátosságait helyben lehet megfelelően detektálni, így ha az Unió központjában nem kellő érzékenységgel veszik figyelembe az „alulról jövő” impulzusokat, az alááshatja a jogalkalmazás eredményességét és hitelességét.

36. Az államoknak – normál esetben – valójában nincsenek extraterritoriális ambícióik, mivel nem a határaikon túllépő kibertér „mint olyan” szabályozása a lényeges számukra. Csakhogy ameddig egy állam egy lehatárolt helyi hálózattal le nem kapcsolja magát a világhálóról, addig az internetre (is) vonatkozó szabályozás – mind az adatáramlás, mind az azt menedzselő vállalatok nemzetközi természete miatt – külföldieket is érinteni fog.

37. A digitális szuverenitás gyakorlása törvényszerűen együtt jár külföldi entitások szabályozásával: az állam külhonosnak minősülő, ám a globális internet révén működésükkel az ő területén is hatást kiváltó szereplőkkel szemben tart igényt a szabályozásra, ami valójában az „extraterritorialitás” kifejezés használatát is megkérdőjelezi. A kifejezés mindössze annyiban indokolt, hogy a szuverenitás gyakorlása a gyakorlati jogi eszközök terén tradicionálisan már extraterritoriálisnak tekintett, máshol honos alanyokra is kiterjedő megoldásokat igényel a digitális környezetben.

38. Az uniós jognak az a megoldása, hogy letelepedési helyüktől függetlenül kötelezi a szolgáltatókat, már a GDPR esetében is indokolt volt a joghatóság kikerülésének megakadályozására, a DSA és az AIA esetében viszont gyakorlatilag ahhoz szükséges, hogy a rendeleteknek egyáltalán értelmük legyen.

39. Egyfelől gazdaságilag és geopolitikailag is kulcskérdés, hogy Európa (idővel) a saját cégeivel vegyen részt a digitális globalizációban, aminek ráadásul hosszabb távon kétségkívül hatása van a hatóságok jogérvényesítő képességére és az állami szuverenitás gyakorlására is. Másfelől viszont a digitális viszonyokra kalibrált „extraterritoriális” szabályozói megoldások éppen arra mutatnak rá, hogy az állam felségjogainak gyakorlása nem függ és nem is függhet a szabályozandó cégek honosságától vagy a tárgyi eszközök fizikai elhelyezkedésétől.

40. A külföldi platformok nem fosztják meg államainkat a szuverenitásuktól. A cselekvés lehetősége és a problémamegoldás felelőssége az államé maradt. A fizikai eszközök lokalizációja mindazonáltal – súlyosabb végrehajtási problémák esetén – a digitális szuverenitás „záróköveként” juthat szerephez. Alapvetően nem akadály a szuverenitás érvényre juttatásának a fizikai alkotóelemek extraterritoriális elhelyezkedése, de alakulhat úgy, hogy végső eszközként az államnak a területén található „vas” vagy hírközlési frekvencia feletti rendelkezésen keresztül kell megakadályoznia, hogy egy renitens szolgáltatás eljusson a végfelhasználókhoz.

41. Ha a jogalkotó azelőtt kényszeríti „belföldön maradásra” a digitális folyamatokat, mielőtt annak gazdasági, pénzügyi és egyéb feltételei megfelelőek lennének, saját gazdaságát, társadalmát és végeredményképpen államának erejét is alááshatja.

42. A magánszereplők kulcspozícióba kerülésére született egyik európai válasz az alapjogok horizontális hatályának soha nem látott kiterjesztése az új technológiák szabályozásában. Ha a kibertérben a techcégek jelentős és közvetlen befolyással vannak az egyének pozíciójára, digitális jogaira és érdekeire, akkor a horizontális hatály tana lehetőséget nyújt az alapjogvédelem „kiszervezésére” e pozíciók biztosítására. A digitális jogviszonyokban ráadásul több olyan egyensúlytalanság is tipikusnak tekinthető, amely az európai szabályozási logika szerint ablakot nyit az alkotmányossági követelményeknek.

43. A horizontális hatály alkalmazásának kihívása, hogy az alapjogi szempontok érvényesülése magánfelek között nem követheti egy az egyben az államra vonatkozó alapjogi doktrínát, mivel itt a jogviszony kötelezeti oldalán is olyan magánfelet találunk, akinek jogait, adott esetben alapjogait és méltányolandó érdekeit szintén el kell ismernie a szabályozásnak és jogalkalmazásnak. Sajátos kérdéseket vet föl továbbá az is, hogy az új technológiák szabályozásában nemcsak az alapjogok, hanem más alkotmányjogi követelmények (pl. olyan jogállami elvárások, mint az átláthatóság vagy az elsámoltathatóság) is horizontális hatályúvá váltak.

44. A digitális szuverenitás gyakorlására kidolgozott újabb jogi konstrukciók egy része kifejezetten arról szól, hogy a szabályozás által kitűzött célokat a releváns magánszereplők valósítsák meg. A digitális aktorokat proxy-ként használó megoldások egyik formája szigorú kötelezettségként jelenik meg, és leginkább bizonyos tartalmak üldözését várja el tőlük. Ebben a körben a jogalkotó vagy jogalkalmazó magánál tartja a jogellenesség megállapításának jogát, de igazodva a kibertér adottságaihoz nem saját eszközeivel próbálja elérni a jogszerű állapotot, hanem az architektúra kulcspozícióiban lévőktől várja el a „rendteremtést”.

45. Még izgalmasabb az újabb konstrukcióknak az a köre, amikor a jogalkotó tulajdonképpen már a konkrét teendők megállapítását is átengedi magánszereplőknek. Ezekben az esetekben a szabályozó csupán absztraktabb szempontokat határoz meg, de ezek érvényesülésére nem ír elő kötött, szigorú kötelezettségeket, hanem puhább kereteket teremt, amelyen belül a digitális aktoroktól várja a konkrétabb szabályok és mércék kidolgozását. Az egyik legjobb példa erre a megoldásra a DSA kockázatértékelésre és -csökkentésre vonatkozó konstrukciója.

46. Az állam szabályozó hatalmának ilyen kiszervezése – még ha látjuk is a kibertéri viszonyok közti indokoltságát – valóban tűnhet úgy, hogy a jogalkotó átengedte a „kormányzás” és a normaalkotás felségjogát, és magán szabályozásoknak szolgáltatta ki az online szférát. Pedig nem erről van szó. Vagy legalábbis nem erről van szó akkor, ha a megszabott kereteken belüli szolgáltatói teljesítést gondos jogalkalmazás ellenőrzi, amely készen áll arra, hogy indokolt esetben azonnal belépjen a konkrét kötelezettségek megszabásába is. A konstrukció megőrzi a határozott hatósági fellépés lehetőségét arra az esetre, ha a szolgáltatók jobban féltenék üzletileg sikeres működésüket, mint a jogalkotó által kijelölt értékeket. A jogalkalmazón múlik, készen áll-e ekkor a társadalmi érdek konkretizálására és érvényesítésére

47. Az önkéntes magatartási kódexeknek világos és előremutató szerepe van akkor, amikor egy szükséges mértékben már szabályozott (vagy legalább szabályozható) területen születnek. A GDPR esetében erről van szó: a jogalkotó az egyébként részletesen meghatározott normák (adatkezelőkre vonatkozó kötelezettségek) minél sikeresebb alkalmazása érdekében

intézményes teret nyitott az érintettek tapasztalatainak „becsatornázására”, illetve az érintettek bevonásával igyekszik pontosítani generálklauzulák tartalmát. Nem visznek azonban előrébb ezek a kódexek akkor, ha valójában a jogalkotói tanácstalanság szüli őket, mint például a platformokat a dezinformáció elleni küzdelemre buzdító uniós elvárások esetében. A DSA példája azt mutatja: a jogalkotó – kiváltképp a szolgáltatók nem őszinte részvétele esetén – végül semmiképp sem kerülheti el a világosabb normák megkövetelését.

II. Felforgatott demokrácia: a közösségi média szabályozása a demokrácia védelmében

1. A közösségi média és a demokrácia

48. A demokráciára gyakorolt technológiai hatások számos aspektusa közül a közösségi média átalakító erejének kérdését több okból is érdemes kiemelni. Egyrészt a közösségi platformok éppen azon a területen idéztek elő alapvető változásokat, amely egy demokratikus rendszer működésének *sine qua non* eleme: felforgatták a közvélemény demokratikus formálódásának mechanizmusait. Másrészt a demokratikus berendezkedést érő kihívások közül talán itt figyelhető meg a legjobban az a szabályozási innováció, amellyel az Európai Unió a digitális környezet sajátos viszonyai között igyekszik megvédeni az alkotmányos rend alapértékeit.

49. A közösségi média – rendkívül szerteágazó társadalmi, gazdasági, kulturális és egyéb funkciói között – az alkotmányjog számára megragadható módon azáltal van közvetlen hatással a demokrácia állapotára, hogy a közvélemény alakulásának egyik legfontosabb fórumává vált. Nem kérdés, hogy a platformok működése komoly hatással van a közvélemény formálódásának demokratikus értékeire.

50. A platformok társadalmi jelentősége olyan ténykérdés, amely önmagában véve megalapozza a működésükkel kapcsolatos szabályozási dilemmákat. A közösségi média közrehatásának mikéntje – mindenekelőtt például az, hogy tevékenysége mennyiben illeszkedik a hagyományos értelemben vett szerkesztői felelősség körébe – természetesen fontos kérdés a jogi részletek kidolgozásánál, de nem perdöntő annak az alapvető kérdésnek az eldöntésénél, hogy van-e társadalmi vagy adott esetben szabályozói feladat a közösségi média demokráciára gyakorolt hatásával összefüggésben.

51. Bár a szabályozó a demokratikus értékek veszélyeztetésével igazolható teendőkre fókuszál, a közösségi média messze nem csak negatív hatással van a demokratikus folyamatokra. A negatív következményekkel jelentős demokratikus hozadék – mindekelőtt a részvételi lehetőségek radikális bővülése – mellett kell számot vetnünk, ami különösen is összetetté teszi a kérdéskör jogi megragadását, és finomhangolt megközelítést igényel.

52. Az európai doktrína szerint az államnak nemcsak lehetősége, hanem bizonyos körben alkotmányos kötelezettsége van arra, hogy tevőlegesen, különösen jogalkotással hozzájáruljon az alkotmányos értékek érvényesüléséhez. Nincs ez másképp a közvélemény demokratikus értékei terén sem. A közösségi média és a demokratikus közvélemény alkotmányjogi kritériumrendszerének találkozásakor kiváltképp két európai dogmatikai konstrukció jut fontos

szerephez: az alapjogok horizontális hatálya, illetve az állam objektív intézményvédelmi kötelezettségének a tana.

53. Az alapjogok horizontális hatályának tézise napjainkban egyre nagyobb teret nyer a szólásszabadság területén, különösen a közösségi média és felhasználóinak viszonyában. Eszerint a platformok nem alakíthatják és alkalmazhatják közösségi szabályait teljes mértékben a saját belátásuk szerint, hanem figyelemmel kell lenniük felhasználók jogaira is, elsősorban szólásszabadságukra.

54. A demokratikus közvélemény értékeinek objektív, intézményes védelme olyan állami beavatkozásokat tehet indokolttá, amelyek a közvélemény alakulásának szerkezetét, kereteit érintik. Olyan demokratikus „dizájn” kialakítása vagy fenntartása lehet az állam fellépésének legitim célja, amely biztosíthatja az eszmék és vélemények minél sokszínűbb áramlását.

2. Demokrácia-kihívások a közösségi média működésében

55. Mai működési mechanizmusaival a közösségi média számos ponton veszélyeket rejt a demokratikus értékek érvényesülésére – akár úgy, hogy tovább erősít korábban már meglévő negatív tendenciákat, akár úgy, hogy új kockázatokat hoz magával. Ezeknek a következményeknek a jelentőségét ráadásul radikálisan felerősíti, hogy a közösségi média nemcsak hogy nem hozta el a korábbinál több szereplőből álló nyilvánosság korszakát, hanem minden eddiginél erősebb koncentrációra vezetett egy-két globális óriáscég dominanciájával.

56. A bejegyzések vagy profilok felfüggesztésétől és törlésétől sem visszariadó széles körű moderálás a kezdeti demokratikus vívmánytól messzire repítheti a közösségi platformokat. Az online platformok ráadásul minden eddiginél hatékonyabban működtethető kapuőrökké válhatnak. Nem volt még olyan mechanizmus, amely a társadalmi párbeszéd ekkora jelentőséggel bíró szegmenséből ennyire hatékonyan, egyetlen klikkeléssel tudta volna eltüntetni bárkinek a hangját. Nincs ugyanis hatékonyabb kontroll annál, mint amikor az online térben kódok és algoritmusok szereznek érvényt előírásoknak.

57. Annak ellenére, hogy a demokráciák továbbra is nemzetállami keretbe rendeződnek, az internet korában a nyilvános diskurzus túllép a nemzeti határokon: a társadalmi eszmecsere itt nem sok-sok nemzeti szolgáltató, hanem egy-két globális behemót platformján zajlik. A demokráciák nemzeti szintje és a platformok globális jelenléte közti távolságot nemcsak jogi-legitimitási alapon nehéz áthidalni, hanem társadalmi-kulturális okból is, hiszen ezek a szolgáltatók nem (vagy jóval kevésbé) férnek hozzá a lokális környezethez.

58. Az egyik jelentős és újszerű probléma a társadalmi diskurzus szélsőséges széttöredezésének kockázata. Közvélemény szociológiai értelemben csak akkor alakulhat ki, ha az emberek többsége közös információs tapasztalathoz fér hozzá. Ezzel szemben a közösségi platformok által közzétett információkból nyilvánvaló, hogy a szolgáltatókat a tartalmak minél tökéletesebb személyre szabása vezérli ajánlórendszereik fejlesztésekor, és más releváns szempont nem is nagyon jelenik meg az algoritmusaik paramétereiről szóló tájékoztatásban. A visszhangkamrák létét és mértékét érintő bizonytalanságokhoz képest a perszonalizáció

vitathatatlanul veti fel a fragmentáció problémáját: beláthatatlan következményekkel járhat, ha teljes mértékben egyéni szempontok (érdeklődés, ízlés, kedvtelés) szerint alakítjuk, kihez mi jut el a közösségi diskurzusból.

59. A közösségi médiaplatformok ajánlórendszereinek működési sajátosságaiból adódó további kihívás a szélsőséges polarizáció. A közösségi média figyeleméhsége, viralitása és interaktivitása előnyben részesítheti a tudatos megfontolást és átgondolást háttérbe szorító azonnali reakciókat, illetve az emberek identitására és konfliktusaira építő túlzó, szenzációhajhász vagy érzelmekre ható tartalmakat.

60. Bár legkevésbé sem állítható, hogy a dezinformáció probléma újkeletű lenne a társadalmi kommunikációban, arra nézve konszenzus látszik, hogy a belőle fakadó társadalmi költségek mértéke és terjedelme együtt nőtt azzal a forradalommal, amely lehetővé tette, hogy egy üzenetet azonnal és szinte ingyenesen el lehessen juttatni a tömegekhez. Egyes technológiák, például az automatizált szolgáltatások (ún. botok) mesterségesen felerősítik a dezinformáció terjedését, amelyet hamis fiókok is elősegíthetnek, akár nagyszabású koordinációban (ún. 'trollgyárak').

61. A közvélemény alakítását célzó digitális manipulációs és visszaélősszerű tevékenységek, beleértve a botok vagy hamis fiókok használatával végzett összehangolt műveleteket, bármilyen időszakban komoly kérdéseket vetnek föl, de különösen is érzékeny következményekkel járhatnak választási kampányidőszakban. A részvételi és kampányolási lehetőségek bővítése mellett a közösségi média egyszersmind a közvélemény manipulálására és a választási folyamatok integritásának megkérdőjelezésére irányuló akciók, külföldi beavatkozási kísérletek egyik csatornája is lett.

3. Európai eszköztár a demokrácia megerősítésére

62. Európa a közösségi média által teremtett új demokratikus részvételi lehetőségek megőrzése érdekében az alapjogok horizontális hatályának tanát hívta segítségül: a DSA egyrészt átláthatósági (indokolási) és más eljárási szabályokkal, másrészt érdemi korlátok beépítésével igyekszik keretek közé terelni a tartalommoderálást.

63. A DSA 14. cikk (4) bekezdésében foglalt generálklauzula – mely szerint a közvetítő szolgáltatóknak kellő gondossággal, objektíven és arányosan kell eljárniuk a szerződési feltételeik alkalmazása és érvényesítése során, kellően figyelembe véve a felhasználót megillető alapvető jogokat, például a véleménynyilvánítás szabadságát – nem pusztán az indokolási és egyéb eljárási kötelezettségek elvi alapja, hanem önállóan alkalmazandó érdemi szabály.

64. A jogalkalmazás izgalmas kérdése, hogy miként alakíthatók ki azok a tesztek, amelyek feloldják a szolgáltatók speciális és jogos „közösségi” érdekei, valamint a felhasználók szólásszabadsága közötti ütközéseket. Kiindulópontként rögzíthető, hogy minél nagyobb egy platform, vagyis minél inkább általános, mindenki számára nyitott fóruma a társadalmi párbeszédnek, annál kevésbé hivatkozhat sajátos közösségi szempontokra, illetve minél inkább

egy legitim társadalmi vitában való részvételként értelmezendő egy adott véleménynyilvánítás, annál kevésbé hozhatók fel vele szemben jogosnak vélt platformüzemeltetői érdekek.

65. A mércék kialakításában központi szerep hárul a nemzeti bíróságokra mint a nemzeti jogba közvetlenül beépülő uniós rendelet értelmezőire. A DSA 14. cikke így „köldökzsinórt” jelenthet a platformokon folyó kommunikáció és a közvélemény demokratikus, nemzeti közege között: a demokratikus legitimációval rendelkező bíróságok legalább esetileg lehetőséget kapnak arra, hogy a társadalmi párbeszéd legitim demokratikus normáit meghatározzák és érvényesítsék a szolgáltatók eljárásával szemben.

66. A DSA egyik fő célja a transzparens online környezet megteremtése, amely célkitűzés szempontjából kitüntetett jelentősége van a közvélemény formálódására jelentős befolyással lévő ajánlórendszerekre előírt átláthatósági követelményeknek (DSA 27. cikk). Az átláthatósági követelmények nyomán közzétett információk ismeretében összességében azt mondhatjuk, hogy az átláthatóság bizonyos mértékben valóban megteremtette az alapot arra, hogy a platformok működésének valóságát összevessük a közvélemény demokratikus formálódásának kritériumaival. Az ajánlórendszerek működési logikájára és a főbb paraméterekre vonatkozó tájékoztatások alapján kijelenthető, hogy a nagy platformok kizárólag a perszonalizáció jegyében állítják össze a felhasználók számára ajánlott tartalmakat, és algoritmusaik ismertett szempontrendszerében nem tűnik föl olyan tényező, amely hangsúlyt adna a demokratikus közvélemény értékeinek.

67. Az átláthatósági kötelezettségeken túl a DSA a közösségi média társadalmi hatásainak szabályozására óvatos megoldást választott: alapvetően nem jogszabályban foglalt kemény követelményekkel szorítja rá a platformokat bizonyos célok szolgálatára, hanem kockázatértékelés és -csökkentés intézményesítésével próbálja felmérni és kezelhetővé tenni a káros következményeket. Ez a megoldás hivatott arra is, hogy a demokratikus értékek védelmét előmozdítsa.

68. Az óriásplatformok kockázatelemző jelentéseiből megfogalmazhatók azok a következtetések, amelyek a DSA alkalmazásának első fontos tapasztalatát adják, és a jelenlegi törekvések elégtelenségére mutatnak rá:

- A platformok jelentései a demokratikus közvélemény formálódására veszélyt jelentő kockázatok közül néhányal (pl. perszonalizáció és fragmentáció) még csak nem is foglalkoznak.
- A kockázatcsökkentési intézkedések között sok olyat találunk (pl. downranking és upranking), amelynek hatékonysága a szélsőséges perszonalizáció miatt nagyon nehezen vagy egyáltalán nem ellenőrizhető.
- A kockázatértékelő jelentésekben adott információk néha (pl. az interakciók súlyának kérdésében) nincsenek összhangban a transzparenciakövetelmények alapján a felhasználóknak nyújtott nyilvános tájékoztatásokkal.
- A platformok nem foglalkoznak kellő súllyal a közösségi média tevékenységében és hatásában komoly szereppel bíró egyes funkciók működésével. A lájkolással, megosztási lehetőségekkel és egyéb funkciókkal facilitált azonnali, érzelmi alapú interakciók alapvető nyomot hagynak a közösségi diskurzuson, és több kockázat

gyökerét jelentik. A jelentésekből nem olvasható ki olyan intézkedési terv vagy intenzív gondolkodás, amely – legalább bizonyos esetekben – ezeknek a funkcióknak a használatát érintené.

- A platformok ezzel szemben nagy szerepet szánnak és ténylegesen is óriási energiákat fektetnek olyan megoldások kidolgozásába (pl. tényellenőrzés), amelyek hatékonysága megkérdőjelezhető.
- A platformok nem vállalják föl az adott kockázatot egyértelműen nagyobb eséllyel kezelő megoldást, ha az erős hatással járna sikerüket megalapozó működési mechanizmusaikra. Míg a szolgáltatók saját felfogásában is „közösségük alapja a hitelesség”, addig a kockázatcsökkentő intézkedések között – a Facebook politikai hirdetésekre vonatkozó szabályzatának kivételével – nem jelenik meg a hiteles identifikáció kérdése.
- A kockázatértékelési jelentések rendszerének gyenge pontja mutatkozik meg abban, hogy az Európai Bizottság rendkívül lassan végzi el az elemzések értékelését és a kockázatcsökkentő intézkedések megfelelőségének vizsgálatát. Egy olyan gyorsan változó valóságban, mint amelyet a közösségi média digitális működése jelent, bármilyen jogi szabályozás komoly kihívások elé nézne, a nagy átfutási idővel rendelkező eljárások hatékonysága viszont egészen biztosan rendkívül csekély.

69. Egyelőre megalapozottnak tűnik a konklúzió: a platformok kényesen ügyelnek arra, hogy a kockázatok kezelésére hozott intézkedéseik ne érintsék működési mechanizmusuknak az üzleti modelljük számára kiemelten fontos elemeit, így néhány ponton elkerülhetetlennek látszik a demokratikus értékek védelmét zászlajára tűző uniós jog keményebb fellépése. Ennek hiányában nem kérdéses, hogy a platformszabályozás magasztos céljai el fognak bukni a szolgáltatók üzleti modelljének áttörhetetlenségén. A demokratikus közvélemény érdekei szigorúbb beavatkozást indokolhatnak mindenekelőtt az alábbi területeken:

- Nagyon erős érvek szólnak a tartalomkínálat totális személyre szabásának áttörése mellett. Egy olyan kísérlet, amely arra kötelezi a közösségi média platformokat, hogy bizonyos körben általános jelleggel ajánljanak plurális forrásokból származó, a társadalmi viták szempontjából kiemelten fontos tartalmakat, előrelépést jelenthet a fragmentáció, a polarizáció és a dezinformáció tekintetében is.
- Az azonnali, minimális átgondolást is nélkülöző cselekvési lehetőségek (lájkolás, kommentelés, megosztás) finomhangolása, késleltetése értelmes kísérlet lehet arra, hogy a közvélemény formálódásában valamivel nagyobb tér nyíljon a zsigeri reakciókon túli kommunikációnak.
- A közösségi médiában való nyilvános kommunikáció bizonyos körben valódi hitelesítéshez köthető. A fióknyitásnál alkalmazott tényleges azonosítás önmagában csak a szolgáltató felé jelentene nagyobb azonosíthatóságot, és ettől független további kérdés lenne, hogy mely körben maradhatna meg a névtelen vagy álnéven való közlés lehetősége a fiók használója számára. A nyilvánosság és az anonimitás szempontjainak arányos, alapjogokat tiszteletben tartó összehangolása az Emberi Jogok Európai Bíróságának joggyakorlata alapján elvégezhető.

70. Az európai alkotmányjogi megközelítésében nagyon erős érvek szólnak amellett, hogy az államnak ki kell használnia a rendelkezésére álló mozgásteret, és jogi eszközökkel is meg kell próbálnia védeni a demokratikus párbeszédet a közösségi média torzító hatásaitól. Látni kell azonban, hogy a jogi lépések jó esetben egy-két ponton hozhatnak érdemi előrelépést, de valódi áttörés semmiképp sem várható tőlük. A demokrácia betegségeit ugyanis nem a platformok okozták. A diagnózis már megjelenésük előtt felállítható volt, még ha elterjedésük óta romlott is a beteg állapota. A platformszabályozás nem fogja megoldani a demokratikus párbeszéd nyomasztó problémáit, mivel azok a közösségi média szerepénél jóval mélyebb gyökerekkel kapaszkodnak a társadalmi valóságba. A problémák jelentős része, amelyeket sokan a platformok nyakába varrnak, valójában a nyilvánosságunk működésének már meglévő súlyos anomáliáira mutatnak rá.

III. Felforgatott méltóság: az egyén alkotmányjogi pozíciója a digitális valóságban

1. Az emberi méltóság jogi fogalmának új elemei

71. Az újabb infokommunikációs vívmányok már az egyén digitális térben elfoglalt pozíciójának alkotmányjogi fundamentumait érintik és kezdik ki. A mesterséges intelligencia különféle alkalmazásai minden korábbinál közelebb hozták hozzánk a gépek világát. Bizonyos képességeik egyre jobban imitálják azokat a gondolkodási, értékelési és döntéshozatali kvalitásokat, amelyeket mindezidáig kizárólag az embernek tulajdonítottunk. Mindez értelemszerűen azt a kérdést is kiélezte, hogy miben tudjuk megragadni azt a sajátos lényegyet, ami – a gépek működésének határt szabva – továbbra is egyedül az embert jellemzi.

72. Az e tekintetben legfontosabb uniós rendeletek (GDPR, DSA, AIA) egyes szabályai már kimondatlanul is a mögöttes antropológiai kérdésre adnak válaszokat, nem engedve, hogy az emberi személyiséget digitális adatokkal teljes mértékben leírható valóságnak tekintsük. Ezek a válaszok abból a szempontból is kiemelt figyelmet érdemelnek, hogy az emberi méltóság mindig nehezen konkretizálható fogalmának új tartalmi elemeivel gazdagítják az európai jogi gondolkodást. Másrészt a kérdés gyakorlati tétellel is bír, hiszen az emberi méltóság lényeges tartalmához tartozó jogosultságoknak a technológiák gyorsan változó szabályozási környezetében is biztos alappá kell válniuk.

73. Az emberi méltóság fogalmát és (alkotmány)jogban betöltött szerepét hagyományos kettősség lengi körül: egyfelől a nyugati emberi jogi kultúra (sőt az egész alkotmányosság) központi értéke és alapja, amelyen egész alapjogi rendszerünk nyugszik, másfelől önálló konkrét tartalma bizonytalan és állandó viták tárgyát képezi.

74. Az emberi méltóság modern jogi fogalma kezdettől fogva keresi a szekuláris fogódzókat, amelyekbe bárki, világnézeti meggyőződésétől függetlenül belekapaszkodhat, ha az emberi mivolt lényeges elemeit keresi. Az utóbbi évek technológiai fejlődésére reagáló európai jogalkotás figyelemreméltóan aktívnak tekinthető ebben a keresésben. Ahogy ugyanis egyre közelebb férkőznek hozzánk a legújabb technológiai vívmányok, és bizonyos képességeik

egyre jobban hasonlítanak ránk, úgy éleződik ki a kérdés: mi az, ami már csakis az ember lényegéhez tartozik, ezért határt szab a technológiai alkalmazások felforgató erejének.

75. Ha alaposabban szemügyre vesszük a legújabb technológiák európai szabályozását, az új rendelkezések felszíne alatt éppen az történik, amire a szakirodalom az emberi méltóság „specifikációjaként” utal: az uniós rendeletek számos ponton az emberi méltóság elvont tartalmának konkrét, gyakorlati elemeit ragadják meg. Maguk az új szabályok nem neveznek meg az emberi méltóságból kiolvasztott újabb jogokat, de enélkül is világos, hogy számos új rendelkezés valójában az emberi személyről annak sajátos méltósága alapján vallott meggyőződés egy-egy fontos tartalmi jellemzőjét emeli ki.

76. A digitális profilalkotás a konkrét személyhez kötődő információkon alapulva bizonyos mértékben valósághű képet tükröznek vagy tükrözhetnek az egyénről, ami a folyamatok személyre szabásának nagy pontosságával és hatékonyságával kecsegtet. Haszonelvű megközelítésben nagyon úgy tűnik, hogy az automatizált, vagyis teljes mértékben profilozáson alapuló döntés a leghatékonyabb. Áhított hatékonyság ide vagy oda, azt láthatjuk, hogy az európai jogalkotás gátat kíván szabni a folyamatoknak.

77. Már a GDPR is túllépett az adatvédelem szűkebben vett technikai keretein, és jogot adott a kezünkbe az ellen, hogy olyan, joghatással vagy egyéb jelentős hatással járó döntés alanyai legyünk, amelyet kizárólag automatizált módon hoztak meg, ideértve a profilozási eljárásokat is. A DSA pedig egyrészt eleve megtiltja, hogy szenzitív adatok (pl. faji, etnikai hovatartozás vagy politikai vélemény) alapján profilokat állítson fel a platform szolgáltatója, másrészt jogot biztosít a felhasználónak arra, hogy a platformot olyan ajánlórendszer működtetésére szorítsa vele szemben, amely nem profilozáson alapul.

78. Többről van itt szó, mint a profilozási eljárás lehetséges hibáiról, hiszen azokra elég lenne speciális rendelkezésekkel reagálni. A rendeletek összességében azzal szemben nyújtanak védelmet, hogy – ha mi azt nem akarjuk, akkor – ne lehessen adatokból profilt rajzolni rólunk, illetve ne lehessen digitális profilunk alapján automatizált döntést hozni ügyeinkben. E mögött az alapvető követelmény mögött az emberi méltóság olyan értelmezése sejlik föl, amely az emberi személyt léténél fogva többnek tartja múltbéli információkból összeállítható profilnál.

79. Az AIA prediktív algoritmusokra vonatkozó egyes rendelkezéseiből is az a gondolat sejlik fel, hogy az ember mint a cselekvés szabadságának méltóságával rendelkező személy jövőbeli magatartása fogalmilag nem olvasható ki historikus adatokból. Még ha adott esetben döntést is kell hozni a személyével összefüggő várható kockázatokról – például a bűnismétlés veszélyének megítélésekor –, ezt a döntést nem hozhatja meg a kizárólag a digitális profilból dolgozó mesterséges intelligencia. Az ember mindig több marad adatok összességénél, személyisége fogalmilag mélyebb és nyitottabb az adatként megfogható, rögzíthető valóságnál, ezért értékelése sosem bízható kizárólag gépekre

80. Konkrét tilalmak vagy egyéni elutasítás hiányában ugyanakkor lehetőség van digitális profilok és automatizált folyamatok alkalmazására. A szabályozások azonban még ez utóbbi esetben is érvényesítenek olyan határozott követelményt, amely az emberi méltóság elemeként

fogható fel: már a GDPR-ben megjelenik, az AIA-ben pedig részletes követelményrendszerre bővül az emberi beavatkozás kötelező biztosítására vonatkozó elvárása.

81. Honnan ered az a jogunk, hogy ne gépek döntsenek rólunk, hanem egy másik ember értékelje az ügyünket? A döntéshozatal hatékonysága melletti érvek ezzel ellentétes irányt támogatnak. Egyrészt jelentősége van a korábban már kimondott tézisnek, mely szerint az ember sosem lesz leírható digitális információk összességével. Személye léténél fogva kimeríthetetlen mégoly tömeges mennyiségű adat számára is. Másrészt ugyanerre jutunk a másik oldalról, a döntéshozó entitás felől közelítve: a bemeneti adatokba és logikákba zárt gép számára fogalmilag hozzáférhetetlen a digitális információkkal és műveleti szabályokkal le nem írható valóság. Az emberi beavatkozás és felügyelet követelménye attól véd meg minket, hogy olyan döntéshozatali útra lépjünk, amely eleve elveszíti az adatokon túli világ figyelembevételének képességét, ezzel együtt az emberi méltósággal való összhang esélyét.

82. Napjaink gépei a korábbiaknál jóval mélyebbre képesek hatolni az emberi akaratképződés és véleményformálás terepéül szolgáló agyi működésbe. A védelem terén az AIA az első kulcsfontosságú lépést teszi meg, amikor nem csupán alkalmazási feltételeket támaszt, hanem egyenesen betiltja az e tekintetben legveszélyesebb alkalmazásokat. A szabályozás tehát reagál az új kihívásra, és az emberi méltóság új, a gondolat- és vélemény szabadságon túli aspektusaként védelem alá veszi magát a gondolkodási folyamatot, egyfajta „kognitív önrendelkezést” biztosítva az érintetteknek.

83. Ezek az európai fejlemények nagy jelentőséggel bírnak: megmutatkozik bennük a közös európai jogi gondolkodás, amely a racionális hatékonyságot jelentősen növelő technikai eszközökkel szemben több esetben az emberi méltóság értékének ad elsőbbséget. Látnunk kell azonban azt is, hogy a Big Data-probléma méregfogát ezek az európai követelmények sem húzzák ki. A Big Data-probléma méregfoga ugyanis maga a teljes körű digitális adatolás és rögzítés, amelyet sokan újfajta permanens megfigyelésként értékelnek, és kibékíthetetlen ellentétben lévőnek látnak az emberi személy kibontakozásával. Ezeket a megfontolásokat akkor sem söpörhetjük le az asztalról, ha a belőlük fakadó cselekvési tervek kétségkívül utópisztikusak. Innen nézve aggasztó lehet, hogy míg egy-egy újabb alkalmazás vagy esemény kapcsán „minivitákat” folytatunk egyes konkrét témákról, addig rendkívül kevés vita folyik a legfontosabb kérdésről, a tömeges megfigyelések kumulatív hatásáról az emberi személyre.

2. Az információs önrendelkezés délibábja

84. Az információs önrendelkezés koncepciója óriási vívmány volt az európai alkotmányjog számára, ez azonban nem fedheti el azt a valóságot, hogy tényleges érvényesülése a megalkotásától kezdve nehézségekbe ütközött. Már a kibertér igazi berobbanását és az internetes platformok megjelenését megelőzően is olyan környezetben kellett érvényesülnie, amikor az adatkezeléssel érintettek sokkal jobb alkupozícióban lévő gazdasági szereplőkkel találták szemben magukat. A tényleges helyzet – az önrendelkezés garanciális jelentősége mellett is – hamar egyértelművé vált: gazdasági érdekeiket követve vagy a szolgáltatási előnyöket keresve az adatalanyok általában zokszó nélkül megadják a hozzájárulásokat.

85. A kibertér ráadásul eleve (platformok nélkül is) olyan környezetnek tűnt, amelyben különös erővel jelentkeznek az információs önrendelkezés kihívásai. Ennek két fő oka a „tudáshiány” („*knowledge gap*”) és a „beleegyezés tévHITE” („*consent fallacy*”). Az előbbi arra utal, hogy az egyének valójában keveset vagy semmit sem tudnak azokról a körülményekről, amelyek között a személyes adataikat digitálisan gyűjtik, értékesítik vagy feldolgozzák, márpedig ez a széles körű egyéni tudatlanság megakadályozza, hogy az adatvédelmi „piacon” megfelelő normák alakuljanak ki a személyes adatok felhasználására vonatkozóan. A tudatlanság egyrészt az eleve nem transzparens infrastruktúrából (a kódokból), másrészt az átláthatatlanság fenntartásában érdekelt piaci szereplők magatartásából adódik.

86. A „beleegyezés tévHITE” arra utal, hogy a digitális térben nincsenek meg az informált, önkéntes hozzájárulás feltételei. A rendszerszintű tudáshiány aláássa a tényleges informáltságot, és a jól ismert felhasználói reflexek pedig a beleegyezés önkéntességét is megkérdőjelezzik. A hozzájárulás megadása „üres rituálék” keretében történik, amelyben a felhasználók egyáltalán nem veszik a fáradságot az adatkezelés körülményeinek átgondolására, a szolgáltatók pedig nekik kedvező nyelvezetben igyekeznek minél szélesebb körben felhatalmazást nyerni az adatok gyűjtésére.

87. Az internet – az okoseszközök és mindenekelőtt az okostelefonok révén – olyan szinten ágyazódik be a mindennapi életünkbe, ami példa nélküli a korábbi technológiai struktúrákhoz képest. A mindennapi tennivalók sietős intézése közben azonban nem reális az adatvédelmi szempontok lehatárolt, tudatos értékelése: a felhasználók a napi feladataik hatékony elvégzését tartják szemük előtt, és ez törvényszerűen szorítja háttérbe a személyes adataik kezelése fölötti aggodalmakat.

88. A digitalizációban eleve benne rejlő problémákat végképp kiélezte az internetes platformok hatalomátvétele a kibertér működése fölött. A platformok üzleti modellje még inkább felerősítette az informáltság hiányával kapcsolatos nehézségeket, és minden korábbinál nyilvánvalóbbá tette a digitális interakciók egyik velejáróját, az érintettek „adatvédelmi rövidlátását” („*privacy myopia*”). A digitális eszközök és alkalmazások használóinak nincs lehetőségük ténylegesen felmérni vagy értékelni azokat a kockázatokat, amelyek a róluk gyűjtött egyes információtypusokból fakadnak, illetve azt, hogy ezeket az információkat a jövőben miként lehet felhasználni, mivel ezeknek az információknak az értéke kumulatív és kapcsolódó.

89. A platformok azonban nemcsak a korábbi nehézségeket súlyosbították, hanem új frontvonalat is nyitottak az adatvédelem terén: alapvető kihívást intéztek a legfontosabb alkotmányjogi követelményhez, a célhoz kötöttséghez. Minden egyéb (az informáltságot vagy az önkéntességet érintő) bonyodalom mellett is az adatkezelés célja meghatározható és kellőképpen specifikálható volt korábban, mivel valamilyen behatárolható gazdasági tevékenységhez vagy ügýítípushoz kötődött. Az internetes platformoknak az online jelenlétet alapjaiban meghatározó szerepe azzal jár, hogy felhasználók milliói, sőt milliárdjai magánéletük ügyeit ma már túlnyomórészt ezeken a felületeken intézzik, miközben a szolgáltatók több tízezer adatpont alapján minden létező aktivitást rögzítenek.

90. Ahogy az ajánlórendszerek működésénél, úgy az adatok gyűjtése esetében is az a cél áll a platformok működésének középpontjában, hogy a terméket, annak funkcióit, tartalmait az egyéni ízléshez közelítve minél tökéletesebben perszonalizálják, ideértve természetesen a személyes érdeklődésre igényt tartó, targetált reklámokat is. Ezzel a célmegjelöléssel azonban van egy alapvető probléma: egyáltalán nem tölti be a konkretizálás és a releváns adatkör lehatárolásának funkcióját. Mindezek az alapvető problémák tovaryűrűző hatással vannak, és valamennyi követelményre vagy érintetti jogosultságra rányomják a bélyegüket. Konkretizálható cél és lehatárolható adatkör nélkül értelemszerűen az átláthatóság kritériuma sem tudja betölteni rendeltetését.

91. Az a rendezetlenség, amely az alkotmányjog doktrínájának és az információs önrendelkezés digitális valóságának összefüggéseit jellemzi, egy általános probléma egyik első és látványos megmutatkozása. Ez a probléma pedig az alapjogok horizontális hatályának homályossága és gyakorlati tisztázatlansága. A társadalom digitalizálódásával egyre inkább magánszereplők váltak személyes adatok gyűjtőivé, ráadásul egyre nagyobb adatbázisok tekintetében. Érthető és támogatható, hogy az európai jog az adatvédelem kiterjesztésével válaszolt erre, ám a horizontális hatály intézményesítése – amelynek éppen elég kihívás lett volna a magánfelekre irányadó gyakorlati szttenderdek hiánya – dogmatikai bizonytalanságok mellett történt.

92. Alkotmányjogi dogmatikai szempontból önmagában nem aggályos, sőt indokolt lehet, hogy az olyan követelmények, mint a célhoz kötöttség, az informáltság, vagy az adattakarékosság elve más, enyhébb mércét támasszon a magánfél adatkezelővel szemben, mint közhatalmi szervek esetében. A horizontális hatály koncepciójával összeegyeztethető, ha a vállalkozás szabadsága alapján tevékenykedő magánszereplők – a technológiai fejlődés természetszerűen kísérletező jellegét is figyelembe véve – valamelyest nagyobb mozgásteret kapnak a cél (nem) konkretizálása vagy a releváns adatok körének meghatározása terén. Magánfél adatkezelők esetében tehát olyan célok is elfogadhatók lehetnek, amelyek állami szervtől – a kellő konkretizálás hiánya miatt – nem lennének azok.

93. Az információs önrendelkezés koncepciója két okból sem képes a kibertérben a korábbi adatvédelmi szintet nyújtani az egyének számára. Egyrészt a felhasználók gyengébb alapjogi mankókra támaszkodhatnak személyes adataik védelmében, mivel a digitális magánszereplők kezét az alapjog horizontális hatálya kevésbé köti meg, mint a vertikális az állami adatkezelőét. Megköti, de saját érdekeik is sokat nyomnak a latban, és ez nagyobb mozgásteret biztosít nekik. Másrészt ott, ahol ez a védelem nem lenne elég a digitális szférában, az információs önrendelkezés egyébként sem jó alap a védelem sáncainak felépítéséhez, mivel az egyének egész egyszerűen nincsenek abban a helyzetben, hogy saját kezükben tartsák az online folyamatok ellenőrzését. Ha kielégítő védelmet már nem várhatunk az információs önrendelkezés koncepciójától, akkor más megoldások felé kell tekintenünk: az önrendelkezést minimális védelmi szintnek tekintve kiegészítő szabályozási megoldásokra van szükség az egyén digitális pozíciójának megfelelő biztosítására.

94. Az egyik előrelépési lehetőség, hogy célirányos technikai előírásokkal jobban helyzetbe hozzuk az egyént: az architektúrába olyan megoldásokat kell beépíttetni, amelyek lehetővé teszik a gépek közötti adatvédelmi „tárgyalásokat”, és így a felhasználók nevében saját gépeik

tudnának eljárni. Ez azonban az alapvető problémát minden bizonnyal nem oldaná meg, hiszen valójában továbbra is az önrendelkezésre bízna az adatvédelem rendezését: az egyénnek kellene átlátnia az adataira vonatkozó folyamatokat és következményeket, hiszen a saját eszközt valamilyen tartalmi szempontok alapján kellene instruálni.

95. A következő fellépési irány az önrendelkezés helyett a jogviszony másik oldalára, vagyis a szolgáltatókra fókuszál, és információs bizalmasként (*information fiduciary*) szabályozná az infokommunikációs szolgáltatókat, ennek megfelelő speciális státuszbeli követelményeket terhelve rájuk. Információs bizalmasként a közösségi média vállalatokat három fő kötelezettség terhelné: gondossági (*duty of care*), bizalmasági (*duty of confidentiality*) és lojalitási (*duty of loyalty*). Az információs bizalmas koncepciója valós választ jelent az önrendelkezés kihívásaira, és nagyon jó érzékkel emeli középpontba az egyéni felhasználón túli felelősségi kérdéseket. Nem világos azonban, hogyan lehetne összeegyeztetni már meglévő (pl. a részvényesek javára szóló) lojalitási kötelezettségekkel, illetve hogy miként lehetne pontosítani az ügyfélérdekeket a tömeges számú felhasználóval rendelkező platformok esetében. Látni kell továbbá, hogy az információs bizalmas koncepciója többet megválaszolatlanul hagy a kibertér nyomasztó kérdései közül: nem látszik alkalmasnak például a választási beavatkozások, a dezinformáció vagy a gyűlöletkeltés problémájának kezelésére, illetve nem világos a hatása a politikai hirdetések mikrotargetálásának kezelésére sem.

96. A harmadik cselekvési irányt a problémacentrikus, célzott szabályozói beavatkozások jelenthetik. Az alapgondolat megdöbbenően egyszerű: a gyakorlat alapján azonosítani kell az információs önrendelkezés által nem kellően rendezett, ám az egyén védelmét társadalmi okból feltétlenül igénylő helyzeteket, és korlátozásokkal vagy tilalmakkal kell rendbe tenni őket. Hiába az alapgondolat faék egyszerűsége, mégis önálló megoldási irányként kell fókuszba helyezni, mert a tapasztalat azt mutatja, hogy sokszor a felismert szabályozási igény esetén is hallgat vagy kifogásokat keres a jogalkotó. Pedig egy-egy célzott korlátozással, tilalommal vagy előírással a szabályozó akár teljes mértékben megváltoztathatja a piaci folyamatok dinamikáját.

97. A szabályozó feladata, hogy azonosítsa azokat a rossz gyakorlatokat, amelyek már mindenképp jogalkotói, illetve hatósági választ indokolnak. Ezt a folyamatot jól támogathatja, ha a személyes adatok kezeléséhez kötődő magánszféra kérdéseket az egyéni adatkezeléseken túl intézményes, rendszerszintű hatásokat felmérő kockázatalapú megközelítésben is vizsgáljuk. Az a feladat azonban mindenképp a szabályozói felelősséget viselő hatóságokra és jogalkotókra marad, hogy a társadalmi kockázatokat és a szolgáltatók kockázatkezelő affinitását a digitális környezet sajátosságai között értékeljék, és szükség esetén konkrét előírásokkal avatkozzanak be. Ha a lazább, kockázatértékelésen alapuló eljárási kereteket az indokolt esetekben nem egészítik ki keményebb intézkedések, akkor az intézményes hatások kontrollja vágyálom marad.

98. A negyedik lehetséges út a személyes adatok folyamatos rögzítésének, a „digitális megfigyelésnek” a főszabály szerinti tiltása lenne. Bár a kibertér számos nyitott kérdésével csak ez a radikális irány tudná megoldani az egyének védelmében, a társadalmi-gazdasági körülmények tükrében nem érdemes reális lépésként számolni vele.

C) A MONOGRÁFIA IRODALOMJEGYZÉKE

ABIRI, GILAD –GUIDI, SEBASTIAN: The Platform Federation. *Yale Law Journal of Law and Technology*. 26/2. (2024)

ABIRI, GILAD: Moderating from Nowhere. *Brigham Young University Law Review*. 47/3. (2022)

ABIRI, GILAD – BUCHHEIM, JOHANNES: Beyond True and False: Fake News and the Digital Epistemic Divide. *Michigan Technology Law Review*. 29/1. (2022)

AHMED, KAMAL: Zuckerberg: My Facebook manifesto to re-boot globalisation. *BBC.com*. 2017. február 16.

ANANNY, M. – CRAWFORD, K.: Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*. 20/3. (2018)

ARENDT, HANNAH: *Between Past and Future*. New York, Viking, 1968.

AZZI, ADÈLE: The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation. *Jipitec*. 9/2. (2018)

BAGARIC, MIRKO – ALLEN, JAMES: The vacuous concept of dignity. *Journal of Human Rights*. 5. (2006)

BAKER, C. EDWIN: Harm, Liberty, and Free Speech. *Southern California Law Review*. 70/4. (1996-1997)

BAKER, C. EDWIN: *Media, Markets, and Democracy*. Cambridge-New York, Cambridge University Press, 2001.

BALÁS P. ELEMÉR: Személyiségi jog. In: SZLADITS KÁROLY (szerk.): *Magyar magánjog*. Grill Károly könyvkiadóvállalata, 1941.

BALÁZS ZOLTÁN: Emberi méltóság. *Jogelméleti Szemle*. 2005/4.

BALOGH ZSOLT: Az emberi méltóság: jogi absztrakció vagy alanyi jog. *Iustum, aequum, salutare*. 2010/4.

BALKIN, JACK M.: Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. *UC Davis Law Review*. 51/3. (2018)

BALKIN, JACK M.: Old-School/New-School Speech Regulation. *Harvard Law Review*. 127/8.

BALKIN, JACK M.: How to Regulate (and Not Regulate) Social Media. *Journal of Free Speech Law*. 1/1. (2021)

BALKIN, JACK M.: Free Speech is a Triangle. *Columbia Law Review*. 118/7. (2018)

BALKIN, JACK M.: Cultural Democracy and the First Amendment. *Northwestern University Law Review*. 110/5. (2016)

BALKIN, JACK M.: Fixing Social Media's Grand Bargain. *Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper*. 1814. (2018)

BALKIN, JACK M.: Information Fiduciaries and the First Amendment. *U.C. Davis Law Review*. 49/4. (2016)

BALTHASAR, ALEXANDER: A felségjogok átruházása az osztrák szövetségi alkotmány alapján – lehetőségek, keretek és kontroll. In: CHRONOWSKI NÓRA (szerk.): *Szuverenitás és államiság az Európai Unióban: Kortárs kérdések és kihívások*. Budapest, ELTE Eötvös, 2017.

BARLOW, JOHN PERRY: A Declaration of the Independence of Cyberspace. Davos, 1996. február 8.

BAYER, JUDIT: *Digital media regulation within the European Union. A framework for the new media order*. Baden-Baden, Nomos, 2024.

BECKER, SEBASTIAN – PENFRAT, JAN: The DSA Fails to Reign in the Most Harmful Digital Platform Businesses – But It Is Still Useful. In: JORIS VAN HOBOKEN ET AL (szerk.): *Putting the DSA into Practice*. Berlin, Verfassungsbooks, 2023.

BELAND, DANIEL: *States of Global Insecurity: Policy, Politics and Society*. New York, Worth Publishers, 2008.

BELLANOVA, ROCCO – CARRAPICO, HELENA – DUEZ, DENIS: Digital/sovereignty and European security integration: an introduction, *European Security*. 31/3. (2022)

BEN-SHAHAR, OMRI: Data Pollution. *University of Chicago Public Law & Legal Theory Working Paper*. 679. (2018)

BERLINER, DANIEL: The Political Origins of Transparency. *The Journal of Politics*. 76/2. (2014)

BERTRAND, M. – MULLAINATHAN, S.: Are Emily and Greg more employable than Lakisha and Jamal? A field experiment on labor market discrimination. *NBER Working Paper Series*. Working Paper No. 9873.

BEYLEVELD, DERYCK – BROWNSWORD, ROGER: Human Dignity, Human Rights, and Human Genetics. *The Modern Law Review*. 61/5. (1998)

BHAGWAT, ASHUTOSH: Regulating in the Face of Constant Change: The Case of Social Media. In: KROTOSZYNSKI ET AL. (szerk.): *Platform Regulation in the United States and Europe: Across the Great Divide*. Oxford University Press, megjelenés alatt.

BHAGWAT, ASHUTOSH: *Our Democratic First Amendment*. Cambridge, Cambridge University Press, 2020.

BILLER-ANDORNO, NIKOLA ET AL.: *Democracy in the Digital Age*. European Group on Ethics in Science and New Technologies, 2023.

BIRNHACK, MICHAEL D. – ELKIN-KOREN, NIVA: The Invisible Handshake: The Reemergence of the State in the Digital Environment, *Vanderbilt Law Journal* 8/2. (2003)

- BISLEY, NICK: *Rethinking Globalization*. New York, Palgrave Macmillan, 2007.
- BLACKSTONE, SIR WILLIAM: *The Sovereignty of the Law: Selections from Blackstone's Commentaries on the Laws of England* (szerk. GARETH JONES). London, Macmillan, 1973.
- BORK, ROBERT H.: Neutral Principles and Some First Amendment Problems. *Indiana Law Journal* 47/1. (1971)
- BORONKAY MIKLÓS: A képmáshoz és a hangfelvételhez fűződő jog. *In Medias Res*. 2013/1.
- BOTERO ARCILA, BEATRIZ – GRIFFIN, RACHEL: *Social media platforms and challenges for democracy, rule of law and fundamental rights*. European Parliament, 2023.
- BOYLE, JAMES: Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors, *University of Cincinnati Law Review*. 66 (1997. január)
- BRANDEIS, L. D.: What publicity can do. *Harper's Weekly*, 1913. december 20.
- BUBLITZ, JAN CHRISTOPH – MERKEL, REINHARD: Crime against minds: on mental manipulations, harms and a human right to mental self-determination. *Criminal Law and Philosophy*. 8/1. (2014)
- BUBLITZ, JAN CHRISTOPH: Freedom of Thought in the Age of Neuroscience: A Plea and a Proposal for the Renaissance of a Forgotten Fundamental Right. *Archives for Philosophy of Law and Social Philosophy*. 100/1.
- BUSCH, CHRISTOPH – MAK, VANESSA: Putting the Digital Services Act into Context: Bridging the Gap between EU Consumer Law and Platform Regulation. *Journal of European Consumer and Market Law*. 10/3. (2021)
- CALHOUN, BRITT: Shaping the public sphere: English coffeehouses and French salons and the age of the enlightenment. *Colgate Academic Review*. 3/1. (2012)
- CAROZZA, PAOLO G.: Human Dignity and Judicial Interpretation of Human Rights: A Reply. *European Journal of International Law*. 19/5. (2008)
- CASTELLS, MANUEL: *Az identitás hatalma: Az információ kora. Gazdaság, társadalom és kultúra II. kötet*. Budapest, Gondolat-Infonia, 2006.
- CHANDER, ANUPAM – SUN, HAOCHEN: Sovereignty 2.0. *Vanderbilt Journal of Transnational Law* 55/2. (2022)
- CHEMERINSKY, ERWIN: *Constitutional Law*. New York, Aspen Publishers, 2006.
- CHESNEY, BOBBY – CITRON, DANIELLE: Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*. 107/6. (2019)
- CHEUNG, ANNE SY: From Data Subjects to Data Sovereigns: Addressing the Limits of Data Privacy in the Digital Age. In: ANUPAM CHANDER – HAOCHEN SUN (szerk.): *Data Sovereignty*. New York, Oxford University Press, 2023.

CHRISTAKIS, THEODORE: European Digital Sovereignty, Data Protection, and the Push toward Data Localization. In: ANUPAM CHANDER – HAOCHEN SUN (szerk.): *Data Sovereignty*. New York, Oxford University Press, 2023.

CHRISTAKIS, THEODORE: After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe. *European Law Blog*. 2020. július 21.

CHRISTAKIS, THEODORE: “European Digital Sovereignty”: Successfully Navigating between the “Brussels Effect” and Europe’s Quest for Strategic Autonomy. *Studies on Digital Governance* (2020. december) 70.

CHRONOWSKI NÓRA – PETRÉTEI JÓZSEF: Szuverenitás. In: JAKAB ANDRÁS – KÖNCZÖL MIKLÓS – MENYHÁRD ATTILA – SÜLYÖK GÁBOR (szerk.): *Internetes Jogtudományi Enciklopédia (Alkotmányjogi rovat)*.

CITRON, DANIELLE KEATS – PASQUALE, FRANK: The Scored Society: Due Process for Automated Predictions. *Washington Law Review*. 89/1. (2014)

COE, PETER: Anonymity and pseudonymity: Free speech’s problem children. *Media and Arts Law Review*. 22/2. (2018)

COHEN, JULIE E.: *Between Truth and Power: The Legal Constructions of Informational Capitalism*. New York, Oxford University Press, 2019.

COOTER, ROBERT – ULEN, THOMAS: *Law and Economics*. (2nd. ed.). London, Paerson, 1997.

COPLEY, CAROLINE: Merkel fears social bots may manipulate German election. Reuters, 2016. november 24.

COUTURE, STEPHANE – TOUPIN, SOPHIE: What does the notion of „sovereignty” mean when referring to the digital? *New Media & Society*. 21/10. (2019)

CSINK LÓRÁNT – MAYER ANNAMÁRIA: *Variációk a szabályozásra: Önszabályozás, társszabályozás és szabályozó hatóság a médiajogban*. Budapest, Médiatudományi Intézet, 2012.

DASKAL, JENNIFER: The Un-territoriality of Data, *Yale Law Journal* 125/2. (2015)

DATTA, ANUPRIYA: Meta to stop running political ads on Facebook and Instagram. *Euractiv*. 2025. július 25.

DAVENPORT, T. – BECK, J.: *The Attention Economy: Understanding the New Currency of Business*. Cambridge MA, Harvard Business School Press, 2001.

DE GREGORIO, GIOVANNI: *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*. Cambridge, Cambridge University Press, 2022.

DEVINS, CARYN – FELIN, TEPPON – KAUFFMAN, STUART – KOPPL, ROGER: The Law and Big Data. *Cornell Journal of Law and Public Policy*. 27/2. (2018)

- DEZSŐ MÁRTA: A szuverenitás. In: KUKORELLI ISTVÁN (szerk.): *Alkotmánytan*. Budapest, Osiris, 1999.
- DREYER, STEPHAN – SHULTZ, WOLFGANG: *The General Data Protection Regulation and Automated Decision-making: Will it deliver?* Bertelsmann Stiftung, 2019.
- DRINÓCZI TÍMEA: A párbeszéd hatása az állami szuverenitásra. *MTA Law Working Papers*. 2014/27.
- DUNN, JOHN: *Breaking Democracy's Spell*. New Haven-London, Yale University Press, 2014.
- DUPRÉ, CATHRINE: Dignity, Democracy, Civilisation. *Liverpool Law Review*. 33/3. (2012)
- ELMER-DEWITT, PHILIP: First Nation in Cyberspace. *Time International*. 1993. december 6.
- ESKENS, SARAH – TIMMER, JELTE – KOOL, LINDA – VAN EST, RINIE: *Beyond control. Exploratory study on the discourse in Silicon Valley about consumer privacy in the Internet of Things*. Den Haag, Rathenau Instituut, 2016.
- FATIMA, ROUMATE: *Artificial intelligence and the New World order: Frontiers of artificial intelligence, ethics and multidisciplinary applications*. Cham, Springer, 2024.
- FISS, OWEN M.: *Liberalism Divided: Freedom of Speech and the Many Uses of State Power*. Boulder, Westview, 1996.
- FLORIDI, LUCIANO: The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology* 33/3. (2020)
- FOER, FRANKLIN: Facebook's war on free will. *The Guardian*. 2017. szeptember 19.
- FRANTZIOU, ELENI: *The Horizontal Effect of Fundamental Rights in the European Union*. Oxford, Oxford University Press, 2019.
- FRELON, DEEN – WELLS, CHRIS: Disinformation as Political Communication. *Political Communication*. 37/2. (2020)
- FUKUYAMA, FRANCIS: *Államépítés*. Budapest, Századvég, 2005.
- FUKUYAMA, FRANCIS – GROTO, ANDREW: Comparative Media Regulation in the United States and Europe. In: NATHANIEL PERSILY – JOSHUA A. TUCKER (szerk.): *Social Media and Democracy: The State of the Field, Prospects for Reform*. Cambridge University Press, 2020.
- GÁRDOS-OROSZ FRUZZINA: *Alkotmányos polgári jog? Az alapvető jogok alkalmazási a magánjogi jogvitákban*. Budapest-Pécs, Dialóg Campus, 2011.
- GEESE, ALEXANDRA: Why the DSA Could Save Us From the Rise of Authoritarian Regimes. In: JORIS VAN HOBOKEN ET AL (szerk.): *Putting the DSA into Practice*. Berlin, Verfassungsbooks, 2023.
- GORWA, ROBERT – ASH, TIMOTHY GARTON: Democratic Transparency in the Platform Society. In: NATHANIEL PERSILY – JOSHUA A. TUCKER (szerk.): *Social Media and Democracy: The State of the Field, Prospects for Reform*. Cambridge University Press, 2020.

GOSZTONYI GERGELY – LENDVAI GERGELY: Deepfake és dezinformáció: Mit tehet a jog a mélyhamisítással készített álhírek ellen? *Médiakutató*. 25/1. (2024)

GRAFANAKI, SOFIA: Platforms, the First Amendment and Online Speech: Regulating the Filters. *Pace Law Review*. 39/1. (2018)

GRIMM, DIETER: *The Constitution of European Democracy*. Oxford, Oxford University Press, 2017.

GYÖRFI TAMÁS: Az emberi méltósághoz való jog dogmatikai problémái. *Fundamentum*. 2003/1.

HABERMAS, JÜRGEN: Reflections and Hypotheses on a Further Structural Transformation of the Political Public Sphere. *Theory, Culture & Society*. 39/4. (2022)

HARDY, I. TROTTER: The Proper Legal Regime for Cyberspace, *University of Pittsburgh Law Review*. 55 (1994)

HEAD, S. W. – STERLING, C. H.: *Broadcasting in America: A Survey of Television, Radio, and New Technologies (4th ed.)*. Boston, Houghton Mifflin, 1982.

HENKIN, LOUIS: That 'S' Word: Sovereignty, and Globalization, and Human Rights, et Cetera. *Fordham Law Review* 68/1. (1999)

HILLA, JOHN: The Literary Effect of Sovereignty in International Law. *Widener Law Review*. 2008/1.

HIRST, PAUL – THOMPSON, GRAHAM: *Globalization in Question: The International Economy and the Possibilities of Governance*. Cambridge, Polity Press, 1996.

HJARVARD, STIG: The Mediatization of Society: A Theory of the Media as Agents of Social and Cultural Change. *Nordicom Review*. 29. (2008)

HJORT, JONAS – TIAN, LIN: The Economic Impact of Internet Connectivity in Developing Countries. *Annual Review of Economics*. 17. (2025)

HURLEY, MIKELLA – ADEBAYO, JULIUS: Credit Scoring in the Era of Big Data. *The Yale Journal of Law and Technology*. 18. (2016)

JACOBSEN, TRUDY – SAMPFORD, CHARLES – THAKUR, RAMESH (szerk.): *Re-envisioning Sovereignty: The End of Westphalia?* Burlington, Ashgate, 2008.

JAKAB ANDRÁS: *Az európai alkotmányjog nyelve*. Budapest, Nemzeti Közszerzői Egyetem, 2016.

JAKAB ANDRÁS: A szuverenitás fogalmához kapcsolódó kompromisszumos stratégiák, különös tekintettel az európai integrációra. *Európai Jog*. 2006/2.

JAKAB, ANDRÁS: What Can Constitutional Law Do against the Erosion of Democracy and the Rule of Law? On the Interconnectedness of the Protection of Democracy and the Rule of Law. *Constitutional Studies*. 6.

- JELLINEK, GEORG: *Allgemeine Staatslehre*. Berlin, Verlag von O. Häring, 1900.
- JOHNSON, DAVID R. – POST, DAVID: Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*. 48/2. (1996)
- JÓRI ANDRÁS: *Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése*. PhD dolgozat, PTE ÁJK Doktori Iskola, 2009.
- JÓRI ANDRÁS: Adatvédelem: az alapjogvédelmi tesztől az érdekmérlegelésig. *Alkotmánybírósági Szemle*. 2018/1.
- JOSSLINE, DAPHNE – WALLACE, WILLIAM: Non-State Actors in World Politics: A Framework. In: DAPHNE JOSSELINE – WILLIAM WALLACE (szerk.): *Non-State Actors in World Politics*. New York, Palgrave, 2001.
- KARDOS GÁBOR: Az államok szuverén egyenlősége. In: JAKAB ANDRÁS – FEKETE BALÁZS (szerk.): *Internetes Jogtudományi Enciklopédia (Nemzetközi jog rovat)*.
- KATZ, RAUL – CALLORDA, FERNANDO – JUNG, JUAN: *The impact of digital transformation on the economy*. International Telecommunication Union, 2025.
- KELLER, DAPHNE: The European Union's New DSA and the Rest of the World. In: JORIS VAN HOBOKEN ET AL (szerk.): *Putting the DSA into Practice*. Berlin, Verfassungsbooks, 2023.
- KELLO, LUCAS: *The Virtual Weapon and International Order*. New Haven, Yale University Press, 2017.
- KELSEN, HANS: Sovereignty and International Law. *The Georgetown Law Journal*. 48/4. (1960)
- KELSEN, HANS: The Principle of Sovereign Equality of States as a Basis for International Organization. *The Yale Law Journal*. 53/2 (1944)
- KHAN, LINA M. – POZEN, DAVID E.: A Skeptical View of Information Fiduciaries. *Harvard Law Review*. 133/2. (2019)
- KISS JÁNOS: Népszuverenitás. *Fundamentum*. 2006/2.
- KLONICK, KATE: The New Governors: The People, Rules, and Processes Governing Online Speech, *Harvard Law Review*, 131/6. (2018)
- KOLOBA, STEPHAN: The GDPR's extra-territorial scope: data protection in the context of international law and human rights law. *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 80/4. (2020)
- KOLTAY, ANDRÁS: Freedom of Expression and the Regulation of Disinformation in the European Union. In: KROTOSZYNSKI ET AL. (szerk.): *Disinformation, Misinformation, and Democracy*. Cambridge-New York, Cambridge University Press, 2025.
- KORFF, DOUWE – BROWNE, IAN: *The use of the Internet & related services, private life & data protection: trends, technologies, threats and implications*. Council of Europe, 2013.

- KOSACK, S. – FUNG, A.: Does transparency improve governance? *Annual Review of Political Science*. 2014.
- KOSKENNIEMI, MARTTI: *From apology to utopia: The structure of international legal argument*. Lakimiesliiton Kustannus, Helsinki, 1989.
- KRASNER, STEPHEN D.: *Sovereignty: Organized Hypocrisy*. Princeton NJ, Princeton University Press, 1999.
- KROTOSZYNSKI, RONALD J.: Disinformation, Misinformation, and Democracy: Defining the Problem, Identifying Potentially Effective Solutions, and the Merits of Using a Comparative Legal Approach. In: KROTOSZYNSKI ET AL. (szerk.): *Disinformation, Misinformation, and Democracy*. Cambridge-New York, Cambridge University Press, 2025.
- KUNER, CHRISTOPHER: *Transborder Data Flows and Data Privacy Law*. Oxford, Oxford University Press, 2013.
- LEMLEY, MARK A.: The Splinternet. *Duke Law Journal*. 70. (2021)
- LENDVAI GERGELY FERENC: Deepfake a szólásszabadság tükrében – reflexiók a jog perspektívájából. In: ACZÉL PETRA – VESZELSZKI ÁGNES (szerk.): *Deepfake: a valótlán valóság*. Budapest, Gondolat Kiadó, 2023.
- LESSIG, LAWRENCE: *CODE – version 2.0*. New York, Basic Books, 2006.
- LIPPMANN, WALTER: *Public Opinion*. New York, Free Press Paperbacks, 1992.
- LORENZ, NORBERT: *Die Übertragung von Hoheitsrechten auf der Europäischen Gemeinschaften*. Frankfurt am Main, Peter Lang, 1990.
- MAJTÉNYI LÁSZLÓ: A méltóság, a szabadság meg a Sólóyom-életmű. *Élet és irodalom*. 68/51-52. (2024. december 19.)
- MAJTÉNYI LÁSZLÓ: *Az információs szabadságok*. Budapest, Complex, 2006.
- MANYIKA, JAMES – ROXBURGH, CHARLES: *The great transformer: The impact of the Internet on economic growth and prosperity*. McKinsey Global Institute, 2011.
- MADIEGA, TAMBIAA: Digital sovereignty for Europe. *EPRS Ideas Paper* (2020. július).
- MANTELERO, ALESSANDRO: Fundamental Rights Impact Assessment in the DSA. In: JORIS VAN HOBOKEN ET AL (szerk.): *Putting the DSA into Practice*. Berlin, Verfassungsbooks, 2023.
- MATTSON, DAVID – CLARKE, SUSAN: Human dignity in concept and practice. *Policy Sciences*. 44/4. (2011)
- MAYER-SCHÖNBERGER, VIKTOR: Generational Development of Data Protection in Europe. In: PHILIP E. AGRE – MARC ROTENBERG (szerk.): *Technology and Privacy: The New Landscape*. The MIT Press, 2017.
- MEIKLEJOHN, ALEXANDER: The First Amendment is an Absolute. *Supreme Court Review*. 1961 (1961)

METZ, CADE: Now Anyone Can Tap the AI Behind Amazon's Recommendations. *Wired.com*. 2015. április 9.

MICKLITZ, HANS-WOLFGANG ET AL. (szerk.): *Constitutional Challenges in the Algorithmic Society*. Cambridge, Cambridge University Press, 2022.

MIKLÓS GELLÉRT: A deepfake-tartalmak szabályozása az Európai Unió jogában. In: ACZÉL PETRA – VESZELSZKI ÁGNES (szerk.): *Deepfake: a valótilan valóság*. Budapest, Gondolat Kiadó, 2023.

MILLER, ARTHUR R.: *The Assault on Privacy: Computers, Data Banks and Dossiers*. Ann Arbor, University of Michigan Press, 1971.

MITCHELL, WILLIAM J.: *City of Bits: Space, Place, and the Infobahn*. Cambridge, Mass., MIT Press, 1995.

MOUNK, YASCHA: The Undemocratic Dilemma. *Journal of Democracy*. 29/2. (2018)

MRÁZ ATTILA: Deepfake, demokrácia, kampány, szólásszabadság. In: TÖRÖK BERNÁT – ZÓDI ZSOLT (szerk.): *A mesterséges intelligencia szabályozási kihívásai*. Budapest, Ludovika Egyetemi Kiadó, 2021.

MUELLER, MILTON L.: Against Sovereignty in Cyberspace. *International Studies Review* 22 (2020)

NAGY KRISZTINA – POLYÁK GÁBOR: Az internetes forgalomirányító szolgáltatók működésének alapjogi vonatkozásai. *MTA Law Working Papers*. 2018/5.

NAPOLI, PHILIP M.: Access and Fundamental Principles in Communication Policy. *Law Review of Michigan State University Detroit College of Law*. 2002/3. (2002)

NAPOLI, PHILIP M.: Deconstructing the Diversity Principle. *Journal of Communication* 49/4. (1999)

NETANEL, NEIL: Applying Militant Democracy to Defend against Social Media Harms. *Cardozo Law Review*. 45/2. (2023)

NEWMAN, NIC: *Overview and key findings of the 2025 Digital News Report*. Reuters Institute, 2025. június 17.

O'MAHONY, CONOR: There Is No Such Thing as a Right to Dignity. *International Journal of Constitutional Law*. 10/2. sz. (2012)

O'REGAN, ELLEN: Europe's GDPR privacy law is headed for red tape bonfire within 'weeks'. *Politico.eu*. 2025. április 3.

OPPENHEIM, LASSA: *International Law: A Treatise. Vol. I. Peace*. New York-Bombay, Longmans, Green, and Co., 1905.

ORTOLANI, PIETRO: If You Build it, They Will Come. The DSA “Procedure Before Substance” Approach. In: JORIS VAN HOBOKEN ET AL (szerk.): *Putting the DSA into Practice*. Berlin, Verfassungsbooks, 2023.

PAPP JÁNOS: *A közösségi média szabályozása a demokratikus nyilvánosság védelmében*. Budapest, Wolters Kluwer, 2022.

PARISER, ELI: *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*. New York, Penguin, 2011.

PASQUALE, FRANK: Two Visions for Data Governance: Territorial vs. Functional Sovereignty. In: ANUPAM CHANDER – HAOCHEN SUN (szerk.): *Data Sovereignty*. New York, Oxford University Press, 2023.

PASQUALE, FRANK: From Territorial to Functional Sovereignty: The Case of Amazon. *The Law and Political Economy Project Blog*. 2017. december 6.

PATAKI GÁBOR – SZŐKE GERGELY LÁSZLÓ: A Google és a Facebook adatvédelmi tájékoztatási gyakorlata a GDPR szabályozásának tükrében. In: POLYÁK GÁBOR (szerk.): *Algoritmusok, keresők, közösségi oldalak és a jog: A forgalomirányító szolgáltatások szabályozása*. Budapest, HVG-ORAC, 2020.

PETERS, JONATHAN: The “Sovereigns of Cyberspace” and State Action: The First Amendment’s Application (or Lack Thereof) to Third-Party Platforms, *Berkeley Technology Law Journal*. 32/2. (2017)

PETRÉTEI JÓZSEF: *Az alkotmányos demokrácia alapintézményei*. Budapest-Pécs, Dialóg Campus, 2009.

PHILPOTT, DANIEL: Sovereignty. In: GEORGE KLOSKO (szerk.): *The Oxford Handbook of the History of Political Philosophy*. Oxford-New York, Oxford University Press, 2011.

PHILPOTT, DANIEL: Sovereignty: an Introduction and Brief History. *Journal of International Affairs*. 48/2. (1995)

PICCARDI, TIZIANO ET AL.: Social Media Algorithms Can Shape Affective Polarization via Exposure to Antidemocratic Attitudes and Partisan Animosity. *arXiv:2411.14652*

PIERUCCI, FEDERICO: Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. *Digital Society*. 4/27. (2025)

POHLE, JULIA – THIEL, THORSTEN: Digital Sovereignty. *Internet Policy Review*. 9/4.

POLATIN-RAUBEN, DANA – WRIGHT, JOSS: An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. *4th USENIX Workshop on Free and Open Communications on the Internet*.

PONGRÁCZ ALEX: A szuverenitásfogalom változásának 21. századi fejleményei. *Pro Publico Bono*. 2018/2.

- POST, ROBERT C.: Blasphemy, the First Amendment and the Concept of Intrinsic Harm. *Tel Aviv University Studies in Law*. 8. (1988)
- POST, ROBERT C.: The Internet, Democracy, and Misinformation. In: KROTOSZYNSKI ET AL. (szerk.): *Disinformation, Misinformation, and Democracy*. Cambridge-New York, Cambridge University Press, 2025.
- POST, ROBERT C.: The Constitutional Status of Commercial Speech. *UCLA Law Review*. 48/1. (2000-2001)
- POST, ROBERT C.: *Democracy, Expertise, and Academic Freedom*, New Haven-London, Yale University Press, 2012.
- POST, ROBERT C.: Community and the First Amendment. *Arizona State Law Journal*. 29/2. (1997)
- POST, ROBERT C.: Participatory Democracy and Free Speech. *Virginia Law Review*. 97/3. (2011)
- POST, ROBERT C.: Meiklejohn's Mistake: Individual Autonomy and the Reform of Public Discourse. *University of Colorado Law Review*. 64/4. (1993)
- POST, ROBERT C.: Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere. *Duke Law Journal*. 67/5. (2018)
- PURTOVA, NADEZHDA: The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. *Law, Innovation and Technology*. 10/1.
- RICHARDS, NEIL M.: The Dangers of Surveillance, *Harvard Law Review*. 126/7. (2013)
- RILEY, STEPHEN: The Function of Dignity. *Amsterdam Law Forum*. 5/2. (2013)
- RILEY, STEPHEN: Human Dignity: Comparative and Conceptual Debates. *International Journal of Law in Context*. 6/2. (2010)
- ROSENZWEIG, PAUL: The International Governance Framework for Cybersecurity. *Canada-United States Law Journal* 37/2. (2012)
- SANDEL, MICHAEL J.: America's Search for a New Public Philosophy. *Atlantic Monthly*. Mar. 1996.
- SARTORI, GIOVANNI: *Demokrácia*. Budapest, Osiris, 1999.
- SCHAUER, FREDERICK: Categories and the First Amendment: A Play in Three Acts. *Vanderbilt Law Review*. 34/2. (1981)
- SCHAUER, FREDERICK: The Phenomenology of Speech and Harm. *Ethics*, 103/4. (1993)
- SCHAUER, FREDERICK: Harm(s) and the First Amendment. *The Supreme Court Review*. 2011.
- SCHWARTZ, PAUL M.: Privacy and Democracy in Cyberspace. *Vanderbilt Law Review*. 52/6.
- SCOTT, JAMES C.: *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven-London, Yale University Press, 1998.

SETTLE, JAIME E.: *Frenemies: How Social Media Polarizes America*. Cambridge University Press, 2018.

SIMONCINI, ANDREA – LONGO, ERIK: Fundamental Rights and the Rule of Law in the Algorithmic Society. In: HANS-W. MICKLITZ ET AL. (szerk.): *Constitutional Challenges in the Algorithmic Society*. Cambridge-New York, Cambridge University Press, 2022.

SMITH EKSTRAND, VICTORIA – FOX, ASHLEY: Regulating the Political Wild West: State Efforts to Disclose Sources of Online Political Advertising. *Journal of Legislation*. 47/1. (2021)

SPICER, MICHAEL W.: What Do We Mean by Democracy? Reflections on an Essentially Contested Concept and Its Relationship to Politics and Public Administration. *Administration & Society*. 51/5. (2018)

STEVENSON, MEGAN T. – SLOBOGIN, CHRISTOPHER: Algorithmic Risk Assessments and the Double-Edged Sword of Youth. *Washington University Law Review*. 96/3. sz. (2018)

STRAND, ROGER – KAISER, MATTHIAS: *Report on Ethical Issues Raised by Emerging Sciences and Technologies*. Council of Europe, Committee on Bioethics, 2015.

STRANGE, SUSAN: *The Retreat of the State: The Diffusion of Power in the World Economy*. Cambridge, Cambridge University Press, 1996.

SYED, NABIHA: Real Talk About Fake News: Towards a Better Theory for Platform Governance, *The Yale Law Journal Forum*. 127 (2017/2018)

SUSSKIND, JAMIE: *Politika a jövőben. Életünk a technológia uralta világban*. Budapest, Atheneum, 2022.

SUNSTEIN, CASS R.: *Republic.com 2.0*. Princeton, Princeton University Press, 2007.

SUNSTEIN, CASS R.: Is Social Media Good Or Bad for Democracy? *SUR- International Journal on Human Rights*. 15/27. (2018)

SUNSTEIN, CASS R. – VERMEULE, ADRIAN: Conspiracy Theories: Causes and Cures. *Journal of Political Philosophy*. 17/2. (2009)

SVANTESSON, DAN: A Starting Point for Re-thinking “Sovereignty” for the Online Environment. In: ANUPAM CHANDER – HAOCHEN SUN (szerk.): *Data Sovereignty*. New York, Oxford University Press, 2023.

SZABÓ MARCEL – LÁNCZOS PETRA LEA – GYENEY LAURA: *Az Európai Unió jogi fundamentumai*. Budapest, Szent István Társulat, 2014.

SZÁSZ PÉTER: A kaputelefonokat is eléri a GDPR. *Napi.hu*. 2018. október 20.

SZILÁGYI PÉTER: *Jogi alaptan*. Budapest, Osiris, 1998.

SZIKORA TAMÁS: Az online platformokon megjelenő politikai hirdetések szabályozási kihívásai Európában és az Egyesült Államokban. *Iustum Aequum Salutare*. 21/2. (2025)

SZIKORA TAMÁS: Kísérletek a választási deepfake szabályozására az Egyesült Államokban. *ITKI Blog*. 2025. április 1.

TAKÁCS PÉTER: *Államtan*. Budapest, Budapesti Corvinus Egyetem, 2010.

TARDE, GABRIEL: On Communication and Social Influence (szerk. Terry N. Clark) (1969)

THIEL, THORSTEN: A polarizing multiverse? Assessing Habermas' digital update of his public sphere theory. *Constellations*. 30/1. (2023)

TÓTH ANDRÁS: A tisztességes adatkereskedelmet biztosító szabályozás szükségességéről. *Állam- és Jogtudomány*. 2021/3.

TÖRÖK BERNÁT: *Szabadon szólni, demokráciában. A szólásszabadság magyar doktrínája az amerikai jogirodalom tükrében*. Budapest, HVG-ORAC, 2018.

TÖRÖK BERNÁT: Az alkotmányjog horizontális hatálya? Gondolatok az algoritmizált döntéshozatal szabályozásához. In: TÖRÖK BERNÁT – ZÖDI ZSOLT (szerk.): *A mesterséges intelligencia szabályozási kihívásai*. Budapest, Ludovika Egyetemi Kiadó, 2021.

TÖRÖK, BERNÁT: Free Speech Principles to Consider When Restricting Disinformation. *Információs Társadalom*. 24/2.

TÖRÖK, BERNÁT: The Fight against Disinformation in the Council of Europe, and the Relevant Case Law of the European Court of Human Rights. In: KROTOSZYNSKI ET AL. (szerk.): *Disinformation, Misinformation, and Democracy*. Cambridge-New York, Cambridge University Press, 2025.

TUCKER, JOSHUA A. – THEOCHARIS, YANNIS – ROBERTS, MARGARET E. – BARBERA, PABLO: From Liberation to Turmoil: Social Media and Democracy. *Journal of Democracy*. 28/4. (2017)

TUCKER, JOSHUA A. ET AL.: *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, Hewlett Foundation, 2018.

TUFEKCI, ZEYNEP: Algorithmic Harms beyond Facebook and Google: Emergent Challenges of Computational Agency. *Colorado Technology Law Journal*. 13/2. (2015)

VALCKE, PEGGY – CLIFFORD, DAMIAN – DESSERS, VILTE KRISTINA: Constitutional Challenges in the Emotional AI Era. In: HANS-W. MICKLITZ ET AL. (szerk.): *Constitutional Challenges in the Algorithmic Society*. New York-Cambridge, Cambridge University Press, 2022.

VANDER MAELEN, CARL: First of Many? First GDPR Transnational Code of Conduct Officially Approved after EDPB Opinions 16/2021 and 17/2021. *European Data Protection Law Review*. 2021/2.

VAN DER SLOOT, BART – ZUIDERVEEN BORGESIU, FREDERIK: Google and Personal Data Protection. In: A. LOPEZ-TARRUELLA (szerk.): *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*. Asser Press (Springer), 2012.

VAN EST, RINIE: *Intimate technology: The battle for our body and behaviour*. Rathenau Instituut, 2025.

VAN EST, RINIE – GERRITSEN, JOOST: *Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality*. Rathenau Instituut, 2025.

VARGA ZS. ANDRÁS: Magyarország szuverenitása. In: CSINK ET AL. (szerk.): *A magyar közjog alapintézményei*. Budapest, Pázmány Press, 2020.

VON DITFURTH, LUKAS: The European Union's Pursuit of Digital Sovereignty through Legislation. *Jipitec*. 16/2. (2025)

WANG, ANQI: Cyber Sovereignty at Its Boldest: A Chinese Perspective. *The Ohio State Technology Law Journal* 16/2. (2020)

WARDLE, CLAIRE –DERAKHSHAN, HOSSEIN: Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe report DGI(2017)09, Council of Europe, 2nd revised edition, August 2018

WARZEL, CHARLIE: The Fake Nancy Pelosi Video Hijacked Our Attention. Just as Intended. *The New York Times*. 2019. május 26.

WEBSTER, FRANK: *Theories of the Information Society*. Abingdon-New York, Routledge, 1995.

WEISS, LINDA: *The Myth of Powerless State: Governing Economy in a Global Era*. Ithaca NY, Cornell University Press, 1998.

WESTERMAN, PAULINE: *Outsourcing the Law. A Philosophical Perspective on Regulation*. Cheltenham, Edward Elgar Publishing, 2018.

WOLFF, ROBERT PAUL: *In Defense of Anarchism (2. ed.)*. New York, Harper, 1998.

WOODS, ANDREW KEANE: Litigating Data Sovereignty. *Yale Law Journal*. 128/2. (2018)

WOODS, ANDREW KEANE: Against Data Exceptionalism. *Stanford Law Review*. 68. (2016. április)

WOOLLEY, SAMUEL C.: Bots and Computational Propaganda: Automation for Communication and Control. In: NATHANIEL PERSILY – JOSHUA A. TUCKER (szerk.): *Social Media and Democracy: The State of the Field, Prospects for Reform*. Cambridge University Press, 2020.

WU, TIM: *The Attention Merchants: The Epic Scramble to Get Inside Our Heads*. New York, Alfred A. Knopf, 2016.

XU, KE: Data Security Law: Location, Position and Institution Construction. *Business and Economy Law Review* 3. (2019)

YERGIN, DANIEL – STANISLAW, JOSEPH: *The Commanding Heights: The Battle between Government and a Marketplace That is Remaking the Modern World*. New York, Simon & Schuster, 1998.

ZAKARIÁS KINGA: *Az emberi méltósághoz való alapjog. Összehasonlító jogi elemzés a német és a magyar alkotmánybírósági gyakorlat tükrében*. Budapest, Pázmány Press, 2019.

ZARKIN, KIMBERLY A. – ZARKIN, MICHAEL J.: *The Federal Communications Commission: Front Line in the Culture and Regulation Wars*. Westport, Greenwood Press, 2006.

ZIEGELDORF, JAN H. – MORCHON, OSCAR G. – WEHRLE, KLAUS: Privacy in the Internet of Things: Threats and Challenges. *Security and Communication Networks*. 2004/7.

ZINGALES, NICOLO: The DSA as a Paradigm Shift for Online Intermediaries' Due Diligence Hail To Meta-Regulation. In: JORIS VAN HOBOKEN ET AL (szerk.): *Putting the DSA into Practice*. Berlin, Verfassungsbooks, 2023.

ZÖDI ZSOLT (szerk.): *Jogi technológiák. Digitális jogalkalmazás*. Budapest, Ludovika Egyetemi Kiadó, 2022.

ZÖDI ZSOLT: Hogy áll Európa a digitális szuverenitással? *ITKI Blog*. 2025. december 17.

ZÖDI ZSOLT: *Platformjog*. Budapest, Ludovika Egyetemi Kiadó, 2023.

ZÖDI, ZSOLT – BÓDIG, MÁTYÁS: Is Code Destined to Supersede Law? Behavioural Control by Code and Legal Theory. *Cambridge Law Journal* 84/1. (2025)

ZÖDI ZSOLT: Átláthatóság és indokolási követelmények az európai platformjogban. *In Medias Res*. 2023/2.

ZÖDI ZSOLT: A chatbotok használatának szempontjai és korlátai a jogász munkában. *Fontes Juris*. 2025/1-2.

ZUBOFF, SHOSHANA: *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Public Affairs, 2019.