

EMBERI JOGI ASPEKTUSOK A DSA-BAN –
Jó-e, ahogy az alapvető jogokat a DSA védeni akarja?
HOHMANN BALÁZS*

* Egyetemi adjunktus, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar. Email: hohmann.balazs@ajk.pte.hu

Tartalomjegyzék

1. Bevezetés, problémameghatározás.....	3
2. Módszertani megfontolások	5
3. Alapjogi készlet – Az Európai Unió alapvető jogok iránti elkötelezettsége és ennek tükröződése a DSA megalkotásához vezető folyamatba.....	6
4. Az EUB és az EJEB vonatkozó esetjoga a DSA megjelenése előtt	9
5. Az e-kereskedelmi irányelv követelményei	14
6. Az ex ante jellegű követelmények azonosítása a DSA szabályozásában.....	17
6.1 Preambulum	17
6.2 Normatív rendelkezések.....	20
7. A kimutatható joggyakorlatok köre.....	24
8. Következtetések és javaslatok.....	29
8.1 Az ex ante szabályozás alkalmazásának előnyei.....	29
8.2 Az ex ante szabályozás alkalmazásának hátrányai, hiányosságai.....	30
8.3 Konklúzió és javaslatok	33
Irodalomjegyzék.....	37
Internetes hivatkozások listája	40
Felhasznált jogszabályok és döntések listája	42

1. Bevezetés, problémameghatározás

Az elmúlt évek fejlődésének eredményeképpen a digitális tér a modern társadalmak működésének és az egyének mindennapi életének meghatározó részévé vált.¹ Az internet penetráció jelentős kiterjedésével,² a kommunikáció még inkább személyre szabott, interaktív és felhasználó által generált tartalmaival,³ és az online platformok globális méretű elterjedésével új lehetőségeket jöttek létre a közösségi kommunikáció, az információhoz való hozzáférés terén.⁴ A területen kimutatható fejlődés eredményeként már nemcsak technológiaként és infrastruktúraként tekinthetünk a platformokhoz kapcsolódó szolgáltatásokra és eszközökre, hanem komoly, akár döntő befolyásoló tényezővé is váltak a társadalom szinte minden folyamatát tekintve.

Mindez azonban magával hozta a kockázatok és kihívások nagyarányú növekedését is. A digitális platformok működése, pusztán a jellemző és irányadó üzleti modellek és az alkalmazott technológiai megoldások miatt az emberi jogok érvényesítése szempontjából jelentős kihívásokat és kockázatokat rejt magában.⁵ A kockázat egyik fókuszpontját éppen az internet szabadsága adja: az online tér decentralizált és globális természete akadályozza a platformok tagállami (s egyébként akár európai szintű) hatóságok által történő felügyeletét és egyben az uniós szabályozás egységes érvényesítését is megnehezíti.⁶ Az uniós jogalkotás homlokterében éppen a jellemzően EU-n kívüli országokból nyújtott, nagymennyiségű felhasználót elérő, kifejezetten népszerű platformszolgáltatások szabályozása található. Ezeket az uniós jogalkotás igyekszik a szabályozás személyi és tárgyi hatálya alá helyezni, és a Brüsszel hatás⁷ tovább éléseként a platformjog minden szabályozási elemében megjelenik a megoldás, amely áthidalni törekszik a joghatósággal kapcsolatos problémákat.⁸ Eközben a platformok üzleti modelljeinek középpontjában szinte minden esetben a felhasználói adatok gyűjtése és az algoritmusokkal támogatott tartalomajánlás- és moderálás áll,⁹ amelyek jelentős hatást gyakorolnak többek között az információhoz való hozzáférésre, a véleménynyilvánítás szabadságára és a magánélethez való jogra. A platformok működésének egyik gyakorlati

¹ Sergey V. VOLODENKOV – Sergey Nikolaevich FEDORCHENKO – Julia ARTAMONOVA: Sociotechnical reality of the digital space of contemporary politics: structure and features. *Political Expertise*, 18(3), 2022. 230-232.

Hadi RHONDA – Shiri MELUMAD – Eric S. PARK: The Metaverse: A new digital frontier for consumer behavior. *Journal of Consumer Psychology* 34(1), 2024. 142-150.

² Leogrande ANGELO – Alberto COSTANTIELLO – Lucio LAURETI: The Broadband Penetration in Europe. *Journal of Applied Economic Sciences* 16(3), 2021.

³ Zhou, ZIHAN, et al.: A Review of Gaps between Web 4.0 and Web 3.0 Intelligent Network Infrastructure. *2023 IEEE 9th World Forum on Internet of Things (WF-IoT)*. IEEE, 2023.

⁴ PAPP János Tamás. *A közösségi média platformok szabályozása a demokratikus nyilvánosság védelmében*. Budapest, Wolters Kluwer, 2022. 16-50.

⁵ KOLTAY András: *Az új média és a szólásszabadság. A nyilvánosság alkotmányos alapjainak újragondolása*. Budapest, Wolters Kluwer, 405-440.

Giovanni DE GREGORIO: From constitutional freedoms to the power of the platforms: protecting fundamental rights online in the algorithmic society. *European Journal of Legal Studies* 11, 2018. 65.

⁶ Michèle FINCK: Digital co-regulation: designing a supranational legal framework for the platform economy. *European law review* 2018/1.

⁷ A "Brüsszel-hatás" az Európai Unió szabályozási hatásának azt a jelenségét írja le, amelynek során az EU jogalkotása globális szinten is meghatározó normává válik, kiterjedve olyan országokra és szereplőkre is, amelyek korábban nem tartoztak az EU joghatósága alá. Ez a hatás különösen erőteljes az adatvédelem és a fogyasztóvédelem területén.

⁸ KLEIN Tamás: Új terület a jogtudomány horizontján? *Jogtudományi Közlöny*, 2024/3. 134-140.

⁹ Rob FRIEDEN, Rob: The internet of platforms and two-sided markets: Implications for competition and consumers. *Villanova Law Review* 63, 2018. 269.

kihívása és egyben az elemzendő szabályozás egyik fókuszpontja éppen a tartalommoderációs gyakorlatok átláthatósága és jogi megfelelőségének biztosítása lett.¹⁰ A jogellenes tartalmak, például a kiskorúak védelme érdekében, a deepfake, a gyűlöletbeszéd vagy a terrorizmus elleni fellépés mentén alkalmazott moderációs megoldások azonban folyamatosan a „határon” táncolnak: alulműködésük esetén jogellenes tartalmak kerülnek nagy tömegek elé, míg a túl szigorú szabályok szerint haladó moderálás könnyen túlszabályozáshoz vezethetnek.¹¹ A „tűlszűrés” jelensége azt eredményezheti, hogy a platformok az uniós előírásoknak való megfelelés érdekében eltávolítanak olyan tartalmakat is, amelyek jogszerűek, de érzékeny vagy vitatott témákat érintenek. Ez a moderálási gyakorlat komoly veszélyt jelent a véleménynyilvánítás szabadságára,¹² különösen olyan csoportok esetében, amelyek marginalizált nézőpontokat képviselnek. Az online platformok, különösen óriásplatformok és a nagyon népszerű keresőmotorok olyan meghatározó szerepet játszanak az információáramlásban, formálják a közvélemény alakulását,¹³ hogy napjainkra nemcsak a szakirodalomban, hanem az európai szabályozásban is egyre nagyobb szerepet kap a kapuőr jellegű vállalkozásokra vonatkozó követelményrendszer.¹⁴ Az algoritmusok működésével kapcsolatos átláthatóság hiánya további kockázatokat rejt, miközben az algoritmus az online platformok egyik legfontosabb eszköze, amely meghatározza, hogy milyen tartalmakat látnak a felhasználók. Az algoritmusok sokáig az üzemeltető vállalkozások védett ismereteként, üzleti titkaként kerültek kezelésre,¹⁵ amely megnehezítette azok ellenőrzését és a szolgáltatók felelősségre vonását. Az algoritmusok működésével kapcsolatos torzítások, például a politikai nézetek, társadalmi csoportok vagy bizonyos felhasználók hátrányos megkülönböztetése, olyan súlyosan sérthetik az emberi jogok érvényesülését,¹⁶ hogy az európai jogalkotónak határozott szabályozási beavatkozásokat kellett tennie ennek elkerülésére, amelyek jelen tanulmány legfőbb témáját adják, ex ante jellegű emberi jogokat védő mechanizmusokként. A szabályozás egy másik csapásirányát a személyes adatok gyűjtésére és kezelésére vonatkozó gyakorlatok keltették, amelyek szintén jelentős emberi jogi aggályokat vetnek fel. A platformok üzleti

¹⁰ TÖRÖK Bernát: *A szólásszabadság a közösségi platformokon és a Digital Service Act*. In TÖRÖK Bernát – ZÖDI Zsolt (szerk.): *Az internetes platformok kora*. Budapest, Ludovika, 2022. 195-200.

Jens BRUNK – Jana MATTERN – Dennis M. RIEHLE: Effect of transparency and trust on acceptance of automatic online comment moderation systems. *2019 IEEE 21st Conference on Business Informatics (CBI)* 1. IEEE, 2019. SUZOR, Nicolas P., et al.: What do we mean when we talk about transparency? Toward meaningful transparency in commercial content moderation. *International Journal of Communication* 13, 2019. 18.

¹¹ Ld. pl. gyakorlati esettanulmányon keresztül: Heather TILLEWEIN – Keely MOHON-DOYLE – Destiny COX: A Critical Discourse Analysis of Sexual Violence Survivors and Censorship on the Social Media Platform TikTok. *Archives of Sexual Behavior* 2024. 1-10.

¹² Poplett RYAN: Is content moderation a concern that is best left to platforms?. *Ethica* 2, 2022. 73.

¹³ TELEKI Lóránt, GÖNCZÖL Tünde: A digitális kapuőrök az ex ante szabályozás, a versenyjog és az adatvédelem kerestűztében. *Verseny és Szabályozás* 1, 2022. 243.

¹⁴ Egy szolgáltatás akkor válik kapuőr jellegűvé, ha olyan domináns piaci pozíciót foglal el egy digitális piac terén, amely lehetővé teszi számára, hogy jelentős mértékben ellenőrizze a piacra lépést, a forgalmazott termékekhez vagy szolgáltatásokhoz való hozzáférést, s egyúttal markánsan képes legyen a fogyasztók, felhasználók figyelmének irányítására.

Ld. a jelen tanulmányban részletesen nem vizsgált digitális piacokról szóló uniós jogszabály (Digital Market Act, a továbbiakban: DMA) követelményrendszere.

¹⁵ Mauro CONTI, et al.: Revealing The Secret Power: How Algorithms Can Influence Content Visibility on Social Media. *arXiv preprint arXiv:2410.17390*, 2024.

Edouard PIGNOT: Who is pulling the strings in the platform economy? Accounting for the dark and unexpected sides of algorithmic control. *Organization* 30(1), 2023. 140-167.

¹⁶ Tatjana JOVANIĆ: *Platform Regulation: Ex Ante Tools and Strategies in the Regulatory Toolkit*. In Dušan V. POPOVIĆ – Rainer KULMS: *Repositioning Platforms in Digital Market Law*. Cham, Springer Nature Switzerland, 2024. 1-34.

modellje napjainkra egyértelműen kétpiacos,¹⁷ ahol a felhasználóktól szereznek meg nagy mennyiségű személyes adatot. Erre épülően a hirdetési bevételek a minél pontosabb célzással kapcsolódnak össze, amelyek sokszor jogszerűtlenül gyűjtött Big Data adatkészletek összegyűjtésén és kezelésén alapulnak. Mindez nemcsak a magánélethez való jogot sértheti, hanem kiszolgáltatottá teszi a felhasználókat az adatokkal való visszaélésekkel szemben,¹⁸ akkor is, ha az adatokat nem az eredeti adatkezelő, hanem egy visszaélés kapcsán ezekhez hozzájutott személy használja fel.

Az alapjogi megfeleléség eközben kisebb, jellemzően európai székhelyű, honos vállalkozások platformszolgáltatásai esetében jelentősen növelhetik a megfelelésséggel kapcsolatos költségeket és adminisztratív terheket, még akkor is, ha a szabályozói megközelítés kockázatalapú és rétegzett követelményrendszert bont ki.¹⁹ Habár a digitális szolgáltatásokról szóló rendelet (a továbbiakban: DSA),²⁰ e tanulmányban is tárgyalt követelményrendszere e tekintetben elsődlegesen az óriásplatformok és a nagyon népszerű keresőprogramokra állapít meg fokozott alapjogvédelmi kötelezettségeket, a megfelelés kérdése a kisebb platformszolgáltatók esetében is felmerülhet, akik gyakran nem rendelkeznek azokkal az erőforrásokkal, amelyek szükségesek az előírások maradéktalan teljesítéséhez, ami gátolhatja az innovációt, és versenyhátrányt okozhat számukra. Ez pedig hosszú távon a nagy platformok további erősödéséhez vezethet, ami még inkább monopolhelyzetbe hozhatja őket, tovább növelve az emberi jogi kockázatokat.

A DSA által előírt ex ante jellegű alapjogvédelmi és kapcsolódó kockázatértékelési mechanizmusok ugyan kifejezetten fontos szabályozási előrelépést jelentenek a gyakorlatban. Ebben a szabályozási térben elvi jelentőséggel merül fel jelen tanulmány legfőbb kutatási kérdése: valóban ez a szabályozás helyes módja? Képes lesz-e az új szabályanyag ex ante jelleggel kezelni a jellemzően ex post jelleggel felmerülő jogsértéseket és károkat? Milyen jogalkalmazói kihívások várnak a tagállami hatóságokra és az Európai Bizottságra az alapjogvédelmi szabályok mentén?

2. Módszertani megfontolások

A kutatás fő célkitűzése, hogy megvizsgálja a DSA ex ante jellegű alapjogvédelmi szabályait és mechanizmusait, annak szempontjából, hogy ezek az előzetes kockázatkezelési és alapjogvédelmi előírások mennyire illeszkednek azon gyakorlati igényekhez és kihívásokhoz, amelyek a bevezető problémafelvetésében vázolásra kerültek. Az ex ante jellegű mechanizmusok potenciálisan további gyakorlati problémákat okozhatnak vagy oldhatnak meg a DSA-ra vonatkozó jogalkalmazási folyamatok során, amelyek esetében az Európai Unió

¹⁷ Sanjana PARIKH: Defining the Market for Two-Sided Platforms. *Berkeley Technology Law Journal* 34(4), 2019. 1305-1336.

¹⁸ Ld. egy gyakorlati esettanulmányban: Xie WENJING – Kavita KARAN: Consumers' privacy concern and privacy protection on social network sites in the era of big data: Empirical evidence from college students. *Journal of Interactive Advertising* 19(3), 2019. 187-201.

¹⁹ Ld. KIS KELEMEN, Bence – HOHMANN Balázs: Is There Anything New Under the Sun? A Glance at the Digital Services Act and the Digital Markets Act from the Perspective of Digitalisation in the EU Authors. *Croatian Yearbook of European Law & Policy* 19(1), 2023. 225-248.

²⁰ Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet) HL L 277.

tagállamai közötti szabályozási különbségek és a nemzeti szintű jogalkalmazási gyakorlatok eltérései mutatkozhatnak.

A kutatás éppen ezért több módszertani megközelítés kombinációjára épül, amelyek egymást kiegészítve biztosítják az elemzés mélységét és relevanciáját. A tanulmány első fejezetei a szabályozás exogenetikus megközelítésre épülő vizsgálatával foglalkoznak, annak érdekében, hogy feltárható legyen a DSA szabályozása mögött megjelenő jogalkotói szándék és kimutathatóvá váljon az erre irányuló európai jogalkotási folyamatok külső tényezőinek – például politikai, társadalmi és technológiai környezet, érdekek – hatásai is. Mindez lehetővé teszi annak értékelését is, hogy a szabályozás milyen mértékben reflektál a digitális platformok működéséből eredő konkrét alapjogi kockázatokra. Kritikai értékelés alá kerül a DSA szabályozási struktúrájának, különösen az ex ante alapjogvédelmi rendelkezéseinek a köre, annak érdekében, hogy – kiegészítve az exogenetikus elemzést – feltárható legyen a szabályozás mögött meghúzódó jogalkotói szándék és értelmezés az Európai Bizottság és az Európai Parlament dokumentumai alapján. E tekintetben kiemelten foglalkozik a kutatás az ex ante jellegű kötelezettségek szempontjából kiemelt jelentőségű szakaszokkal (így 34. cikk – kockázateértékelés, 35. cikk – kockázatsökkentés), s eközben már előre vetítve vizsgálja azokat a szabályozási megoldásokat, amelyek az alapvető jogok érvényesítésére vonatkozó mechanizmusok tekintetében jogalkalmazási problémákat vetnek fel. Az elemzés ezt követően igyekszik összegyűjteni a gyakorlati jogalkalmazási folyamatok már létező formáit, s mindezek tanulságaiból levonni a következtetést a kutatási kérdésre tekintettel, javaslatokat téve a jogalkalmazási feladatok tagállami szintű érvényesítésére, illetve az ex ante és ex post szabályozási megoldások közötti egyensúly megteremtésére.

3. Alapjogi készlet – Az Európai Unió alapvető jogok iránti elkötelezettsége és ennek tükröződése a DSA megalkotásához vezető folyamatban

Az Európai Unió politikáiban az alapvető jogok védelme nem csupán egy alapelv, hanem a közösség működésének és identitásának fundamentuma.²¹ Ez az elköteleződés az Unió alapító szerződéseiből, politikai stratégiáiból és a jogalkotás során alkalmazott normákból egyaránt fakad. Az EU célja, hogy az emberi méltóság, a szabadság, az egyenlőség, a demokrácia és a jogállamiság elvein alapuló térséget hozzon létre, ahol az alapvető jogok érvényesítése minden uniós politika szövetébe beépül.²² Éppen ezért a DSA ex ante alapjogi szabályainak megítélésekor e szerves fejlődést figyelembe kell venni és rendszertanilag e fejlődés eredményeként tekinteni a megalkotott szabályozási megoldásokra – hiszen mindez meghatározza az ex ante alapjog védelmi intézkedések által védeni kívánt, platformok működése szempontjából is kiemelt jelentőségű emberi jogokat és a szabályozási kereteket is a DSA követelményeinek érvényesüléséhez és egyben helytálló értelmezéséhez.

Az EU jogi és politikai alapját képező szerződések, különösen az Európai Unióról szóló szerződés (továbbiakban: EUSZ),²³ és az Európai Unió működéséről szóló szerződés (továbbiakban: EUMSZ),²⁴ teremtik meg az alapvető jogok érvényesítésének alapját, azzal,

²¹ Tobias LOCK: Rights and principles in the EU Charter of Fundamental Rights. *Common Market Law Review* 56(5), 2019.

²² Irakiza DIVIN DE BUFFALO: The charter of fundamental rights, the aims of EU competition law and data protection: Time to level the playing field. *Singapore Journal of Legal Studies*, 2021. 39-55.

KLEIN Tamás: Platform Regulation and the Protection of Fundamental Rights. *Symbolon* 25(2), 2024. 18-20.

²³ Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata. HL C 326., 2012.10.26.

²⁴ Az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata. HL C 326., 2012.10.26.

hogy alapvető fontosságot tulajdonítanak az alapvető jogok védelmének. Az EUSZ 2. cikke kimondja, hogy az Unió az emberi méltóság, a szabadság, a demokrácia, az egyenlőség, a jogállamiság és az emberi jogok tiszteletben tartásán alapul. Ez az alapvető jogok tiszteletben tartását az EU teljes jogrendjének alapjává teszi, még akkor is, ha ezek meglehetősen általános megfogalmazásban kerültek a normaszövegbe. Ezt egészíti ki az EUSZ 3. cikkének (1) bekezdése is, amely szerint az EU egyik fő célja az általa vallott értékek, így az emberi jogok és alapvető szabadságok előmozdítása, amely érvényesül mind az Unió területén, mind annak globális szerepvállalásában. Ez a cél közvetlenül összefügg a DSA globális hatásával, amelynek egyik ambíciója az uniós alapvető jogi normák érvényre juttatása a globalizált digitális világban.

A szabályokat tekintve 2007-es Lisszaboni Szerződés²⁵ fontos fordulópont volt, hiszen kötelező jogi erővel ruházta fel az Európai Unió Alapjogi Chartáját, annak elismerését. Ennek segítségével az EUSZ 6. cikke elismeri az Alapjogi Chartát,²⁶ mint az EU alapvető jogi dokumentumát, és megerősíti az Európa Tanács Emberi Jogok Európai Egyezményéhez (a továbbiakban: EJE) való csatlakozási szándékot.

Ettől kezdve igazán értelmezhetővé válik az EU politikai és szabályozási tevékenységeiben az alapvető jogok horizontális szempontként való érvényesítése,²⁷ vagyis minden területen és szakpolitikában figyelembe kell venni őket és a szabályozást úgy kell összehangolni, hogy a legmagasabb szintű alapjog védelem legyen megvalósítható. Ez adja meg az alaphangot a digitális tér szabályozásához is. A digitális tér, amely a bevezetőben vázoltak szerint az emberek mindennapi életének, a gazdaság működésének és a társadalmi interakciók színterének egyre fontosabb részévé válik és ez a fejlődési folyamat várhatóan tovább folytatódik, így kerül az alapjogi szabályozás homlokterébe.

Az Alapjogi Charta a DSA alapvető emberi jogi vonatkozásainak legfontosabb hivatkozási alapjának tekinthető. A Charta-ba foglalt emberi jogok közül több olyan azonosítható, amely kiemelt jelentőséggel bír majd a DSA ex ante alapjog védelmi szabályainak szempontjából, mert azok erőteljesen kapcsolódnak a platformok működéséhez, jellemző kockázataikhoz. Azt fontos közreadni, hogy az Alapjogi Charta megközelítésmódjában rendszerint passzív, tisztelettartási, tartózkodási kötelezettségeket fogalmaz meg, építve az alapjogok védelmének vertikális szerkezetére,²⁸ s ez önmagában is dilemmára ad okot a DSA ex ante jellegű megközelítéseivel szemben. A releváns emberi- és alapvető jogok azonosítása és vizsgálata azért is különösen fontos, mert az ex ante alapjog védelmi intézkedések, követelmények hatékonysága csak a tekintetben ítéltető meg, hogy az eredetileg védett alapvető és emberi jogi jogosultság érvényesülését milyen mértékben, módon segíti elő. A Charta követelményrendszerében kiemelhető annak 1. cikkébe foglalt emberi méltóság tiszteletben tartása, amely minden modern alapjogi készlet alapja, s mint anyajog, sok esetben kerül elő a jogalkalmazási folyamatokban, így például az online térben megjelenő emberi méltóságot sértő tartalmak jogi megítélése esetén, a gyűlöletbeszéd és a zaklatás elleni fellépés keretében. A Charta 7-8. cikkében közreadott magánélet és a családi élet tiszteletben tartása, valamint a

²⁵ Lisszaboni Szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról, HL C 306. 2007.12.17.

²⁶ Az Európai Unió Alapjogi Chartája. HL C 326., 26/10/2012

²⁷ Eleni FRANTZIOU: The horizontal effect of the charter of fundamental rights of the EU: rediscovering the reasons for horizontality." *European Law Journal* 21(5), 2015. 657-679.

²⁸ KLEIN Tamás: *A DSA alapjogvédelmi mechanizmusa mint alkotmányjogi novum*. In: KOLTAY András – SZIKORA, Tamás – LAPSÁNSZKY András (szerk.): *A vadnyugat vége? Tanulmányok az Európai Unió platformszabályozásáról*. Budapest, ORAC Kiadó, 2024. 275. (2024a)

személyes adatok védelme szintén különös jelentőséggel bírnak, mert a digitális térben a magánélet védelme kiemelt jelentőségű, különösen a platformok gyakorlatában megjelenő tömeges adatgyűjtés és jogszerűtlen felhasználás, valamint ennek speciális védelmi kategóriái (így a kiskorúak és sérülékeny csoportok védelme szempontjából vagy éppen a különleges személyes adatok felhasználása) tekintetében. E tekintetben külön említendő a Charta 24. cikke, amely a gyermekek jogainak megjelenítésével vázolja fel a DSA szempontjából is fontos védendő értékeket – ezek vonatkozásában értelmezhetőek azok a szabályok, amelyek a gyermekek platformokon és online térben való védelméről rendelkeznek. A platformok tartalommoderálási és algoritmusvezérelt folyamataira tekintettel különös jelentősége van a Charta 11. cikkébe foglalt véleménynyilvánítás és a tájékozódás szabadságának, amelyen keresztül az Unió biztosítja a szabad véleménynyilvánításhoz és az információhoz való hozzáféréshez fűződő jogot, amely a DSA szabályozásának is központi alapvetése, érvényesítendő követelménye lett. Hasonlóan fontosnak tekinthető a Charta 21. cikke, amely a megkülönböztetés tilalmáról szól, s különösen fontos lehet az algoritmusok működésének és a digitális platformok gyakorlatainak vizsgálata során. Ezt kiegészítendő a Charta 47. cikke, amelyben a hatékony jogorvoslati jog és a tisztességes eljárás követelményei megjelennek, szintén fontos lehet, hiszen erre alapozható a DSA követelményrendszerében kibontott belső panaszkezelési rendszer és többek között az a követelmény is, hogy az elsődlegesen tartalommoderációs tevékenységgel kapcsolatos panaszokat nem lehet teljesen automatizált módon elbírálni, abban emberi közreműködést kell biztosítani.

Szintén a Lisszaboni szerződés hatályba lépése után az EUSZ által elismert Európa Tanács Emberi Jogok Európai Egyezménye (továbbiakban: EJEE) szintén meghatározó szerepet játszik az uniós alapjogi keretrendszerben, és ezáltal közvetett hatást gyakorol a DSA szabályozására. Ezek közül kiemelhető az 8. cikk, amely a magán- és családi élet tiszteletben tartásához való jogot, és a 10. cikk, amely a véleménynyilvánítás szabadságát biztosítja. Az EJEE értelmezése az Emberi Jogok Európai Bíróságának ítélkezési gyakorlatán keresztül különösen fontos iránymutatást ad a DSA alapjogi megfeleléséhez.

Az EUSZ-be foglalt szabályokat az EUMSZ számos rendelkezéssel egészíti ki, amely releváns lehet a DSA alapjogi keretrendszerének vizsgálata során is, holott ritkábban vizsgált kiindulási pont a megvizsgált szakirodalom körében. Ebben kiemelt jelentőségű az V. cím alatt található, szabadságon, biztonságon és a jog érvényesülésén alapuló térség címet viselő része, amely a 67. cikkbe foglaltak mentén megerősíti az EUSZ szabályozási irányait, különösen annak (1) bekezdése, amely szerint: „(1) Az Unió egy, a szabadságon, a biztonságon és a jog érvényesülésén alapuló térséget alkot, amelyben **tiszteletben tartják az alapvető jogokat és a tagállamok eltérő jogrendszereit és jogi hagyományait.**” Tekintettel arra, hogy a digitális térben az európai állampolgárok és az Európában tartózkodó személyek sok esetben nem csak felhasználói, hanem fogyasztói is az érintett platformszolgáltatásoknak²⁹, ezért kiemelendő az EUMSZ 169. cikke, különösen annak (1) bekezdése, miszerint: „A fogyasztói érdekek érvényesülésének előmozdítása és a fogyasztóvédelem magas szintjének biztosítása érdekében az Unió hozzájárul a fogyasztók egészségének, biztonságának és gazdasági érdekeinek védelméhez, valamint a tájékoztatáshoz, oktatáshoz és az érdekeik védelmét célzó önszerveződéshez való jogaik megerősítéséhez.” E hozzájárulást a (2) bekezdés szerint a belső piac megvalósításával összefüggésben elfogadott intézkedésekben és a tagállami politikát támogató, kiegészítő, figyelemmel kísért intézkedésekben hozza létre az Unió, amely

²⁹ Ennek részletes értelmezését ld. HOHMANN Balázs: *A DSA és a DMA fogyasztóvédelmi irányai a békéltető testületi és hatósági jogalkalmazás tükrében.* In: KOLTAY András – SZIKORA, Tamás – LAPSÁNSZKY András (szerk.): *A vadnyugat vége? Tanulmányok az Európai Unió platformszabályozásáról.* Budapest, ORAC Kiadó, 2024.133-153.

irányultság szintén megjelenik a DSA vizsgált követelményrendszerében, a digitális szolgáltatásokkal összefüggő kockázatokra tekintettel.

A stratégiai dokumentumok köréből kiemelhető e körben az Európai Bizottság 2018-as ajánlása az illegális online tartalmak hatékony kezeléséről,³⁰ amely iránymutatást adott az online platformok vonatkozásában az illegális tartalmak kezelésére, hangsúlyozva az alapvető jogok, így kiemelten a véleménynyilvánítás szabadságának tiszteletben tartását.

Erre tekintettel készült el a Bizottság közleménye Európa digitális jövőjének tervezésének tárgyában,³¹ amely alapját képezte a platformjogi szabályozást adó DSA és DMA megalkotási folyamatában is. A Bizottság ebben a közleményben meghatározta az EU digitális stratégiáját, kiemelve a digitális szolgáltatások felelősségteljes szabályozásának szükségességét az alapvető jogok védelme érdekében. A dokumentum hangsúlyozta a biztonságos és tisztességes digitális környezet megteremtését is. A szabályozási igényt tovább erősítette az Európai Parlament állásfoglalása az Alapjogi Charta végrehajtásáról,³² amelyben értékelte az Alapjogi Charta végrehajtását, és ajánlásokat tett az alapvető jogok hatékonyabb védelmére az EU legfőbb politikáiban, beleértve a digitális szolgáltatások szabályozását is. A Bizottság végül, közvetlenül a DSA javaslatának benyújtása előtt pár nappal közleményt tett közzé az Európai Demokráciára vonatkozó cselekvési tervről,³³ amelyben kiemelte az alapjogok következetes védelmének fontosságát a demokratikus folyamatok digitális védelme érdekében.

4. Az EUB és az EJEB vonatkozó esetjoga a DSA megjelenése előtt

Annak érdekében, hogy a DSA ex ante alapjog védelmi mechanizmusainak vonatkozásában megítélhetővé váljon a védeni kívánt alapjogok érvényesíthetősége, célszerű áttekinteni az Európai Unió Bírósága (továbbiakban: EUB) és az Emberi Jogok Európai Bíróságának (továbbiakban: EJEB) azon ítéleteit. Ezek közül azok kerülnek a tanulmányban elemzésre, amelyek a védett alapjog szempontjából erőteljesen kapcsolódnak a DSA által szabályozott szolgáltatásokhoz, abból a célból, hogy az esetjog tanulságai iránymutatást nyújtsanak a DSA új ex ante alapjogi szabályozásának megítéléséhez.

A döntések vizsgálatához szükség van arra, hogy foglalkozzunk az EU és az Amerikai Egyesült Államok (továbbiakban: USA) platformok alapvető jogi megfelelésére vonatkozó, eltérő szabályozási irányjaival, mert ennek tükrében ítéltető meg teljességgel a DSA-ban kibontakoztatott szabályozási irány. A legfontosabb különbségek a platformszolgáltatók felelősségében mutatkoznak a jogszerűtlen tartalmak kezelése, a platformokon zajló adatkezelési folyamatok és tartalommoderálás megfelelésége kapcsán.

Az USA-ban a platformszolgáltatók felelősségét leginkább a szövetségi szinten meghozott, 1996-os Communication Decency Act (CDA) 230. szakasza határozza meg. Ez a rendelkezés szinte teljes immunitást, felelősségmentességet biztosít a platformoknak a felhasználók által

³⁰ A Bizottság (EU) 2018/334 ajánlása (2018. március 1.) az illegális online tartalom hatékony kezelésére irányuló intézkedésekről C/2018/1177

³¹ A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Európa digitális jövőjének megtervezése. COM/2020/67 final

³² Az Európai Parlament 2019. február 12-i állásfoglalása az Európai Unió Alapjogi Chartájának végrehajtásáról az Unió intézményi keretében (2017/2089(INI))

³³ A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az Európai Demokráciára vonatkozó cselekvési tervről COM/2020/790 final

feltöltött tartalmakért, még akkor is, ha tudomásuk van a tartalom jogszerűtlenségéről. Ugyanazon szakasz alpontja (c(2) alpont) tartalmazza az úgynevezett „jó samaritánus” klauzulát, amely felelősségmentességet biztosít a szolgáltatóknak a polgári jogi felelősséggel szemben is, amennyiben jóhiszeműség mutatható ki a platformszolgáltatók tartalommoderálási tevékenysége kapcsán. E szabályozás jelentős előnye, hogy támogatja a digitális piac fejlődését (legalábbis annak kezdő időszakában), az innovációt és a szabad véleménynyilvánítást, azonban jelentős kritikák is érték, mivel a tartalom moderálásának gyakorlatában túlzottan elnéző a szolgáltatókkal és nem ösztönzi őket beavatkozásra,³⁴ még abban az esetben sem, amikor válsághelyzetet kellene elhárítaniuk tevékenységük során.

A jogszabályi követelménybe foglalt immunitási szabályokat még tovább erősítette az amerikai bírósági gyakorlat: az egyik első kimutatható az USA Negyedik Körzeti Fellebbviteli Bírósága *Zeran v. America Online* ügyben (1997) a bíróság kimondta, hogy az online szolgáltatók nem felelősek a harmadik féltől származó tartalmakért, még akkor sem, ha azok károsak vagy jogellenesek. Ez az eset precedenst teremtett, amely szerint az online platformok mentesülhetnek a felelősség alól, még ha értesítették is őket a tartalom jogellenes jellegéről. A *Blumenthal v. Drudge* ügyben (1998) Columbia Kerületi Bírósága rámutatott, hogy a platformok még abban az esetben is mentesülnek a felelősség alól, ha moderálták az érintett tartalmat, amennyiben nem mutathatók ki a tartalomszolgáltatás további feltételei. A *Doe v. America Online* ügyben (2001) a Floridai Legfelsőbb Bíróság, majd a *Doe v. MySpace* ügyben (2008) a Texas Nyugati Körzetének Kerületi Bírósága megerősítette, hogy a szolgáltató nem felelős a harmadik féltől származó jogellenes tartalmakért, mivel a 230. szakasz védelmet nyújt az ilyen helyzetekben. A bírósági joggyakorlat odáig is eljutott, hogy 2014-ben a *Jones v. Dirty World Entertainment Recordings LLC* ügyben a Hatodik Körzeti Fellebbviteli Bíróság kérésre meghatározta, hogy a platform nem minősül tartalomszerkesztési tevékenységnek, és ezért a 230. szakasz védelmet nyújtott számára.

Az elmúlt években az USA-ban számos reformjavaslat látott napvilágot, amelyek a CDA 230-as szakasz átfogó felülvizsgálatát szorgalmazzák.³⁵ Egyes javaslatok kiterjesztenék a felelősség megállapíthatóságát bizonyos tartalmak, mint például a gyermekek védelme, szexuális visszaélések vagy a terrorizmus támogatása terén, mások a moderálási folyamatok átláthatóságát követelnék meg, de ezek közül egyedül a szexuális jellegű jogellenes tartalmak terén hozott változást az úgynevezett *FOSTA-SESTA* (2018) jogszabálycsomag, amely kivételt teremtett a szakasz alkalmazása alól az online szexkereskedelemmel kapcsolatos tartalmak esetében.

Ehhez képest az európai bírósági jogértelmezés még tovább vitte, erősítette az alapjogok védelmét. Az esetek közül kiemelt jelentőséggel bírnak az úgynevezett Schrems ügyek (Schrems I (C-362/14) illetve Schrems II (C-311/18)). Az esetek alapját az adta, hogy az amerikai szabályozási környezet és a Safe Harbor mechanizmusai nem biztosították az európai adatvédelmi és alapjogi szabályozásnak megfelelő védelmi szintet a személyes adatok USA-ba történő továbbításakor, s ezáltal megsértették az Alapjogi Charta 7. és 8. cikkében foglalt, a

³⁴ GOSZTONYI Gergely: Az internetes tartalomszabályozással kapcsolatos új gondolkodási irányok az Amerikai Egyesült Államokban. *Miskolci Jogi Szemle* 16(4), 2021. 40-54.

³⁵ Michael L. RUSTAD – Thomas H. KOENIG: The Case for a CDA Section 230 Notice-and-Takedown Duty. *Nevada Law Journal* 23, 2022. 533.

személyes adatok védelméhez és a magánélet védelméhez való jogot.³⁶ Mind a Safe Harbor, mind pedig a Privacy Shield egy *soft law* jellegű szabálygyűjtemény volt, amely iránymutatással tartalmazott követendő irányokat az adattovábbítási tevékenységben érdekelt vállalatok és szervezetek számára a személyes adatok védelme tekintetében, akik saját maguk dönthettek, hogy a megfelelés érdekében milyen mélységű szabályokat vezetnek be. A rendszer leggyengébb pontjait az adta, hogy nem biztosított hatékony jogérvényesítési lehetőségeket az érintettek számára, és az, hogy az amerikai titkosszolgálat szinte minden akadály nélkül betekinthezett bármely a platformokon átáramló adatkezelési folyamatba. Mindez pedig nem felelt meg a döntések időpontjában hatályos európai adatvédelmi szabályoknak és az Alapjogi Charta által biztosított jogoknak és szabadságoknak. A bírósági eljárások végül elvezettek oda, hogy előbb a Bizottság által megállapított Safe Harbor rendszert jóváhagyó megfeleléségi határozat,³⁷ majd az ennek érvénytelensége nyomán létrejött Privacy Shield rendszert jóváhagyó megfeleléségi határozat,³⁸ vált érvénytelenné.

Az eset elemzése útján megállapítható, hogy amennyiben a DSA-ban megjelenő ex ante alapjog védelmi mechanizmusok, így a rendszeresen vizsgált kockázatelemzés, a kockázatsökkentésre irányuló intézkedések és a platformokra vonatkozó átláthatósági és adatvédelmi követelményrendszer érvényesült volna a tényállás alapját képező adattovábbítási helyzetben, akkor a Safe Harbor gyengeségei várhatóan már a harmadik országba történő adattovábbítást lehetővé tevő bizottsági határozat kialakítási folyamatában előre azonosíthatók lettek volna, még akkor is, ha ezek az ex ante kötelezettségek a harmadik országbeli adatkezelőket érintették volna elsődlegesen. Végül a Schrems ügyek speciális hozadékaként előrelendült az európai jogalkotás és elfogadták az általános adatvédelmi rendeletet,³⁹ azonban ennek szigorú követelményrendszere ellenére napjainkig sem sikerült minden, a transzatlanti jogszerűtlen adattovábbításból eredő kockázatot megfelelően kezelni, továbbra is aggályos jogi keretek között üzemelnek a legnagyobb közösségi platformok az adatvédelmi követelmények teljesítése szempontjából,⁴⁰ amely eközben hatalmas károkat okoz a személyes adatok továbbításának más, közcélú területein.⁴¹

A Fashion ID kontra Verbraucherzentrale NRW eV (C-40/17) ügy kapcsán, hasonló következtetésre jutunk. Amennyiben a DSA szerinti ex ante alapjogvédelmi mechanizmusok üzemeltek volna és az adatvédelmi szabályokat következetesen magas szinten alkalmazták volna az alapul fekvő ügyben, a vizsgált esetben nem került volna sor a személyes adatok védelméhez és a magánélethez való jog sérelmére. Az ügyben Fashion ID weboldalán

³⁶ KIS KELEMEN Bence – HOHMANN Balázs: A Schrems ítélet hatásai az európai uniós és magyar adattovábbítási gyakorlatokra. *Infokommunikáció és Jog* 13, 2016. 64-70.

³⁷ A Bizottság határozata (2000. július 26.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott biztonságos kikötő adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről. HL L 215.

³⁸ A Bizottság (EU) 2016/1250 végrehajtási határozata (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről. C/2016/4176 HL L 207.

³⁹ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) HL L 119.

⁴⁰ Giovanni TRICCO: The New Transatlantic Data Agreement Placed in Context: Decoding the Schrems Saga Within the Digital Economy. *Journal of Law, Market & Innovation* 3(1), 2024. 82-110.

⁴¹ Ld. pl. Teodora LALOVA-SPINKS, et al.: EU-US data transfers: an enduring challenge for health research collaborations. *Digital Medicine* 7(1), 2024. 215.

Julie HOUILLON-LEONIS: Avenues for Future Transatlantic Transfers of Health Data: Is Less More?. *Global Privacy Law Review* 4(4), 2023.

elhelyezett Facebook-lájkgomb révén a látogatók személyes adatai azok hozzájárulása nélkül, más indokolható és előre meghatározott jogalap és cél nélkül kerültek a Facebook üzemeltetőjéhez, anélkül, hogy a felhasználók tudomással bírtak volna erről. Az EUB kimondta, hogy a weboldal üzemeltetője és a Facebook együttes adatkezelőknak minősülnek, így mindkét fél felelős az adatkezelési szabályok betartásáért, a kockázatértékelési kötelezettség alapján pedig, amelyet a DSA szerint minden a Facebook-hoz hasonló óriásplatform üzemeltetőjének el kell végeznie és intézkedéseket kell hoznia a kockázatok csökkentésére, megállapításra került volna a fenti alapjogokat sértő, elfogadhatatlan mértékű kockázat, amely a konkrét adatkezelés megkezdése előtt kimutathatóvá tette volna a jogszerűtlen gyakorlatot.

A Schrems ügyhöz hasonlóan a González ügyben (C-131/12), a személyes adatok és a magánélet védelme, illetve az emberi méltóság volt az ügy középpontjában. Az ügy alapját szolgáló esetben a spanyol adatvédelmi hatóság azt vizsgálta, hogy a Google keresőmotor által megjelenített régi, de már irreleváns személyes adatok (például adósságokkal kapcsolatos újságcikkek) sértik-e az érintett magánélethez való jogát. Az EUB kimondta, hogy a keresőmotorok ebben az esetben az európai szabályok szerinti adatkezelői státuszban vannak és az érintett kérésére kötelesek eltávolítani a személyes adatokra mutató hivatkozásokat, ha azok pontatlanok, irrelevánsak vagy túlzottak. Ez a döntés vezette be az „elfeledtetés jogának” fogalmát az EU-ban. A döntés azért releváns a DSA ex ante szabályozását tekintve, mert az elfeledtetés jogának technikai biztosítása olyan intézkedésnek minősül, amelyet az algoritmusokat működtető platformszolgáltatóknak a DSA követelményei, s az ezek szerint létrehozott, kockázatértékelési és csökkentési intézkedéseik révén eleve biztosítaniuk kell, úgy, hogy az algoritmusok, amelyeket alkalmaznak, figyelembe vegyék a keresési tevékenység alapjául szolgáló adatok relevanciáját és pontosságát.

Az EJEB gyakorlatát is vizsgálva, a Delfi AS kontra Észtország (2015) ügyben a Bíróság megállapította, hogy az észt hírportál, a Delfi felelőssé tehető a felhasználói által közzétett, gyűlöletkeltő kommentekért. Az ítélet hangsúlyozta, hogy a platformoknak proaktív intézkedéseket kell tenniük az ilyen tartalmak megelőzése érdekében, különösen akkor, ha azok súlyosan sértik mások jogait. Ez az eset rávilágított arra, hogy az online platformoknak felelősséget kell vállalniuk a felhasználói tartalmakért,⁴² és szükség van olyan ex ante szabályozásokra, amelyek biztosítják az alapvető jogok védelmét a digitális térben, nem elégséges ugyanis az e-kereskedelmi irányelv szerinti értesítési és eltávolítási eljárás arra, hogy minden ezzel kapcsolatos jogsértést megfelelően kezeljen. Ezzel szemben a Magyar Tartalomszolgáltatók Egyesülete és Index.hu Zrt. kontra Magyarország (2016) ügyben az EJEB kimondta, hogy a magyar bíróságok aránytalanul korlátozták a véleménynyilvánítás szabadságát, amikor felelőssé tették az Index.hu-t a felhasználói kommentekért, amelyek bár sértőek voltak, nem érték el a gyűlöletbeszéd szintjét. Az ítélet hangsúlyozta, hogy a platformok felelősségének megállapításakor figyelembe kell venni a tartalom jellegét és a moderációs intézkedéseket. Ez az eset aláhúzza annak fontosságát, hogy szükség van a DSA-ban meghatározott ex ante mechanizmusokra, de az azok alapján meghozott intézkedéseknek arányosnak kell lenniük és nem vezethetnek a véleménynyilvánítás szabadságának indokolatlan korlátozásához.

A Glawischnig-Piesczek kontra Facebook Ireland ügyben (C-18/18) az EUB a véleménynyilvánítás szabadsága (Alapjogi Charta 11. cikk) és az emberi méltóság (Alapjogi

⁴² NÁDORI Péter: Úton a tömeges internetes szólás jogi megítélésének új megközelítése felé: A strasbourgi Nagykamara ítélete a Delfi-ügyben. *In Medias Res* 8(2), 2019. 343-366.

Charta 1. cikk) alapjogi követelményeit vizsgálta, s jutott arra a következtetésre, hogy tagállami jogalkalmazó szervek kötelező jellegű döntései alapján az akkori szabályozásban közvetítő szolgáltatóknak minősülő szereplők kötelesek a jogsértő tartalom tekintetében biztosítani azt, hogy az azonos vagy hasonló jellegű tartalmak globálisan, a platformszolgáltatás minden eleméből eltávolításra kerüljenek,⁴³ s ez nem csupán az EU-n belüli eltávolításra vonatkoztatható. eltávolítását, nem csak az EU-n belül. A DSA-t megalkotó európai jogalkotó számára ez a döntés azért bírhatott jelentőséggel, mert a tartalommoderációra vonatkozó ex ante szabályokkal, például a platformok rendszeres kockázatelemzésére és a tartalommoderációs mechanizmusok átláthatóságára vonatkozó követelményekkel megelőzhetővé tehető a jogellenes tartalmak eltávolításának elmulasztását. Az óriásplatformszolgáltató a kockázatértékelés alapján ugyanis köteles előre bevezetni olyan mechanizmusokat, amelyek a már azonosított és bizonyítottan jogszerűtlen tartalmak automatikus felismerésére és eltávolítására szolgálnak.

A UPC Telekabel Wien kontra Constantin Film Verleih GmbH és Wega Filmproduktionsgesellschaft mbH (C-314/12) ügy rávilágít, hogy a jogszerűtlen tartalmak blokkolása valóban globális kötelezettsége a platformszolgáltatóknak, de e tekintetben a blokkolási intézkedések akkor lesznek jogszerűek, amennyiben azok arányosak, hatékonyak és nem korlátozzák szükségtelenül a felhasználók jogait.⁴⁴ A szerzői jogi érintettségű döntésben az EUB kiemelte, hogy a blokkolási intézkedéseknek figyelembe kell venniük a felhasználók alapvető jogait is, így a tájékozódás szabadságát (Alapjogi Charta 11. cikk) és egyúttal a szerzők tulajdonhoz való jogát (17. cikk). Jól mutatja az eset, hogy nem csak a jogalkotónak, vagy a felhasználóknak, de a közvetítő szolgáltatóknak is érdeke fűződik hozzá, hogy a DSA ex ante mechanizmusai elősegítsék a közvetítő szolgáltatók tevékenységét az eltávolítási intézkedések alkalmazása előtt abban, hogy arra kötelezik őket, végezzenek előzetes elemzést, hatásvizsgálatot az alapvető jogok tiszteletben tartása érdekében, azért, hogy az eltávolítás a jogszabályi keretek betartása mellett is arányos maradjon.

Az EUB döntéseinek egy másik csapásiránya a közvetítő szolgáltatók jogállását és annak megítélését befolyásolta, s így hatással van a DSA-ban értelmezett platformszolgáltatók megítélésére is.⁴⁵ Az Airbnb Ireland kontra Franciaország ügyben (C-390/18) az EUB úgy döntött, hogy az Airbnb közvetítő szolgáltatásnak minősül, amelyre az információs társadalommal összefüggő szolgáltatások szabályai vonatkoznak. Az EUB hangsúlyozta, hogy az Airbnb tevékenysége nem tekinthető ingatlanügynöki tevékenységnek, mivel a platform elsődleges célja az, hogy az ingatlantulajdonosok és bérlők közötti kapcsolatot megteremtse, anélkül, hogy közvetlenül beavatkozna a bérleti folyamatba. Ez az ítélet rávilágít, hogy a platformok szerepének megítélése nagyban függ a szolgáltatás természetétől, ami még inkább indokolja a DSA-ban kibontakoztatott ex ante kockázatértékelési követelmények fontosságát. Ezek a mechanizmusok segíthetnek abban, hogy a kockázatok csökkentésére meghatározott belső intézkedések arányosak és az alapvető jogokkal összhangban állóak legyenek, különösen olyan esetekben, amikor a platformok többféle szolgáltatást nyújtanak. Az Uber Spain ügyben (C-434/15) ezzel szemben az EUB kimondta, hogy az Uber olyan közlekedési szolgáltatást

⁴³ Katarina Knol RADOJA: Freedom of Expression on the Internet-Case 18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited. *Balkan Social Science Review* 15(15), 2020. 7-25.

⁴⁴ Peggy VALCKE – Aleksandra KUCZERAWY – Pieter-Jan OMBELET: Did the Romans get it right? What Delfi, Google, eBay, and UPC TeleKabel Wien have in common. *The responsibilities of online service providers* 2017. 101-116.

⁴⁵ KOVÁCS Ildikó: Az európai Bíróság „taxiítéletei”: az uberPop és a star taxi App. *Fontes Iuris* 7(1), 2021. 39-50.

nyújt, amelynek szabályozása az egyes tagállamok hatáskörébe tartozik, és nem minősül közvetítő szolgáltatásnak. Az EUB rámutatott, hogy az Uber tevékenysége nem korlátozódik csupán a sofőrök és az utasok közötti kapcsolat megteremtésére, mivel az alkalmazás aktívan szervezi a szolgáltatást, díjakat szab meg, és közvetlen befolyást gyakorol a szolgáltatás teljesítésére. Az ügy rámutat arra, hogy a platformok szerepe sok esetben nem könnyen ítéltető meg a vonatkozó jogviszonyokban, az nem határolható le pusztán formai, technikai szempontok alapján. Már ez a döntés is jól mutatta, hogy a közvetítő szolgáltatások nyújtása nehezen szabályozható terület, szabályozási hiányosságok esetén több tekintetben kibújót jelenthet a tevékenység hagyományos nyújtására vonatkozó szabályok alól, amelyekből levont tapasztalatok alapján változtatott a közvetítő szolgáltatók jogállásán az európai jogalkotó a DSA segítségével és az ex ante jellegű kötelezettségek bevezetésével.

Hasonló, mégis az alapjogok érvényesítését illetően más szemszögből vizsgálandó ügynek tekinthető a SABAM kontra Netlog NV ügy (C-360/10),⁴⁶ amely az online platformok általános nyomonkövetési kötelezettségét értelmezte, a véleménynyilvánítás szabadsága (Alapjogi Charta 11. cikk) és a vállalkozás szabadsága (Alapjogi Charta 16. cikk) figyelembevételével. Az ügy egy belga szerzői jogi közös jogkezelő, a SABAM és a Netlog közösségi hálózat között zajlott. A SABAM azt kérte, hogy a Netlog állítson fel egy olyan rendszert, amely képes általánosan nyomonkövetni a felhasználók által feltöltött tartalmakat annak érdekében, hogy megakadályozza a szerzői jogot sértő anyagok terjesztését. Az EUB úgy ítélte meg, hogy az általános nyomonkövetési kötelezettség aránytalanul korlátozná az online platformok működését és a felhasználók alapvető jogait. Az ítélet hangsúlyozta, hogy az ilyen kötelezettségek ellentétesek az uniós joggal. Nem véletlenül, hiszen az ítélezés időpontjában az elektronikus kereskedelmi irányelv szabályai alapján a közösségi platformokra közvetítő szolgáltatókként, s azon belül, mint tárhelyszolgáltatókra tekintettek, amely esetében indokolható volt és összhangban állt a jogszabályi kötelezettségekkel a nyomonkövetési kötelezettség hiánya abban az esetben, ha hatékony értesítési és eltávolítási rendszert üzemeltetettek.

5. Az e-kereskedelmi irányelv követelményei

Az EUB és az EJEB fenti esetjoga és az alapjogi készlet érvényesítésének vizsgálata alapján egyértelműen megállapítható, hogy számos kihívással találkozott a jogalkalmazó a DSA megjelenését megelőzően az alapjogok gyakorlati védelmét illetően. Ahhoz, hogy értelmezhetővé váljon, milyen igények merültek fel a DSA, és annak ex ante jellegű szabályozásának megalkotására, a fentiekén túl meg kell vizsgálni az elektronikus kereskedelmi irányelv szabályait (2000/31/EK),⁴⁷ amely a DSA megjelenését megelőzően (s azt követően részben hatályon kívül helyezett szabályokkal) szabályozta az információs társadalommal összefüggő szolgáltatások jogi kereteit. A szabályozás az Európai Unió digitális gazdaságának egyik első mérföldköve volt.

⁴⁶ Stefan KULK – Frederik ZUIDERVEEN BORGESIU: Filtering for copyright enforcement in Europe after the Sabam cases. *European Intellectual Property Review*, Forthcoming, 2013.

⁴⁷ Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól. HL L 178. (a továbbiakban: e-kereskedelmi irányelv)

Az irányelv célja a belső piac működésének elősegítése volt a digitális szolgáltatásokra vonatkozó jogi akadályok csökkentésével.⁴⁸ Bár az irányelv alapvetően sikeresnek bizonyult az online gazdaság fejlődésének előmozdításában, számos jelentős hiányosságot hagyott maga után, különösen az emberi jogok védelmének és azok érvényesíthetőségének területén, amelyet a jogalkotó a modern platformjog és annak részeként a DSA megalkotásával igyekezett kiküszöbölni. Az irányelv megalkotásának idején kifejezetten naprakész szabályozást valósított meg, amely sok éven keresztül szolgálta az Unió gazdaságának fejlődését és az állampolgárok életszínvonalának fejlődését,⁴⁹ de a platformgazdaság előrehaladásával, a felhasználói tartalmakra épülő közösségi média felületek és egyéb technológiai újítások tekintetében nem tudott lépést tartani a digitális gazdaság és az online szolgáltatások gyors fejlődésével, amely végső soron elvezetett oda, hogy a szabályozás már sokkal inkább jogi kikaput biztosított felelősségmentességi szabályain keresztül a szolgáltatóknak, s különösen problémássá vált a felmerülő kockázatok, az emberi jogok védelme és a szabályozási hatékonyság szempontjából. Jelen tanulmány azokra a szabályozási sarokpontokra és hiányosságokra fókuszál, amelyek végül megteremtették az új szabályozás igényeit, és amelyekre a jogalkotó a DSA szabályozásában ex ante jellegű követelményekkel is igyekszik válaszolni.

Az e-kereskedelmi irányelv egyik legnagyobb szabályozási novumának számított az előzetes engedélyezést kizáró elv (4. cikk).⁵⁰ Ez az elv az irányelv szövegébe szöve meghatározta a közvetítő szolgáltatók működésének kereteit. Az elv jelentősége a szolgáltatók terjeszkedésének elősegítésében, a verseny fellendítésében és az egységes digitális piac megalapozásában állt. Az irányelv ezzel a követelménnyel kifejezetten rögzítette, hogy a tagállamok nem tehetik az ilyen szolgáltatások nyújtását előzetes engedélyeztetéshez kötötté. A jogalkotó célja az volt, hogy minimalizálja az e-kereskedelmi szolgáltatásokra nehezedő adminisztratív terheket, és elősegítse a belső piacon belüli szabad versenyt, ezzel ösztönözve a digitális innovációt, biztosítsa a szolgáltatások szabad áramlását. Az engedélyeztetési eljárások harmonizátlansága torzíthatta volna a versenyt, mivel egyes tagállamok szigorúbb előírásokat alkalmazhattak volna, amelyek diszkriminatívak lehettek volna más tagállamok szolgáltatóival szemben. Ezzel szemben az előzetes engedélyeztetés kizárása elősegítette, hogy a szolgáltatók egyetlen tagállam joghatósága alatt működhessenek, és ne kelljen minden tagállamban külön engedélyt szerezniük, ahol szolgáltatásaikat nyújtani kívánták.

Ez a megközelítés összhangban állt a belső piaci szabályokkal, különösen a szolgáltatások szabad áramlásának elvével (EUMSZ 56. cikk).

Az elv alkalmazásának előnyei ellenére az előzetes engedélyeztetést kizáró elv komoly joghatósági problémákat eredményezett, amelyek akadályozták a tagállami hatóságok hatékony felügyeleti tevékenységét a közvetítő szolgáltatások felett. Az irányelv a "származási ország elvére" épült, amely kimondta, hogy egy adott digitális szolgáltatás felett az az ország gyakorol joghatóságot, ahol a szolgáltató letelepedett. Ez azt jelentette, hogy például egy Írországbán bejegyzett, de az EU számos tagállamában működő platform esetében az ír hatóságok voltak illetékesek a szabályozás és ellenőrzés terén. Az eltérő nemzeti szabályozások, valamint a joghatósági különbségek lehetőséget teremtettek a forum shoppingra, amely során a szolgáltatók előnyösebb szabályozási környezetet választottak letelepedési helyül. A probléma

⁴⁸ E-kereskedelmi irányelv, 1. cikk

⁴⁹ KLEIN Tamás: *Az újmédia szabályozásának új iránya? – A Digital Services Act alapjogvédelmi mechanizmusa.* In TÖRÖK Bernát – ZÖDI Zsolt (szerk.): *Digitalizálódó társadalom – Tanulmányok az új technológiák társadalmi-jogi hatásairól.* Budapest, Ludovika Egyetemi Kiadó, 2023. 122-124.

⁵⁰ Strihó Krisztina: Elektronikus kereskedelem. *Debreceni Jogi Műhely* 2(1), 2008.

még súlyosabban jelentkezett akkor, amikor a szolgáltató nem telepedett le az Európai Unió területén, hanem szolgáltatásait harmadik országból nyújtotta az Európai Unió területén található jogalanyok számára. A szabályozás irányukba – akár a sérelmet szenvedett fél járt el vagy akár jogalkalmazást végző szerv próbálta érvényesíteni az uniós joganyagba foglalt szolgáltatói kötelezettségeket – szinte érvényesíthetetlen maradt, mert hiányzott az a mechanizmus, amely megteremtette volna az alapot a szolgáltatók felelősségre vonására, másrésről pedig felelősségvonás esetén a jogkövetkezmények szintén majdhogynem érvényesíthetetlenek maradtak, mert a szolgáltatókat nem tette érdekeltté a szabályozás a szabályok betartására, komolyabb szankciók hiányában. A szabályozás irányelv jellegéből adódóan ráadásul nem eredményezett egységes európai szabályozást, tagállami eltérések mutatkoztak, amelyek erősítettek a fent már vázolt problémákat.

A szabályozás másik fókuszponti problémája a közvetítő szolgáltatók fajtái és hozzájuk kapcsolt felelősségi szabályok jelentették. Egy-egy szolgáltató tekintetében máig irányadó és minden fél számára előnyös szabályokat sikerült megalkotni (így például az egyszerű továbbítást, vagy a gyorsítótárolóban történő rögzítést végző szolgáltatóknál). A platformszolgáltatók és szolgáltatások jelentős része, valamint kifejezetten az alapjogi védelem szempontjából nagy kockázatot jelentő megoldások azonban a tárhelyszolgáltatások kategóriájába kerültek. A szolgáltatónak ebben az esetben a jogellenes tartalomért viselt felelősség alóli mentessége megalapozásához elég volt az, hogy „a szolgáltatónak nincsen tényleges tudomása jogellenes tevékenységről vagy információról, és – ami a kárigényeket illeti – nincsen tudomása olyan tényekről vagy körülményekről, amelyek nyilvánvalóan jogellenes tevékenységre vagy információra utalnának; vagy a szolgáltató, amint ilyenről tudomást szerzett, haladéktalanul intézkedik az információ eltávolításáról vagy az ahhoz való hozzáférés megszüntetéséről.”⁵¹ Egy a szabályoknak megfelelő értesítési és eltávolítási rendszerrel dolgozó szolgáltató ez esetben elkerült minden felelősséget, tekintettel arra, hogy az irányelv egyik kulcsfontosságú szabálya az, hogy a tárhelyszolgáltatóknak nincs általános nyomonkövetési kötelezettsége a felhasználók által elhelyezett tartalmak jogszerűségének ellenőrzésére. Ez a szabály jelentős védelmet nyújtott a szolgáltatók számára, de egyben szabályozási problémát is teremtett, különösen a platformokat üzemeltető szolgáltatók esetében, amelyek tevékenysége jelentősen túlmutatott az egyszerű tárhelyszolgáltatáson.⁵² Az EUB több ítéletében is megerősítette, hogy az e-kereskedelmi irányelv alapján a közvetítő szolgáltatóknak, különösen a tárhelyszolgáltatóknak, nincs általános nyomonkövetési kötelezettségük, ahogy azt láthattuk például a SABAM kontra Netlog NV (C-360/10) ügyben.

Az irányelv nem tett különbséget az egyszerű tárhelyszolgáltatók és a modern platformokat üzemeltető szolgáltatók között. Ez utóbbiak, mint például a közösségi médiaplatformok vagy online piacterek, már nem csupán tárhelyet biztosítottak, hanem aktív szerepet játszottak a tartalmak terjesztésében, moderálásában és ajánlásában. Az ilyen platformok működésére egyértelműen kimutathatóvá vált a tartalommoderáció átláthatóságának hiánya, amely azért alakulhatott ki, mert az e-kereskedelmi irányelv nem tartalmazott részletes előírásokat a digitális platformok tartalommoderációs tevékenységére vonatkozóan. A platformok széles mérlegelési lehetőséget kaptak, hogy saját szabályaik alapján kezeljék a felhasználói tartalmakat, amelyeket részben a vonatkozó szakpolitikai fejlemények (pl. gyűlöletbeszéd elleni fellépés, kiskorúak védelme miatt) folyamatosan szigorítottak, miközben ezek a

⁵¹ E-kereskedelmi irányelv 14. cikk (1) bekezdés

⁵² GOSZTONYI Gergely – Ewa GALEWSKA – Andrej ŠKOLKAY: Challenges of Monitoring Obligations in the European Union’s Digital Services Act. *Elte Law Journal* 12(1), 2024. 49-50.

változtatások gyakran a véleménynyilvánítás szabadságának indokolatlan korlátozásához vezettek. Az irányelv kizárólag a jogszerűtlen tartalmakra összpontosított, és nem foglalkozott a káros, de nem feltétlenül jogellenes tartalmak (például álhírek) kezelésével.

Eközben a felhasználók számára nem állt rendelkezésre megfelelő jogorvoslati mechanizmus a platformok moderációs és egyéb döntéseivel szemben, csupán az értesítési eltávolítási eljárás szabályai voltak lefektetve. Például, ha egy felhasználói tartalmat eltávolítottak vagy felfüggesztették egy fiók működését, számos esetben tisztázatlan volt, hogy milyen módon érvényesíthetik igényeiket a felhasználók.

A platformok tartalmi szűrését közben egyre inkább uralni kezdték a háttérben működő algoritmusok, amelyekkel szemben a szabályozás még nem tudott érdemi választ adni, hiszen kiadásának időpontjában az algoritmus alapú tartalomajánlás és a célzott hirdetések még nem voltak széles körben elterjedtek. Az irányelv ennek megfelelően nem tartalmazott előírásokat az algoritmusok működésének átláthatóságára és a felhasználók személyes adataival való visszaélések megelőzésére. A szabályozási hiányosságok a technológiai lehetőségek hihetetlen bővülésével együtt pedig számos alkalommal eredményezték az emberi jogok sérelmét e jogok explicit védelmének hiányában. Az irányelv ugyan közvetve érintett emberi jogi kérdéseket, mint például a véleménynyilvánítás szabadságát, nem tartalmazott azonban explicit előírásokat az alapvető jogok védelmére vagy érvényesítésére.

Ezek együttes hatására tekintettel gyakorlatilag elkerülhetetlen volt egy új szabályozás megalkotása, amennyiben az Európai Unió tartani kívánt magát a 2. fejezetben felvázolt alapjogi megközelítéséhez és ebből kibontott szakpolitikai irányaihoz.

6. Az ex ante jellegű követelmények azonosítása a DSA szabályozásában

A DSA számos rendelkezést tartalmaz, amelyek célja az emberi- és alapvető jogok védelme a digitális térben, különösen megelőző (ex ante) intézkedések révén. Ez alapján megállapítható lesz azon követelmények köre, amelyektől az európai jogalkotó azt reméli, hogy előrehozott, ex ante jellegű intézkedések útján képesek lesznek arra, hogy a platformszolgáltatások esetében megelőzzék a jogsértések kialakulását, proaktív védelmet biztosítva.

6.1 Preambulum

A DSA preambuluma különösen alkalmas arra,⁵³ hogy jól kimutatható legyen belőle a jogalkotói szándék és egyúttal a rendelet szabályozását a digitális tér vonatkozásában a platformjog kereteire illessze, bemutatva a szabályozás kapcsolódási pontjait is.

A (1)-(3) preambulumbekkezdés rámutat, hogy a közvetítő szolgáltatások jelentős szerepet játszanak az uniós polgárok életében, és ezért alapvető fontosságú, hogy ezek a szolgáltatások a Charta által biztosított alapvető jogok teljes körű tiszteletben tartásával működjenek. Ez a megállapítás hangsúlyozza, hogy a digitális szolgáltatásoknak nemcsak technikai, hanem jogi és etikai kötelezettségeik is vannak az alapvető jogok védelme terén. A (3) bekezdés kiemeli a védelem kiemelt tárgyköreit, így „különösen a véleménynyilvánítás és a tájékozódás szabadságát, a vállalkozás szabadságát, a megkülönböztetésmentességhez való jogot és a fogsztóvédelem magas szintjének elérését”.

⁵³ Folkert WILMAN: The Digital Services Act (DSA) – An Overview. *Available at SSRN 4304586* (2022).

A (9) preambulumbekzdés kifejezi azt a jogalkotói szándékot, amely egy biztonságos, kiszámítható és megbízható online környezet kialakítására irányul, amely kezeli a jogellenes tartalmak online terjesztését és azokat a társadalmi kockázatokat, amelyeket a dezinformáció vagy más tartalmak terjesztése okozhat. Egyúttal pedig rögzíti az Alapjogi Chartában megjelenő alapvető jogok hatékony védelemben való részesítését és az innováció elősegítési szándékát. Ehhez szorosan kapcsolódik a szabályozás rendeleti formában történő megalkotásának indoka is, amely arra alapozódik, hogy az egységes uniós fellépés érdekében egységes, tagállami különbségektől mentes szabályozásra van szükség.

A (153) preambulumbekzdés kifejezetten hangsúlyozza, hogy a DSA „tisztetben tartja a Charta által elismert alapvető jogokat”, például a véleménynyilvánítás és a tájékozódás szabadságát, valamint a tömegtájékoztatás szabadságát és sokszínűségét. A bekezdés az arányosság elvének alkalmazására is utal, amikor az érintett hatóságok közötti alapjogi konfliktusokat kell kezelniük. A (154) preambulumbekzdés kitér arra is, hogy az online óriásplatformok által generált társadalmi kockázatok kezelése prioritást élvez. Ez összhangban áll a DSA azon célkitűzésével, hogy biztonságos és megbízható online környezetet biztosítson, amelyben az alapvető jogok hatékony védelmet élveznek. Ezt megerősítve a (155) bekezdés hangsúlyozza, hogy az alapvető jogok védelme és a belső piac működésének harmonizációja érdekében az uniós szintű szabályozás elengedhetetlen. Az arányosság és szubszidiaritás elve biztosítja, hogy a szabályozás ne lépje túl a célok eléréséhez szükséges mértéket.

A (22) preambulumbekzdés alapján ez az arányosság és egyensúlykeresés megjelenik a jogellenes tartalmak eltávolítására, hozzáférhetetlenné tételére irányuló eljárásokban is, ahol ennek megvalósítása mellett figyelemmel kell lenni a szolgáltatás igénybe vevői alapvető jogainak tisztetben tartására is különösen a véleménynyilvánítás és a tájékozódás szabadságához való jog tisztetben tartásának területén.

A szabályozás (47) preambulumbekzdése foglalkozik a sérülékeny csoportokkal is: kiskorúakat célzó vagy általuk jellemzően igénybevett szolgáltatásoknál a kiskorúak védelmében elrendelt intézkedéseknél a szolgáltatóknak figyelemmel kell lenniük az Alapjogi Chartában rögzített alapvető jogokra (pl. véleménynyilvánítás és a tájékozódás szabadságára, beleértve a tömegtájékoztatás szabadságát és sokszínűségét is), amely egészen biztosan ex ante jellegű kockázatértékelési tevékenységet kíván meg a szolgáltatóktól.

Az (51) preambulumbekzdés egyfajta válasz a korábban az EUB és EJEB gyakorlatában megjelenő esetjogra: a szolgáltatóknak tartalommoderációs tevékenységük során megfelelően célzott intézkedéseket kell hozniuk annak érdekében, hogy azok a jogellenes tartalomnak minősülő konkrét információk eltávolítását vagy az azokhoz való hozzáférés megszüntetését tudják szolgálni, anélkül, hogy indokolatlanul befolyásolnák a szolgáltatás igénybe vevőinek véleménynyilvánítási szabadságát és tájékozódási szabadságát. Megítélésem szerint a szolgáltatók ezt is az ex ante jellegű alapjogvédelmi intézkedések során kimunkált kockázatcsökkentési intézkedések alkalmazásával tudják teljesíteni.

A (79) preambulumbekzdés jelenti az ex ante mechanizmusokra vonatkozó követelmények alapját, magyarázatát. Arra tekintettel, hogy „az online óriásplatformok és a nagyon népszerű online keresőprogramok használatának módja adott esetben erősen befolyásolhatja az online biztonságot, a közvélemény és a közbeszéd alakulását, valamint az online kereskedelmet”, szolgáltatóknak értékelniük kell a szolgáltatásaik kialakításából, működéséből és használatából, illetve a szolgáltatások igénybe vevői általi esetleges visszaélésekből származó rendszerszintű

kockázatokat, és az alapvető jogokra figyelemmel megfelelő kockázatsökkentési intézkedéseket kell hozniuk. Mindez meghatározza a kockázatértékelés kereteit, célját, és azt is, hogy alapvető módszertani megoldás alapján kell véghez vinni mindezt: a hatások és következmények súlyosságára és a kockázat valószínűségére tekintettel kell priorizálni az azok kezelésére szolgáló intézkedések között.

A jogalkotó a (80)-(83) preambulumbekszámlástól kezdve meghatározza a kockázatértékelés területeit – a szabályozás ehelyütt már-már normatív jellegűvé válik meghatározva az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatók számára a rendszerszintű kockázatok négy értékelendő kategóriáját.

E kockázati kategóriák a következők:

1. Jogellenes tartalmak – például gyermekek szexuális bántalmazását ábrázoló anyagok vagy jogellenes gyűlöletbeszéd – terjesztése révén, vagy a szolgáltatásaikkal bűncselekmény elkövetése céljából történő egyéb típusú visszaélések révén valósulnak meg; továbbá ide tartoznak a jogellenes tevékenységek folytatásával összefüggő kockázatok is. Az ilyen terjesztés vagy tevékenységek például jelentős rendszerszintű kockázatot jelenthetnek abban az esetben, ha a jogellenes tartalomhoz való hozzáférés gyorsan és széles körben elterjedhet különösen széles hatókörű felhasználói fiókokon vagy egyéb terjesztési eszközökön keresztül – így azt az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak értékelniük kell.
2. Az Alapjogi Charta által védelmet élvező alapvető jogok – ideértve többek között, de nem kizárólag az emberi méltóság, a véleménynyilvánítás és a tájékozódás szabadsága, így a tömegtájékoztatás szabadsága és sokszínűsége, a magánélethez való jog, a személyes adatok védelméhez való jog, a megkülönböztetésmentességhez való jog, a gyermekek jogai és a fogyasztóvédelem – gyakorlására kifejtett tényleges vagy várható hatások.
3. A demokratikus folyamatokra, a polgári közbeszédre és a választási folyamatokra, valamint a közbiztonságra gyakorolt tényleges vagy előrelátható negatív hatások.
4. Az online óriásplatformok és a nagyon népszerű online keresőprogramok kialakításával, működésével vagy használatával kapcsolatos kockázatok, amelyek tényleges vagy előrelátható negatív hatást gyakorolnak a közegészség és a kiskorúak védelmére, és súlyos negatív következményekkel járnak az adott személy testi és szellemi jóllétére, vagy nemi alapú erőszakot eredményeznek.

A (84) preambulumbekszámlásban a jogalkotó útmutatást ad az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak a kockázatértékelés terjedelmére, abban, hogy azokra a rendszerekre vagy egyéb elemekre kell figyelniük, amelyek hozzájárulhatnak a kockázatokhoz, beleértve az összes releváns algoritmikus rendszert, különösen ajánlórendszereiket és hirdetési rendszereiket, figyelmet fordítva a kapcsolódó adatgyűjtési és felhasználási gyakorlatokra, szerződési feltételeikre és azok érvényesítésére, valamint arra, hogy ezen feladatokkal kapcsolatos kockázatok kezelésére tartalommoderálási folyamataik, technikai eszközeik és elkülönített erőforrásaik megfelelőek-e. Külön felhívja a jogalkotó e tekintetben a figyelmet arra, hogy a szolgáltatóknak azokra az információkra is figyelniük kell, amelyek nem jogellenesek, de hozzájárulnak az e rendeletben azonosított rendszerszintű kockázatokhoz, így például a félrevezető vagy megtévesztő tartalmak terjesztésére vagy felerősítésére.

A (85) preambulumbekkezdés alapján a jogalkotó olyan követelményeket alkotott, amelyek alapján az „online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak meg kell őrizniük az általuk elvégzett kockázatértékelésekhez kapcsolódó valamennyi igazoló dokumentumot”, ezzel fokozva a szolgáltatók elszámoltathatóságát és erősítve az átláthatóságot.

A preambulumbekkezdés (86)-(87) bekezdésében iránymutatást ad a kockázatértékelésben azonosított rendszerszintű kockázatok csökkentési feladataihoz, amelyet a szükséges eszközök használatával, kellő gondossággal eljárva kell végrehajtani, szükségességi és arányossági szempontok mellett alkalmazva, kiemelt figyelmet fordítva a véleménynyilvánítás szabadságára gyakorolt hatásra. Az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak e tekintetben az ilyen kockázatsökkentő intézkedések keretében mérlegelniük kell például a szolgáltatásuk szükséges kialakításának, jellemzőinek vagy működésének – így például az online interfésznek – a kiigazítását, akár a reagálás gyorsaságát és technikai megvalósítását is megváltoztatva. A szabályozás (88) preambulumbekkezdése kiemeli e szolgáltatók algoritmikus rendszereik, különösen ajánlórendszereik vonatkozásában a rendszerszintű kockázatok kezelésének fontosságát, amelyet a (94) preambulumbekkezdés tovább részletez.

Az Európai Bizottság és tagállami hatóságok, így a digitális szolgáltatási koordinátor felügyeleti lehetőségét körvonalazza a (96) preambulumbekkezdés, amely a kockázatok és lehetséges károk felméréséhez szükséges adatokra, az algoritmikus tartalommoderálási rendszerek, az ajánlórendszerek vagy a hirdetési rendszerek pontosságára, működésére és tesztelésére vonatkozó adatokra, illetve a tartalommoderálás vagy az e rendelet értelmében vett belső panaszkezelési rendszerek folyamataira és kimeneteire vonatkozó adatokra azt irányozza elő, hogy azokhoz ezek a hatóságok hozzáférhessenek.

6.2 Normatív rendelkezések

A DSA átfogó célja, hogy biztonságosabb, kiszámítható és megbízható digitális környezetet teremtsen, amelyet a 1. cikkben is rögzítésre kerül, kiemelve, hogy az alapvető jogok védelme központi eleme a szabályozásnak. A rendelet hatály az összes közvetítő szolgáltatásra, így a tárhelyszolgáltatókra, azon belül az online platformokra és online piacokra is kiterjed, de kiemelten kezeli az online óriásplatformokat (VLOP) és a nagyon népszerű keresőprogramokat, amelyeknek különösen nagy hatásuk van az alapvető jogokra.

Áttekintve a DSA által szabályozott szolgáltatásokat, azokat 3 szűkülő típusba foglalhatjuk össze. A legnagyobb csoportot a már említett közvetítő szolgáltatók adják, amelyek felosztása jelentősen nem tér el az e-kereskedelmi irányelvben szabályozott rendszertől - a szolgáltatások az internet alapvető működéséhez elengedhetetlenek, és magukban foglalják a hozzáférést nyújtó szolgáltatókat, a gyorsítótár-szolgáltatókat (caching szolgáltatások) és a tárhelyszolgáltatókat (hosting szolgáltatások).

A szabályozás ugyan fenntartja az e-kereskedelmi irányelvben szereplő, általános monitorozási vagy aktív tényfeltárási kötelezettségek hiányát megállapító rendelkezést (8.cikk), de ezt áttöri a későbbiekben a rétegzett szabályozáson keresztül a legnagyobb és legjelentősebb hatású szolgáltatókra vonatkozó kötelezettségek körében.

A DSA rétegzett szabályozása aszimmetrikus jellegű követelményeket tartalmaz, amely azt jelenti, hogy szolgáltatások méretéhez, természetéhez és kockázati szintjéhez igazodó kötelezettségeket ír elő számukra a szabályozás. Ez egyrészt megvalósul piaci nagyság vagy befolyásoló erőn alapulóan, a kisebb szereplőket (pl. mikro- és kisvállalkozások, induló online platformok) kevesebb és egyszerűbb kötelezettségek terhelik, mint a jelentős hatású, globális platformokat. A szabályozás a kisebb kockázatú szolgáltatások irányába inkább reaktív (ex post), míg az online óriásplatformok és a nagyon népszerű online keresőprogramok esetében sokkal összetettebb, szigorúbb ex ante jellegű kötelezettségeket tartalmaz, tekintettel a felmerülő kockázatok lehetőségére.

A szabályozás közvetítő szolgáltatókon, tárhelyszolgáltatókon belüli harmadik rétegét az úgynevezett online platformok jelentik, amelyek olyan tárhelyszolgáltatók, amelyek harmadik felek által létrehozott tartalmakat tesznek hozzáférhetővé és terjesztenek nyilvánosan, például közösségi médiaoldalak, videómegosztók és e-kereskedelmi platformok. Ezek a szolgáltatók már további kötelezettségekkel néznek szembe, mint például a jogellenes tartalmak kezelésére irányuló mechanizmusok.

A szabályozás legszigorúbb magját az online óriásplatformok és a nagyon népszerű online keresőprogramok adják. Az online óriásplatformok (VLOP) és a nagyon népszerű online keresőprogramok (VLOSE) olyan szolgáltatások, amelyek átlagosan legalább 45 millió, a szolgáltatást aktívan igénybe vevővel rendelkeznek az Unióban, és amelyeket az Európai Bizottság a DSA 33. cikk (4) bekezdéssel összhangban online óriásplatformnak vagy nagyon népszerű online keresőprogramoknak minősített.

A platformszolgáltatások vonatkozásában éppen e rétegzett szabályozásra tekintettel szét kell választani azokat az ex ante jellegű alapjogvédelmi kötelezettségeket, amelyek minden közvetítő szolgáltatás irányába alkalmazandóak lesznek és azokat, amelyek csak az online óriásplatformokra és a nagyon népszerű keresőprogramokra lesznek irányadóak.

Az általános kötelezettségek körében kiemelt jelentőségű a DSA 14. cikke, amely kifejezetten szigorú közzétételi és transzparenciát előíró követelményeket ír elő a közvetítő szolgáltatókra, speciális tájékoztatási kötelezettséggel egybekötve. A 14. cikk (1) bekezdése alapján e tájékoztatási kötelezettségük körében adják köre, a szolgáltatásaik használatával kapcsolatban általuk megszabott korlátozásokat.⁵⁴ A cikk (4) bekezdése szerint kellő gondossággal, objektíven és arányosan kell eljárniuk a korlátozások alkalmazása és érvényesítése során, amely során kiemelt figyelmet fordítanak többek között a Chartába foglaltak szerinti alapjogokra és szabadságokra. A korlátozások az előzetes kockázatértékelési tevékenységen, és az annak eredményeként szükségessé váló kockázatsökkentési intézkedéseken alapulhatnak, amely a szerződési feltételek által válik jogilag kötelezően alkalmazandóvá a szerződő felek között. A szakasz azért is kifejezetten jelentős, mert ennek köszönhetően a szolgáltatás minden lényegi eleme, az összes technológiai megoldás alapjogi elemzés tárgyává tehető, hiszen minden, a szerződési feltételekben meghatározott típusú és aszerint alkalmazott korlátozás során a szolgáltatóknak figyelemmel kell lenniük az alapjogi megfelelésre is. Valójában ugyanez lesz az alapja az átláthatósági jelentési kötelezettségek (24. cikk) és hirdetési- ajánlórendszerek

⁵⁴ João Pedro QUINTAIS – Naomi APPELMAN – Ronan Ó. FATHAIGH: Using terms and conditions to apply fundamental rights to content moderation. *German Law Journal* 24(5), 2023. 881-911.

átláthatósági követelményeinek (26-27. cikk), de ezek kapcsolata csak áttételes az ex ante jellegű tevékenységekkel.

A követelmények szigorúbb körét a 34. cikk határozza meg, amely az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak előírja, hogy azonosítsák, elemezzék és értékeljék szolgáltatásaik és a kapcsolódó rendszerek kialakításából, működéséből vagy a szolgáltatásaik használatából eredő rendszerszintű kockázatokat, legalább évente egyszer, de újabb funkciók és jelentősebb változtatások esetén minden esetben.⁵⁵ Ezt a preambulumbekkezdések elemzésénél már megvizsgált 4 elemzési témakörre kell elvégezni – tekintettel a szolgáltatás keretében alkalmazott rendszerekre is.

A kockázatcsökkentési kötelezettségek 35. cikkben foglalt köre kiegészíti a 34. cikk kockázatértékelési előírásait azáltal, hogy konkrét intézkedéseket határoznak meg az azonosított rendszerszintű kockázatok kezelésére. Az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak észszerű, arányos és hatékony intézkedéseket kell tenniük a kockázatok mérséklése érdekében. Ez megvalósulhat az alkalmazott rendszerek, így a tartalommoderálási rendszerek, ajánlórendszerek, hirdetési rendszerek és az ezek mögött működő algoritmusok módosításával, vagy a felhasználók körében tudatosságnövelő intézkedésekkel, vagy épp a gyermekek jogainak fokozott védelmét célzó eszközök, például szülői felügyeleti rendszerek bevezetésével. Az ex ante jelleg erősítéseként külön figyelmet érdemes fordítani a technológiai megoldások bevezetésének fázisára, a tesztelésre, a megalkotott belső szabályozásra és folyamatokra, mert a szolgáltatók ezen keresztül teljesíthetik az alapjog védelmi kötelezettségeiket. Ez a cikk az ex ante szabályozás szerves része, mivel nemcsak a kockázatok azonosítására, hanem azok megelőzésére is hangsúlyt helyez, a gyakorlati megvalósítás követelményeit értelmezve.

A 36. cikkben meghatározott követelmények, és a válságreagálási mechanizmusok célja, hogy súlyos fenyegetések esetén gyors és hatékony intézkedéseket tegyen lehetővé. A jelentős közbiztonsági vagy közegészségügyi fenyegetések mentén kialakuló válsághelyzetek esetén kiemelt jelentőségű az (1) és (3) bekezdése elemzésünk szempontjából, amely alapján a szolgáltatóknak olyan intézkedésekkel kell kezelnie a kialakuló válsághelyzetet, amelyek feltétlenül szükségesek, indokoltak és arányosak, kellő mértékben figyelembe veszik a (2) bekezdésben említett súlyos fenyegetés komolyságát, az intézkedések sürgős voltát, valamint az összes érintett fél jogait és jogos érdekeit érintő tényleges vagy lehetséges következményeket, külön figyelmet szentelve a Chartában rögzített alapvető jogok érvényesíthetőségére a rendkívüli szituációban.

Az ex ante kötelezettségek szempontjából különös jelentőséggel bír az Európai Bizottság és a tagállami hatóságok, így a digitális szolgáltatási koordinátor hatásköre, ugyanis a szabályok betartása mind attól függ, hogy a platformszolgáltatók felett milyen minőségben sikerül megvalósítani a hatósági felügyeletet, milyen mértékben kerül ellenőrzésre az alapjogok védelmére irányuló mechanizmusok működése, hatékonysága. Az erre vonatkozó hatásköri követelményeket a DSA 51. cikke és az 56. cikke határozza meg. Ez alapján a digitális szolgáltatási koordinátorok hatásköre nem terjed ki az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók kockázatértékelési,

⁵⁵ Niklas EDER: Making systemic risk assessments work: how the DSA creates a virtuous loop to address the societal harms of content moderation. *German Law Journal* 2023. 1-22.

kockázatsökkentési és válságreagálási intézkedéseinek ellenőrzésére és felügyeletére, azok a Bizottság kizárólagos hatáskörébe tartoznak.

A Bizottság ez alapján kulcsszerepet játszik annak biztosításában, hogy az érintett szolgáltatók megfelelően végrehajtsák a DSA ex ante kötelezettségeként azonosítható kockázatértékelési és kockázatsökkentési kötelezettségeiket.

A DSA 66. cikke szerint a Bizottság eljárást indíthat, ha azt gyanítja, hogy egy online óriásplatform vagy keresőszolgáltató megszegte a rendelet valamely követelményét. A digitális szolgáltatási koordinátorok kezdeményezhetik az eljárást, amennyiben rendszerszintű jogsértésre utaló bizonyítékot találnak. Az ilyen vizsgálatok keretében a Bizottság közvetlenül ellenőrizheti a kockázatértékelések megfelelőségét. A 67. cikk értelmében a Bizottság információkéréssel fordulhat a szolgáltatókhoz, amelyeknek meg kell adniuk a kockázatelemzéseikkel, algoritmusaikkal és belső folyamataikkal kapcsolatos adatokat. Ezek az információk alapvető fontosságúak a kockázatok azonosításához és a megfelelő biztosításához.

A Bizottság a 69. cikkben kapott felhatalmazása alapján helyszíni vizsgálatokat is végezhet, amely az érintett szolgáltatók vagy személyek üzleti és technikai tevékenységeinek mélyreható ellenőrzését szolgálják, akár a tagállamok digitális szolgáltatási koordinátorai segítségével. A Bizottság hatáskörei magukban foglalják a vonatkozó dokumentumok és rendszerek vizsgálatát, amely alapján a szolgáltatók kötelesek hozzáférést biztosítani az adatbázisokhoz, algoritmusokhoz és üzleti gyakorlatokhoz. Ez a felhatalmazás az ex ante megfelelőség biztosításának kulcsfontosságú eleme, mivel lehetőséget ad a kockázatok és jogsértések helyszíni feltárására.

A 70. cikk felhatalmazza a Bizottságot, hogy első látásra is megalapozottnak tűnő jogsértések esetén ideiglenes intézkedéseket rendeljen el. Ez különösen sürgős esetekben lehetőséget ad a Bizottság számára, hogy korlátozza a szolgáltatók tevékenységét a károk elkerülése érdekében és biztosítsa az alapvető jogok védelme érdekében az azonnali beavatkozást.

Az érintett szolgáltatók az eljárásban önkéntes kötelezettségvállalásokat is tehetnek a szabályozásnak való megfelelés érdekében, amelyek a Bizottság határozatban kötelezővé tehet, amennyiben azok biztosítják a szabályok betartását. Abban az esetben pedig, ha a vállalások nem teljesülnek, vagy a körülmények változnak, a Bizottság újra indíthatja az eljárást.

Ez az eszköz lehetőséget biztosít arra, hogy a szolgáltatók proaktívan alkalmazkodjanak a szabályozási követelményekhez és saját megoldásokat találjanak megfelelőségük elérésére, erősítve a partnerséget és az együttműködést a Bizottsággal.

A 72. cikk alapján a Bizottság intézkedéseket hozhat a szabályozás végrehajtásának nyomon követésére. Ennek keretében hozzáférést kérhet az érintett szolgáltatók adatbázisaihoz, algoritmusaihoz és elemzéseikhez, valamint külső szakértők segítségét veheti igénybe. A 75. cikk alapján, ha egy szolgáltató szisztematikusan megsérti a szabályokat, a Bizottság fokozott felügyeleti rendszert alkalmazhat. Ez magában foglalja a cselekvési tervek jóváhagyását és ezek végrehajtásának szoros nyomonkövetését.

A Bizottság jogköre kiterjed az érintett szolgáltatók szankcionálására és kötelezettségeik betartatására. A 73. cikk szerint a Bizottság határozatban állapíthatja meg, hogy egy szolgáltató nem teljesítette a rá vonatkozó szabályokat. Ilyen esetekben a szolgáltató további

intézkedéseket köteles végrehajtani a megfelelés érdekében, ellenkező esetben további szankciókra számíthat. A 74. cikk alapján a Bizottság pénzbírságot szabhat ki, amely az érintett szolgáltatók globális éves forgalmának akár 6%-át is elérheti. A 76. cikk lehetőséget biztosít a Bizottságnak napi kényszerítő bírságok kiszabására, ha egy szolgáltató nem tesz eleget a szabályozási kötelezettségeinek. Ez különösen fontos a kockázatértékelési és kockázatsökkentési kötelezettségek megsértése esetén, mert kifejezett kényszerítőerővel rendelkezik a követelmények betartására vonatkozóan.

Ezekén túl elméletben semmi nem zárja ki, hogy az alapjogsérelemmel járó esetben az érintettek a DSA-ban foglalt felügyeleti intézkedéseken túl önállóan indítsanak bírósági igényérvényesítést,⁵⁶ amelyben hivatkozhatnak arra, hogy a szolgáltatót ex ante jellegű alapjog védelmi kötelezettségek terheltek a DSA szabályai alapján.

7. A kimutatható joggyakorlatok köre

A DSA 2022. november 16-i hatálybalépése óta eltelt időszakban az EUB és a tagállami hatóságok gyakorlatában még nem alakult ki jelentős esetjogi gyakorlat a DSA ex ante alapjogvédelmi szabályozásának hatékonyságáról. Ennek oka, hogy a DSA rendelkezéseinek teljes körű alkalmazása fokozatosan lép életbe, és a jogalkalmazás során felmerülő konkrét ügyek feldolgozása időigényes folyamat. Miután az ex ante kötelezettségek jelentős körében felügyeleti hatóságként nem a tagállami digitális szolgáltatási koordinátorok, hanem az Európai Bizottság rendelkezik hatáskörrel, ezért a felügyeleti intézkedések körét ennél a szervnél, az esetleges jogérvényesítéseket az Európai Bíróság eljárásaiban lehetne nyomomonkövetni. Miután az Európai Bíróság döntései között jelen tanulmány megírásának időpontjában még nem található olyan döntés, amely a tanulmányban vizsgált kötelezettségek érvényesítését vizsgálja, ezért az Európai Bizottság nyilvános dokumentumainak elemzésére terjed ki jelen elemzés terjedelme.

A Bizottság 2023 áprilisában állapította meg először a DSA szabályai szerint az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók körét, 17 platformot és 2 keresőmotort kijelölve, akiknek 2023 augusztusától kell megfelelniük a DSA vonatkozó követelményeinek.⁵⁷ A Bizottság eljárásaira ettől az időponttól lehetett számítani.

Ezt követően a Bizottság már több platformszolgáltatótól kért információt a DSA 67. szakasza alapján, és ezek szinte minden esetben legalább részben érintették az adott szolgáltató ex ante jellegű kötelezettségeit is. A Bizottság napjainkra több 66. cikk szerinti eljárást is elindított. A Bizottság nyilvános felületei, kiadott közleményei és állásfoglalásai alapján a Bizottság összes eljárása nyomomonkövethető, ezek alapján a szabályozás hatályba lépése óta az alábbi esetekben járt el a Bizottság:

- 2023. október 13. X – Információkérés illegális tartalom és dezinformáció állítólagos terjesztése, különösen terrorista és erőszakos tartalmak és gyűlöletbeszéd terjesztése

⁵⁶ A magánjogi igényérvényesítésről ld.: GÁRDOS-OROSZ Fruzsina – BEDŐ Renáta: Az alapvető jogok érvényesítése a magánjogi jogviták során. Alkotmánybírósági szemle, 2018/2., 3-10. és Klein (2024a) i.m. (27. l.) 270.

⁵⁷ <https://digital-strategy.ec.europa.eu/en/news/digital-services-act-commission-designates-first-set-very-large-online-platforms-and-search-engines>

ügyében.⁵⁸ Az információkérést követően a Bizottság 2023. december 18-án eljárást indított a 66. cikk felhatalmazása alapján a Hamász Izrael elleni terrortámadásaival összefüggésben illegális tartalmak terjesztése miatt. Az eljárás számos ponton érintette a szolgáltatás kockázatértékelési és kockázatsökkentő intézkedéseit, valamint a DSA által előírt, az EU-n belüli illegális tartalomra vonatkozó értesítési és intézkedési mechanizmus működését, beleértve azt is, hogy az X mekkora és milyen erőforrásokat szentelt a tartalommoderációs tevékenységének. A Bizottság 2024. május 8-án újabb információkéréssel kereste meg a szolgáltatót, hogy további részleteket tudjon meg az X tartalommoderációs tevékenységeiről és erőforrásairól, az X által a generatív mesterséges intelligenciaeszközök uniós alkalmazásával kapcsolatban végzett kockázatértékelésről, valamint a folyamatban lévő eljárás által érintett egyéb területekről.⁵⁹ 2024. júliusában a Bizottság közzétette előzetes véleményét, amely alapján a szolgáltató megsértette a DSA sötét mintákkal, reklámok átláthatóságával és a kutatók adathozzáféréseivel kapcsolatos követelményeit. Habár a megállapítások alapján elsődleges alapjogsérelem nem valósult meg, de az ex ante kötelezettségek körében a kockázatértékelés és csökkentés hatékonysága nem volt megfelelő a fenti témakörök tekintetében a Bizottság véleménye szerint.

- 2023. október 19. TikTok – Információkérés illegális tartalom és dezinformáció állítólagos terjesztése, különösen terrorista és erőszakos tartalmak és gyűlöletbeszéd terjesztése ügyében.⁶⁰ Az információkérést követően a Bizottság 2024. február 19-én eljárást indított a 66. cikk felhatalmazása alapján, a kiskorúak védelme, a reklámok átláthatósága, a kutatók adathozzáférése, valamint az addiktív design és a káros tartalmak kockázatkezelése körében.⁶¹ Az eljárás folyamatban van.
- 2023. október 19. Meta - Információkérés kockázatértékelések és kockázatsökkentő intézkedések a választások integritásának védelme érdekében, valamint a Hamász által Izraelben elkövetett terrortámadásokat követően, különös tekintettel az illegális tartalmak és a dezinformáció terjesztésére és felerősítésére.⁶²
- 2023. november 6. AliExpress - Információkérés a fogyasztók online védelmét szolgáló kockázatértékelésekkel és kockázatsökkentő intézkedésekkel kapcsolatos kötelezettségek, különös tekintettel az illegális termékek, például a hamisított gyógyszerek online terjesztésére vonatkozóan.⁶³ Az információkérést követően a Bizottság 2024. március 14-én eljárást indított a 66. cikk felhatalmazása alapján, a kockázatok kezeléséhez és mérsékléséhez, a tartalom moderálásához és a belső panaszkezelési mechanizmushoz, a hirdetési és ajánlórendszerek átláthatóságához, a kereskedők nyomon követhetőségéhez és a kutatók adathozzáférésehez kapcsolódó kötelezettségek vonatkozásában.⁶⁴ Az eljárás folyamatban van.

⁵⁸ [The Commission sends request for information to X under the Digital Services Act | Shaping Europe's digital future](#)

⁵⁹ <https://digital-strategy.ec.europa.eu/en/news/commission-requests-information-x-decreasing-content-moderation-resources-under-digital-services>

⁶⁰ <https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-tiktok-under-digital-services-act>

⁶¹ <https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-tiktok-under-digital-services-act>

⁶² <https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-0>

⁶³ <https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-aliexpress-under-digital-services-act>

⁶⁴ <https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-aliexpress-under-digital-services-act>

- 2023. november 9. TikTok és Youtube - Információkérés az online kiskorúak védelmét szolgáló kockázatértékelésekkel és kockázatsökkentő intézkedésekkel kapcsolatos kötelezettségek, különös tekintettel a mentális és fizikai egészséget érintő kockázatokra, valamint a szolgáltatásaik kiskorúak általi használatára vonatkozóan.⁶⁵
- 2023. november 10. Meta és Snapchat - Információkérés az online kiskorúak védelmét szolgáló kockázatértékelésekkel és kockázatsökkentő intézkedésekkel kapcsolatos kötelezettségek, különös tekintettel a mentális és fizikai egészséget érintő kockázatokra, valamint a szolgáltatásaik kiskorúak általi használatára vonatkozóan.⁶⁶ Az információkérést követően a Bizottság 2024. május 10-én eljárást indított a 66. cikk felhatalmazása alapján, a Meta ellen a kiskorúakat érintő intézkedései és üzleti modellje miatt. Az eljárás folyamatban van.⁶⁷
- 2023. november 15. Amazon - Információkérés a fogyasztók online védelmét szolgáló kockázatértékelésekkel és kockázatsökkentő intézkedésekkel kapcsolatos kötelezettségek, különös tekintettel az illegális termékek terjesztésére és az alapvető jogok védelmére, valamint az ajánlórendszereknek a DSA vonatkozó rendelkezéseinek való megfelelésére vonatkozóan.⁶⁸ 2024. július 5-én a Bizottság újabb információkat kért a szolgáltatótól, a platform által az ajánlási rendszerek és paramétereik átláthatóságával kapcsolatos DSA-kötelezettségeknek, valamint a hirdetési adattár és a kockázatértékelési jelentés fenntartására vonatkozó rendelkezéseknek való megfelelés érdekében hozott intézkedésekről.⁶⁹
- 2023. december 1. Meta - Információkérés a kockázatok értékelésére és a kiskorúak védelmével kapcsolatos hatékony enyhítő intézkedések meghozatalára vonatkozó kötelezettségek, beleértve a gyermekek szexuális zaklatásával kapcsolatos, saját készítésű anyagok (SG-CSAM) Instagramon történő terjesztését is. Tájékoztatást kérnek továbbá az Instagram ajánlórendszeréről és a potenciálisan káros tartalmak felerősítéséről.⁷⁰
- 2023. december 15. Apple és Google - Információkérés App Store-t és a Google Play-t érintő rendszerszintű kockázatok azonosítási módszertanára vonatkozóan
- 2024. január 18. 17 szolgáltatónak küldött információkérés azzal kapcsolatban, hogy miként tesznek eleget a kutatói adathozzáférés biztosításának, amelyet a Bizottság az átláthatóság, elszámoltathatóság alapjának tekint.⁷¹
- 2024. március 1. Meta - Információkérés a Facebook és az Instagram hirdetési gyakorlatára, az ajánlórendszerekre és az említett előfizetési lehetőség bevezetésével kapcsolatos kockázatértékelésekre vonatkozó kötelezettségek tárgyában.⁷²

⁶⁵ <https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-tiktok-and-youtube-under-digital-services-act>

⁶⁶ <https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-meta-and-snap-under-digital-services-act>

⁶⁷ <https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-meta-under-digital-services-act-related-protection>

⁶⁸ <https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-amazon-under-digital-services-act>

⁶⁹ <https://digital-strategy.ec.europa.eu/en/news/commission-requests-information-amazon-under-digital-services-act>

⁷⁰ <https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act>

⁷¹ <https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-17-very-large-online-platforms-and-search-engines-under>

⁷² <https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-1>

- 2024. március 14. LinkedIn - ⁷³ Információkérés azzal kapcsolatban, hogyan felel meg a szolgáltatásuk a személyes adatok különleges kategóriáinak felhasználásával profilalkotáson alapuló hirdetések bemutatása tilalmának. A Bizottság információkérésére tekintettel a szolgáltató teljesen inaktíválta a kapcsolódó hirdetési szolgáltatásokat.⁷⁴
- 2024. március 14. 6 óriásplatform és 2 keresőmotor - Információkérés a generatív mesterséges intelligenciához kapcsolódó kockázatokra vonatkozó intézkedéseikről, mint például az úgynevezett "hallucinációk", amikor a mesterséges intelligencia hamis információkat szolgáltat, a deepfake terjesztése, valamint az úgynevezett automatizált manipuláció tekintetében, amely félrevezetheti a választókat egy választás során. A Bizottság további információkat kért azokra a belső dokumentumokra vonatkozóan, amelyek a generatív mesterséges intelligenciának a választási folyamatokra, az illegális tartalmak terjesztésére, az alapvető jogok védelmére, a nemi alapú erőszakra, a kiskorúak védelmére, a mentális jólétre, a személyes adatok védelmére, a fogyasztóvédelemre és a szellemi tulajdon védelmére gyakorolt hatásával kapcsolatos kockázatértékelésekről és kockázatsökkentő intézkedésekről szólnak.⁷⁵ A Microsoft nem tett eleget az információkérésnek, így a Bizottság 2024 májusában kötelezte az információk kiadására.⁷⁶
- 2024. április 17. TikTok – Információkérés, amelyben a szolgáltató új TikTok Lite alkalmazásának az EU-ban történő bevezetése előtt elvégzett kockázatértékelését kérte kiadni.⁷⁷ A Bizottság 2024. április 24-én,⁷⁸ 66. cikk szerinti eljárást indított a szolgáltató ellen, arra tekintettel, hogy a DSA értelmében köteles lett volna kockázatértékelési jelentést benyújtani, amely tartalmazza a várható rendszerszintű kockázatok mérséklésére irányuló intézkedéseket, mielőtt olyan új funkciókat indítanának, amelyek valószínűleg kritikus hatással lehetnek ezekre. A Bizottság eljárására tekintettel a TikTok felfüggesztette a szolgáltatást egy átmeneti időszakra.⁷⁹ 2024 augusztusában pedig a szolgáltató úgy döntött, hogy véglegesen megszünteti a Lite szolgáltatáselemet a megfelelésének biztosítása érdekében.⁸⁰
- 2024. április 30. Facebook és Instagram - Információkérés feltételezett jogsértések ügyében, amelyek a Meta szolgáltatásainak megtévesztő reklámokkal és politikai tartalmakkal kapcsolatos politikájára és gyakorlatára vonatkoznak. A kifogások arra is vonatkoztak, hogy az európai parlamenti választások előtt nem állt rendelkezésre hatékony, harmadik féltől származó, valós idejű, polgári diskurzust és választásokat figyelő eszköz, tekintettel arra, hogy a Meta a CrowdTangle nevű, valós idejű, nyilvános információkkal foglalkozó eszközét megfelelő helyettesítő eszköz nélkül

⁷³ <https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-linkedin-potentially-targeted-advertising-based-sensitive-data>

⁷⁴ <https://digital-strategy.ec.europa.eu/en/news/statement-commissioner-breton-steps-announced-linkedin-comply-dsa-provisions-targeted-advertisement>

⁷⁵ <https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-linkedin-potentially-targeted-advertising-based-sensitive-data>

⁷⁶ <https://digital-strategy.ec.europa.eu/en/news/commission-compels-microsoft-provide-information-under-digital-services-act-generative-ai-risks>

⁷⁷ <https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-tiktok-regarding-launch-tiktok-lite-france-and-spain>

⁷⁸ <https://digital-strategy.ec.europa.eu/en/news/commission-opens-proceedings-against-tiktok-under-dsa-regarding-launch-tiktok-lite-france-and-spain>

⁷⁹ <https://digital-strategy.ec.europa.eu/en/news/statement-commissioner-breton-announcement-tiktok-suspend-tiktok-lites-reward-programme-eu>

⁸⁰ <https://digital-strategy.ec.europa.eu/en/news/tiktok-commits-permanently-withdraw-tiktok-lite-rewards-programme-eu-comply-digital-services-act>

megszüntette.⁸¹ 2024. augusztus 16-án a Bizottság újabb információkérést küldött több információt kérve arról, hogy milyen intézkedéseket hozott a szolgáltató annak érdekében, hogy eleget tegyen azon kötelezettségének, hogy a kutatók számára hozzáférhető adatokhoz, valamint arról, hogy tervezi a választások és a közvélemény alakulásának megfigyelésére szolgáló funkcióinak frissítését.⁸²

- 2024. június 13. Pornhub, Stripchat és az XVideos – Információkérés a kiskorúak online védelmével kapcsolatos kockázatok gondos felmérése és csökkentése, valamint az illegális tartalmak és a nemi alapú erőszak terjedésének megakadályozása érdekében hozott intézkedések körében. A Bizottság többek között részleteket kért a pornográf platformok által elfogadott korhatár-biztosítási mechanizmusokról.⁸³ A Bizottság 2024. október 18-án újabb információkérést küldött a szolgáltatóknak, amelyben az átláthatósági jelentéstételi kötelezettséget vizsgálja, mivel a Bizottság gyanúja szerint nem rendelkeznek világos és könnyen érthető információkkal a tartalommoderálási gyakorlatokról. Az információkérés terjedelme kiterjedt a bírósági végzésekre, értesítésekre, a tartalommoderálási folyamatokra, a belső panaszkezelő rendszerre, valamint a tartalommoderáláshoz használt automatizált eszközökre vonatkozó információkra.⁸⁴
- 2024. június 28. Temu és Shein – Információkérés a DSA-kötelezettségeknek való megfelelés érdekében hozott intézkedések az úgynevezett "értesítési és intézkedési mechanizmussal", az online felületekkel, a kiskorúak védelmével, az ajánlórendszerek átláthatóságával, a kereskedők nyomon követhetőségével és a beépített megfelelőséggel kapcsolatban.⁸⁵ 2024. október 31-én a Bizottság 66. cikk szerinti eljárást indított a Temu ellen, a fenti tárgykörökben tapasztalt gyakorlatok jogszerűtlensége miatt.⁸⁶
- 2024. október 2. TikTok, Snapchat, Youtube – Információkérés az ajánlórendszerek kialakításával és működésével kapcsolatban, beleértve a felhasználók mentális egészségét és a káros tartalmak terjesztésére vonatkozó intézkedéseket.⁸⁷ 2024. november 29-én a Bizottság újabb információkéréssel fordult a TikTok irányába a platformon megjelenített felhasználói tartalmak manipulációja esetén a kockázatok kezeléséről, kiemelten a visszaélés szerű rendszerhasználat, az ajánlórendszereiből eredő kockázatokra, valamint a választási folyamatokkal kapcsolatos rendszerszintű kockázatokra.⁸⁸

⁸¹ <https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-facebook-and-instagram-under-digital-services-act>

⁸² <https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-2>

⁸³ <https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-illegal-content-and-protection-minors-pornhub-xvideos-and>

⁸⁴ <https://digital-strategy.ec.europa.eu/en/news/commission-requests-information-under-digital-services-act-pornhub-stripchat-and-xvideos-their>

⁸⁵ <https://digital-strategy.ec.europa.eu/en/news/commission-requests-information-online-marketplaces-temu-and-shein-compliance-digital-services-act>

⁸⁶ <https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-temu-under-digital-services-act>

⁸⁷ <https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-youtube-snapchat-and-tiktok-recommender-systems-under-digital>

⁸⁸ <https://digital-strategy.ec.europa.eu/en/news/commission-sends-additional-request-information-tiktok-under-digital-services-act>

- 2024. október 11. Temu – Információkérés az online piactéren illegális termékeket értékesítő kereskedők jelenléte és újbóli megjelenése ellen hozott intézkedésekről.⁸⁹

8. Következtetések és javaslatok

Az Európai Unió stratégiai jellegű dokumentumai, jogi normái és a vonatkozó joggyakorlat elemzését követően több következtetést és javaslatot lehet levonni a DSA ex ante alapjog védelmi szabályozásának tekintetében, figyelemmel a megfogalmazott kutatási kérdésre. Ezek áttekinthetősége érdekében két csapásirányon, az ex ante szabályozás előnyeit és esetleges hátrányait vizsgálva csoportosítva adja közre a tanulmány.

8.1 Az ex ante szabályozás alkalmazásának előnyei

Az ex ante szabályozás egyik kiemelt előnye, hogy proaktívan, a problémák bekövetkezése előtt próbálja kezelni azokat. Ez különösen fontos az online térben, ahol a jogsértések terjedési sebessége és hatása jelentősen felülmúlja a hagyományos offline problémákét. A DSA 34. cikkében foglalt kockázatértékelési kötelezettség kifejezetten ezt a célt szolgálja. Az óriásplatformok és a nagyon népszerű keresőmotorok szolgáltatói kötelesek rendszeres kockázatértékelést végezni, amely során azonosítják a rendszerszintű alapvető jogokat veszélyeztető kockázatokat. Ezeket kötelesek rendszeresen felül is vizsgálni, akkor is, ha egy, a kockázatokat jelentősen érintő új funkciót vagy szolgáltatáselemet kívánnak bevezetni az európai piacra.

A szabályozás előnyei több módon jelentkeznek:

- egyrészt az érintett szolgáltatók, miután azonosításra kerülnek az Európai Bizottság által, valójában nem tehetik meg, hogy nem foglalkoznak a kötelezettséggel, európai jelenlétük esetén rá vannak kényszerítve, hogy elvégezzék a kockázatértékelést, annak megfelelő kockázatsökkentési és válságkezelési mechanizmusokat alkalmazzanak,
- másrészt a következetes jogalkalmazási tevékenység segítségével elérheti az Európai Bizottság, hogy a szolgáltatók tényleges ellenőrzés hiányában önkéntes jogkövetést tanúsítsanak, tartva attól, hogy a követelmények be nem tartása esetén a Bizottság formális információkéréssel, majd a DSA 66. cikke szerinti eljárás megindításával fogja kezelni a meg nem felelést,
- mindez pedig elvezethet oda, hogy az európai alapjogi készlet elemei beépülnek a szolgáltatók által alkalmazott szolgáltatásokba, azok algoritmusába, megvalósítva a *legality by design* koncepciót, amely a DSA követelményrendszerében is megjelenik (31. cikk).

A fentiek meg is jelennek a Bizottság jogalkalmazási folyamataiban: a TikTok 7. fejezetben hivatkozott TikTok Lite rendszere tekintetében, az előzetes kockázatértékelési dokumentáció hiánya miatt és a rendszerszintű kockázatok kezelésére tervezett intézkedésekkel kapcsolatos aggályokra tekintettel a Bizottság határozott fellépést tett formális információkéréssel és 66. cikk szerinti eljárással, amelyre válaszul a szolgáltató előbb átmenetileg, majd végleg kivezetette a tervezett szolgáltatást az európai piacról. Hasonló helyzetet láthatunk a LinkedIn tekintetében a célzott hirdetési tevékenységre vonatkozóan, s mindezek arra utalnak, hogy a DSA

⁸⁹ <https://digital-strategy.ec.europa.eu/en/news/commission-requests-information-under-digital-services-act-temu-traders-selling-illegal-products>

szabályozása és az Európai Bizottság fellépése elegendő súlyt biztosít a DSA vonatkozó szabályainak végrehajtásához.

A szabályozás egy fontos hozadéka eközben, hogy láthatóvá teszi a platformok és a mögöttük működő algoritmusok szempontrendszerét, megfontolásait. Ezeket egyrészt közzé kell tenniük a szolgáltatóknak az általános szerződési feltételek keretében (mint a szolgáltatás során alkalmazható korlátozások), másrészt rendszeresen be kell számolniuk ezek teljesüléséről az átláthatósági kötelezettség megvalósításának részeként. Ennek keretében világos tájékoztatást kell nyújtaniuk a felhasználók számára a tartalommoderációs gyakorlatokról, az algoritmus alapú döntéshozatalról és az adatkezelési gyakorlatokról. Ezek hiányosságai esetén a Bizottság a fentiekhez hasonlóan eljárást indíthat a követelmények érvényesítése érdekében. Az átláthatóság növelése ugyan csak áttételesen erősíti az alapvető jogok védelmét, de mégis preventív hatást gyakorolhat, egyrészt a felhasználók tudatosságának növelésével (láthatóvá teszi a szolgáltatás használatával felmerülő kockázatokat), másrészt azzal, hogy kevésbé rejthetők el az alapjogi szempontból kockázatos gyakorlati megoldások.

A DSA ex ante szabályai a tekintetben is új, megbízhatóbb védelmet jelenthetnek az alapvető jogok területén, hogy a szolgáltatók kockázatértékelési tevékenységének központjában a rendszerszintű kockázatok felmérése és kezelése áll, amelyek a szolgáltatások üzemeltetéséből adódnak. Ezek a kockázatok nemcsak egyéni szinten, hanem kollektív, társadalmi szinten is jelentős alapjogi sérelmeket okozhatnak. E rendszerszintű kockázatok pedig nem olyan könnyen megkerülhetőek, mint azt a szolgáltatók tették korábban egy-egy egyedi alapjog sérelmi ügyben, amelyek ugyan érintették a szolgáltatások működésének egyik vagy másik funkcióját vagy részét, de mégis folyamatosan hagytak kibúvót a szolgáltatóknak azáltal, hogy az egyedi ügyben felmerülő jogsérelemre reagáltak a jogalkalmazó szerv döntése alapján, miközben a szolgáltatással kapcsolatban felmerült rendszerszintű kockázatok több ízben nem javultak. Erre példát szolgáltatathat az óriásplatformok és a választások kérdése – korábban számtalan ízben felmerült a platformok szerepe és felelőssége választási eredmények befolyásolása kérdésében (Cambridge Analytica ügy), mégis a szolgáltatók jelentős, érdemi előrelépés nélkül üzemeltethették tovább szolgáltatásaikat a DSA hatályba lépése előtt, holott alapjogi szempontból éppen a felhasználók és az érintett ország vagy közösség egyik legfontosabb alapvető jogosultságát korlátozták vagy veszélyeztették. A DSA hatályba lépését követően egyértelműen kimutatható az Európai Bizottság joggyakorlatában az az irány, amely az ilyen jellegű visszaélések megelőzését szolgálja, számos szolgáltatóval van folyamatban információkérés vagy 66. cikk szerinti eljárás a választási integritás kérdéseire és a befolyásolás egyéb jelenségeire vonatkozó, rendszerszintű kockázatok azonosítása és kezelése tárgyában.

8.2 Az ex ante szabályozás alkalmazásának hátrányai, hiányosságai

Az ex ante szabályozás kapcsán fontos következtetésként adható közre, hogy a szabályozás nagyon hatékony lehet bizonyos típusú rendszerszintű kockázatok kiszűrésében és azok kezelésében, valamint a 8.1. fejezetben vázolt előnyök mentén átláthatóság növelő hatása lehet a felhasználók irányába, nagyobb betekintést és felügyeletet biztosítva a felügyeletet ellátó szervezeteknek – egyúttal azonban be kell látni, hogy nem tud minden esetre megoldást nyújtani az alapvető jogok sérelmeinek sajátosságai miatt.

Az alapvető jogok területén bekövetkező sérelmek sok esetben csak ex post válnak felismerhetővé, miután egy konkrét esemény vagy döntés már bekövetkezett, olyannyira, hogy ezek jogi megítélése sok esetben többfórumos jogalkalmazási folyamatok és minden

jogorvoslati lehetőség kimerítése után is vitatható vagy vitatott marad. Az ex ante szabályozás, amelynek központi elemei előzetes kockázatelemzésen és megelőző mechanizmusokon alapulnak, éppen ezért nehezen alkalmazhatóak olyan jogsértésekre, amelyek jellege több esetben egyéni nézőpontból értelmezhető, vagy csak utólag értékelhető.

Mindez oda vezethet, hogy a szolgáltatók a kockázatértékelésüket a várható szituációkra, a felhasználók várt és modellezett magatartására, elképzelt élethelyzetekre fogják elkészíteni, hiszen azokat (ugyan akár tesztüzem után) a technológiai megoldás, szolgáltatás bevezetése előtt kell megtenniük, még akkor is, ha ezt a kockázatértékelést utána kötelesek rendszeresen felülvizsgálni és kiigazítani, s mindebben az Európai Bizottság információkérési megkeresései is egyfajta irányzékot jelenthetnek számukra. Éppen a kockázatértékelési módszertan az, ami immanensen magába foglalja azt a kockázatot, hogy a gyakorlatban előfordulhat olyan eset, alapjog védelmi szempontból kritikus szituáció vagy megoldás, amelyet a szolgáltatók nem képesek pontosan előrejelezni. Kiválóan mutatja ennek kockázatát az EUB korábbi gyakorlatából a Glawischnig-Piesczek kontra Facebook Ireland Ltd. (C-18/18) ügy, ahol EUB ítéletében hangsúlyozta, hogy egy adott tartalom eltávolítása nem feltétlenül orvosolja önmagában az okozott alapjog sérelmet, és önmagában az ex post jellegű beavatkozás vagy annak hiánya is jelenthet újabb sérelmet e tekintetben. Az eset arra is rávilágít, hogy a jogsértések pontos kontextusa és jelentősége csak utólag állapítható meg, különösen, ha vitás a jogsértés tényleges bekövetkezése. Elviekben ezt a problémát orvosolja a belső panaszkezelési rendszer használata és az eset összes körülményét érintő kivizsgálás, kivételes helyzetekre tekintettel a válságkezelési mechanizmusok alkalmazása a DSA szabályai mentén, de a gyakorlatban azonban nagyon nehezen megítélhető, hogy valóban sérült-e alapvető jog, így például a véleménynyilvánítás szabadsága.

Ráadásul az alapvető jogok tulajdonságai nem egyezők e tekintetben: vannak olyan potenciális alapjog sérelmek, amelyek jól detektálhatók, kifejezetten előre lehet jelezni bekövetkezésüket egy-egy technológiai megoldás adott környezetben való alkalmazása során, míg más alapjogok esetében a szabályozás tárgyát képező kockázatok nem számszerűsíthetők vagy objektíven nem jól megfigyelhetők vagy mérhetők. Míg a konkrét és azonnali károkkal járó sérelmek általában jól mérhetők, addig az olyan alapvető jogi sérelmek, mint például a véleménynyilvánítás szabadsága, gyakran szubjektív megítélés alá esnek. A helyzetet az is rontja, hogy a platformszolgáltatások tekintetében éppen azoknak az alapjogoknak a sérelme várható, amelyek esetében az előrejelezhetőség vagy az eset jogi megítélése bizonytalan, s e tekintetben a kockázatértékelés ex ante jellegű megoldásai veszíthetnek hatékonyságukból, így nem lesznek képesek minden esetben megelőzni a jogsértést. Ebben az esetben is lehet azonban szerepük: ha nem is lehetséges a jogsérelem megelőzése annak bekövetkezése előtt, mégis kedvezőbb kereteket teremthet az ex post jellegű intézkedésekre, igényérvényesítésre és hatósági beavatkozásra az, hogy a hatóságoknak és bíróságoknak nem kell minden kapaszkodó nélkül felépíteni a vizsgált tényállást, hanem abban segítségére lehetnek a DSA szabályai alapján kiépült belső szabályozási rendszer megoldásai és dokumentumai. Egy alapjog sérelmi esetben ha a bekövetkezett sérelem jogi megítélését nem is befolyásolja például az előzetesen lefolytatott kockázatértékelés alapossága, a szolgáltatóra kiszabható szankciók tekintetében mégis jelentőséggel bírhat, hogy a szolgáltató mennyire volt tisztában a kockázat jelenlétével, milyen megelőző intézkedéseket vezetett be, ezekhez milyen erőforrásokat rendelt, s például ismétlődő esetben megtette-e a szükséges intézkedéseket annak érdekében, hogy elejét vegye további sérelmek kialakulásának. Ilyen szempontból az ex ante szabályozás áttételes előnyét állapíthatjuk meg, amely egyszerre ösztönzi a szolgáltatókat folyamatos fejlődési pályán tartani szolgáltatásaikat alapjog védelmi szempontból, s egyúttal megalapozza az igényérvényesítés és felelősségre vonás alapját is.

Azt is látni kell, hogy az ex ante jellegű kötelezettségeknek van korlátja, és ez egyes kötelezettségek megformálásában markánsan érzékelhető válik. Ilyen az átláthatósági kötelezettségek köre: a DSA a szolgáltatóknak előírja egyrészt, hogy az általános szerződési feltételek keretében adjanak kereteket a szolgáltatásaikat érintő korlátozásokról, másrészt rendszeres időközönként készítsenek átláthatósági jelentéseket, amelyek magukba foglalnak számos olyan tevékenységgel kapcsolatos beszámolót, amely az alapjogok védelme szempontjából is kulcsfontosságú (így pl. a tartalommoderációs tevékenység tapasztalatairól, alkalmazott megoldásairól). Ugyanakkor érzékelhető, hogy az átláthatóság fokozására nem feltétlenül alkalmas egy évenként közreadott jelentés. Az átláthatóságot fokozó intézkedéseknek ennél sokkal mélyebben, szervezesebben kellene beleépülniük a szolgáltatások nyújtásába ahhoz, hogy valóban bekövetkezzen a felhasználók irányába a szolgáltatás átláthatóvá tétele az egyedi szolgáltatásnyújtási folyamatban.⁹⁰ Mindennek viszont technológiai korlátai is vannak: az alkalmazott algoritmusok természetükből fakadóan nem mindig alkalmasak működési metódusok teljes bemutatására, s egyúttal pl. a tartalommoderáció területén alkalmazott automatizált megoldások nem képesek figyelembe venni a tartalmak kontextusát, amely viszont kulcsfontosságú az alapvető jogok védelme szempontjából. Egy ezen a téren alkalmazott algoritmus nem mindig tudja felismerni, hogy egy tartalom kontextusában ironikus vagy sértő, gyűlöletbeszédet valósít meg vagy más jogsértést okoz, ami hibás döntésekhez vezethet és végül a szolgáltató felelősségét eredményezheti olyan esetekben is, amikor jelenleg nincs más elérhető technikai megoldás egy adott probléma kezelésére. Ezt egyébként a DSA szabályozása is figyelembe veszi, amikor a (86) preambulumbekkezdésben kijelenti, hogy a rendszerszintű kockázatok kezelésére szolgáló intézkedéseknek arányosnak kell lenniük az azokat üzemeltető szolgáltatók gazdasági kapacitásaival, de kérdéses, hogy mennyire fog megjelenni a felügyeletet ellátó szervek döntéseinek mérlegelésében.

Az ex ante szabályozás eközben jelentős adminisztratív terhet ró az érintett szolgáltatókra, különösen a kisebb szereplőkre. A folyamatos kockázatértékelés, a kockázatcsökkentési intézkedések bevezetése és fenntartása, a jelentéstételi kötelezettségek és független auditok nagyban növelik a megfelelőség költségeit, és különösen hátrányosan érinthetik az innovációra és növekedésre törekvő kisebb vállalkozásokat. Habár a DSA rétegzett szabályozása, a mikro- és kisvállalkozások szabályozás hatálya alóli részleges kizárása (19. cikk, de megjelenik más helyeken is, mint a DSA 15. cikke az átláthatósági jelentési kötelezettségek körében), azt a célt szolgálja, hogy a megfelelőség költségei igazodjanak a nyújtott szolgáltatás nagyságrendjéhez és kockázataihoz, egyúttal mégis kialakulhat egy réteg, amely már a szigorúbb szabályok betartására kötelezett, de akár jelentős versenyhátrányba hozhatja az ex ante szabályozásnak való megfelelés. Ilyen eset lehet az, amikor a mikro- vagy kisvállalkozás szolgáltatása eléri a DSA 33. cikkében meghatározott küszöbértékeket és mégis eleget kell tennie a követelményeknek (ld. 19. cikk (2) bek.). Erre a DSA 33. cikkének (6) bekezdése alapján, a kijelölést követően a szolgáltatónak négy hónapja van. Ez idő alatt kell, hogy teljes mértékben megfeleljen a DSA vonatkozó kötelezettségeinek, amely az életbe lépő kötelezettségek alapján meglehetősen szűknek tekinthető. Erre a minősítési problémára gyakorlati példaként hozható fel a Zalando esete, akit az Európai Bizottság óriásplatformként vett nyilvántartásba, s ennek megfelelően tekint rá a jogalkalmazási folyamatok során, küldi meg számára információkérési megkereséseit, de eközben a szolgáltató éppen csak elérte azokat a minősítési határokat, amelyet a DSA 33. cikke meghatározott. A Zalando erre tekintettel 2023. júniusában keresett nyújtott be az Európai Unió Bíróságához vitatva a Bizottság minősítését, azzal érvelve, hogy az Európai Bizottság nem vette figyelembe üzleti modelljének többségi kiskereskedelmi jellegét, és hogy tevékenysége nem jelent "rendszerszintű kockázatot" a harmadik féltől

⁹⁰ ZÖDI Zsolt: Átláthatósági és indokolási követelmények az európai platformjogban. *In Medias Res* 12(2), 2023. 5-24.

származó káros vagy jogszerűtlen tartalom terjesztése szempontjából, hivatkozva arra, hogy a minősítés időpontjában nem volt világos és következetes módszertan annak értékelésére, hogy egy vállalat óriásplatformnak minősül-e. A bíróság eljárása jelen tanulmány megírásakor még folyamatban van, de jól mutatja azt, hogy a piaci szolgáltatók közül is azonosítható egy olyan réteg, amely épphogy eléri a minősítési határt a DSA követelményei alapján, de erőforrásait tekintve jóval kisebb és európai székhelyű szereplőnek tekinthető, mint a versenytársai, de számára a szabályozás, különösen annak ex ante jellegű szabályai jelentős versenyhátrányt okozhatnak a megemelkedő megfelelési költségek okán.

Másrészről az ex ante jellegű kötelezettségek speciális piacra lépési korlátot hozhatnak létre: míg a korábbi szabályozás jogsérelem kialakulásának hiányába megengedte azt, hogy a szolgáltató hosszú évek gyakorlati működésének tapasztalatai alapján kísérletezze ki, hogy miként tud a jogszerű működést minél inkább megvalósító szolgáltatásokat és mögöttük működő technológiai megoldásokat létrehozni, addig a jelenlegi szabályozás, különösen ha annak szigorúbb követelményeit vesszük figyelembe, már a bevezetés pillanatában a legmagasabb szintű felkészültséget várja el. Mindez indokolható a platformok okozta negatív hatások és az alapjogok mindenek felett érvényesülő védelme szempontjából, de sok tekintetben innovációhűtő hatásuk lehet, amely megterheli az európai gazdaság fejlődését.

8.3 Konklúzió és javaslatok

A DSA ex ante szabályozási kerete jelentős előrelépést jelent az alapvető jogok védelmében, különösen a gyorsan változó digitális térben. Az előzetes kockázatértékelések, az átláthatósági követelmények és a rendszerszintű problémák kezelése számos esetben előremutató jelleggel teszik kézzel foghatóvá egyes szolgáltatások adottságait és a rendszerszintű kockázatokat. Így van ez akkor is, ha az érintett alapjog megsértése jellemzően ex post érzékelhető vagy várható intézkedés a szolgáltatótól, mert az ex ante szabályozásnak megfelelő belső szabályozási környezet és dokumentumok létrehozása és fenntartása kedvezőbb kereteket teremt az ex post jellegű intézkedésekre, igényérvényesítésre és hatósági beavatkozásra. Az ex ante szabályozás áttételes előnyeként azonosítható az is, hogy a szolgáltatók kénytelenek folyamatos fejlődési pályán tartani szolgáltatásaikat és az azokba beépülő technológiai megoldásokat alapjog védelmi szempontból felülvizsgálni, s ez egyúttal megalapozza az igényérvényesítés és felelősségre vonás alapját is, amennyiben ezt a fejlődési ívet nem tartják.

Az ex ante szabályozás sikeressége nagymértékben függ attól, hogy mennyire képes rugalmasan alkalmazkodni az új kihívásokhoz, és mennyire támogatja azt az ex post szabályozás, azaz a Bizottság, a tagállami digitális szolgáltatási koordinátorok és bíróságok a jogérvényesítés során. A szolgáltatók, a megfelelés magas költségei miatt várhatóan csak abban az esetben fogják tartani magukat a DSA követelményrendszeréhez, ha ezt kikényszeríti a következetes jogalkalmazás. E tekintetben kifejezetten pozitív szabályozási fejlemény, hogy az elaprózódó tagállami jogalkalmazás helyett a Bizottság széles körű hatáskörrel rendelkezik az ex ante kockázatértékelési és kockázatsökkentési kötelezettségek, valamint a válságkezelési mechanizmusok felügyeletére. Ezek a hatáskörök biztosítják, hogy az online óriásplatformok és keresőszolgáltatók megfelelően végrehajtsák a DSA előírásait, és proaktívan kezeljék a rendszerszintű kockázatokat. A Bizottság felügyeleti tevékenysége, amely magában foglalja az információgyűjtést, vizsgálatokat, szankciókat és a folyamatos nyomon követést, kulcsszerepet játszik a digitális szolgáltatások szabályozásának hatékonyságában és az alapvető jogok védelmében.

A lefolytatott elemzés alapján több javaslat is megtehető az ex ante alapjogvédelmi kötelezettségek alkalmazásának fejlesztésére, ezeket az alábbiakban ismertetem:

1. Kockázatértékelési módszerek továbbfejlesztése

A Bizottság gyakorlatában már most észlelhető az az irányultság, amely nagyon helyeselhető módon, a rendszerszintű kockázatok értékelésére vonatkozóan részletes, egységesített módszertanok kidolgozását jelenti. Ilyennel találkozhatunk a választási integritás kérdéseire és a befolyásolás egyéb jelenségeire vonatkozó, rendszerszintű kockázatok azonosítása és kezelése tárgyában kiadott iránymutatások tekintetében,⁹¹ vagy az online dezinformációs kampányok területén.⁹² Az iránymutatások segíthetik a szolgáltatókat abban, hogy a várható szituációkra, a felhasználók várt és modellezett magatartására, elképzelt élethelyzetekre elkészített kockázatértékelések több év alatt eljussanak oda, hogy érdemben közelítsék a valós folyamatokat, akár úgy, hogy a szolgáltatók a kockázatértékelés elkészítéséhez is automatizált, mesterséges intelligenciára épülő megoldásokat alkalmaznak a jellemző rendszerszintű kockázatok felméréséhez.

2. Partnerség és együttműködés

A fentihez képest hasonló jelentőségű lehet a Bizottságnak azon lehetősége, hogy amennyiben saját értesülései, illetve a formális információszolgáltatási megkeresése alapján úgy találja, hogy a szolgáltató ugyan nem valósít meg jogsértést a DSA szabályai mentén az ex ante jellegű kötelezettségek teljesítése szempontjából, de megítélése szerint helye lenne a szolgáltatáson vagy az ex ante kötelezettségek teljesítésének módján fejleszteni, úgy proaktív konzultációba kezdjen amire lehetőséget adnak számára a DSA-ban foglalt szabályok. Hasonlóképp célszerű lehet arra törekedni, hogy a DSA 66. cikke alapján megindult eljárásokban lehetőség szerint a nem megfelelést megállapító határozat létrehozatala helyett arra törekedjen, hogy, amennyiben az eset összes körülménye engedi, a szolgáltató kötelezettségvállalásokat tegyen, mert ez a megoldás egyszerre biztosíthatja az alapjogok magas szintű védelmét, a DSA szabályainak való megfelelést, s egyúttal a szolgáltatók bevonását a döntésbe és a számukra legkevésbé hátrányos technológiai megvalósítás kiválasztását is. Az így elért önkéntes jogkövetés fontos lehet, mert bár komoly represszív erővel rendelkező bírságtételekkel dolgozhat a Bizottság, végső soron elérheti, hogy a tagállami hatóságok – így a digitális szolgáltatási koordinátor jelzése alapján a tagállami bíróság - korlátozzák, elérhetetlenné tegyék ideiglenesen a szolgáltatást egy adott tagállamban a DSA 82. cikk (1) bekezdésében és a DSA 51. cikk (3) bek. b) pontjában foglaltaknak megfelelően, mégis ezek az intézkedések olyan költség- és időigényesek, hogy célszerűbb lehet a megfelelés gyorsabb módját elérni, ha arra lehetőség van. Ez akár a minősítési határokat elérő, de kisebb szereplők megfelelését is elősegíthetné, mert lehetőséget adna egyedi feltételek megállapítására.

3. Jogalkalmazási folyamatok láthatóvá tétele a felhasználók széles köre számára

Lehet bármilyen hatékony a Bizottság vagy a digitális szolgáltatási koordinátorok

⁹¹ <https://digital-strategy.ec.europa.eu/en/news/commission-publishes-guidelines-under-dsa-mitigation-systemic-risks-online-elections>

⁹² <https://digital-strategy.ec.europa.eu/en/library/digital-services-act-study-risk-management-framework-online-disinformation-campaigns>

(önállóan vagy amikor bevonja őket a Bizottság ebbe) tevékenysége az ex ante jellegű kötelezettségek érvényesítése tárgyában, ha az eljárások és azok eredménye nem jól látható az európai állampolgárok és kifejezetten az adott szolgáltatást igénybe vevő felhasználók számára. Nagy szükség lenne arra, hogy a folyamatban lévő információkéréseket, s különösen a DSA 66. cikke alapján indult eljárásokat interaktív, jól elérhető, jól értelmezhető, közérthető, s akár grafikailag értelmező, felhasználóbarát formában is megjelenítse, saját nyilvános felületein, akár olyan szabályok beiktatásával, amelyek kötelezővé teszik a szolgáltatóknak a folyamatban lévő eljárások vagy a megállapított jogsértések közzétételét a felhasználók számára jól látható módon. A Bizottság ugyanis jelen pillanatban sajtóközleményekben, hírfolyamban és jelentésekben tájékoztatja a nyilvánosságot az aktuális eljárásokról, holott ezek helyett vagy mellett a felhasználók tudatosításában az nyújtana érdemi segítséget, ha a felhasználók ugyanolyan könnyen kapnának ezekről információt, mint amilyen könnyen elérik a platformszolgáltatásokat egyébként. E tevékenységben a digitális szolgáltatási koordinátoroknak is nagy szerepe lehet, mert saját tagállamuk tekintetében segíthetik ezen információk disszeminálását az adott állam közvélemény formálódási folyamataira tekintettel.

4. Az ex ante jellegű kötelezettségek rendszer szintű megközelítése

A kutatásban lefolytatott elemzés alapján az ex ante jellegű kötelezettségek ugyan a szabályozás hangsúlyos elemei, de nem tekinthetünk rá úgy, hogy az alapjogi védelem egyetlen formájára. Az ex ante kötelezettségek nem mindenhatóak, s bár a jogalkotó olyan szabályozást alkotott meg, amely alapján az az érzés keletkezhet az ezeket értelmezőben, hogy a szolgáltatónak a kockázatértékelés segítségével a rendszerszintű kockázatok kezelésén keresztül minden olyan sérelmet meg kellene tudnia szüntetni, ami felmerülhet a szolgáltatás nyújtásával összefüggésben, a gyakorlati eseteket is figyelve, ez nem fog bekövetkezni minden esetben. Az ex ante szabályozás, a kockázatértékelés és kockázatsökkentési intézkedésekkel, valamint más, a DSA-ban foglalt követelményekkel együtt, különösen azok megfelelő alkalmazása esetén, a felmerülő jogsértések kialakulásának kockázata akár nagyságrendekkel is csökkentheti, de emellett is fennmaradhatnak olyan helyzetek, amelyeket sem a kockázatértékelési tevékenység, sem a válságkezelési mechanizmusok nem lesznek képesek kezelni (pl. azért mert még senki számára nem nyilvánvaló, hogy egyáltalán olyan helyzet kialakulhata technológiai fejlődés útján), s amelyeket ex post megoldásokkal kell majd kezelni. Erre tekintettel az ex ante jellegű szabályozás egy fontos, de nem csak önmagában értelmezendő eleme a rendszerszintű kockázatok és jogsértések kezelésének.

- 5. Valós idejű átláthatósági megoldások:** Az éves jelentések mellett szabályozással, egységesített módszertani megoldásokkal ösztönözni kell a szolgáltatókat valós idejű vagy ahhoz közelítő tájékoztatási rendszerek bevezetésére, amelyek képesek lennének az egyedi szolgáltatási folyamatban is átfogó információkat nyújtani a felhasználóknak, annak érdekében, hogy valóban érdemi átláthatóság érzetük alakulhasson ki, s a szabályozás alapján is megvalósulhasson az átláthatóság materiális (azaz nem formális, pusztán dokumentumok közzétételében mért) megvalósítása. Ilyen megoldások

lehetnének a moderációs döntésekről és az alkalmazott algoritmusok változásairól szóló közérthető, akár automatikus formában elkészülő és megküldött értesítések.

Az ex ante szabályozás a fentiek alapján, bár nem tökéletes, de jelentős szabályozási lépés az online tér rendszerszintű kockázatainak kezelésére. A javasolt fejlesztések megvalósításával megítélésem szerint tovább erősíthető az alapjogok védelme és a digitális szolgáltatások szabályozásának hatékonysága.

Irodalomjegyzék

Leogrande ANGELO – Alberto COSTANTIELLO – Lucio LAURETI: The Broadband Penetration in Europe. *Journal of Applied Economic Sciences* 16(3), 2021.

Jens BRUNK – Jana MATTERN – Dennis M. RIEHLE: Effect of transparency and trust on acceptance of automatic online comment moderation systems. 2019 IEEE 21st Conference on Business Informatics (CBI) 1. IEEE, 2019.

Mauro CONTI, et al.: Revealing The Secret Power: How Algorithms Can Influence Content Visibility on Social Media. arXiv preprint arXiv:2410.17390, 2024.

Giovanni DE GREGORIO: From constitutional freedoms to the power of the platforms: protecting fundamental rights online in the algorithmic society. *European. Journal of Legal Studies* 11, 2018. 65.

Irakiza DIVIN DE BUFFALO: The charter of fundamental rights, the aims of EU competition law and data protection: Time to level the playing field. *Singapore Journal of Legal Studies*, 2021. 39-55.

Niklas EDER: Making systemic risk assessments work: how the DSA creates a virtuous loop to address the societal harms of content moderation. *German Law Journal* 2023. 1-22.

Michèle FINCK: Digital co-regulation: designing a supranational legal framework for the platform economy. *European law review* 2018/1.

Eleni FRANTZIOU: The horizontal effect of the charter of fundamental rights of the EU: rediscovering the reasons for horizontality." *European Law Journal* 21(5), 2015. 657-679.

Rob FRIEDEN, Rob: The internet of platforms and two-sided markets: Implications for competition and consumers. *Villanova Law Review* 63, 2018. 269.

GOSZTONYI Gergely: Az internetes tartalomszabályozással kapcsolatos új gondolkodási irányok az Amerikai Egyesült Államokban. *Miskolci Jogi Szemle* 16(4), 2021. 40-54.

GOSZTONYI Gergely – Ewa GALEWSKA – Andrej ŠKOLKAY: Challenges of Monitoring Obligations in the European Union's Digital Services Act. *Elte Law Journal* 12(1), 2024. 49-50. GÁRDOS-OROSZ Fruzsina – BEDŐ Renáta: Az alapvető jogok érvényesítése a magánjogi jogviták során. *Alkotmánybírósági szemle*, 2018/2., 3-10.

HOHMANN Balázs: A DSA és a DMA fogyasztóvédelmi irányai a békéltető testületi és hatósági jogalkalmazás tükrében. In: KOLTAY András – SZIKORA, Tamás – LAPSÁNSZKY András (szerk.): *A vadnyugat vége? Tanulmányok az Európai Unió platformszabályozásáról*. Budapest, ORAC Kiadó, 2024. 133-153.

Julie HOUILLON-LEONIS: Avenues for Future Transatlantic Transfers of Health Data: Is Less More?. *Global Privacy Law Review* 4(4), 2023.

KIS KELEMEN Bence – HOHMANN Balázs: A Schrems ítélet hatásai az európai uniós és magyar adattovábbítási gyakorlatokra. *Infokommunikáció és Jog* 13, 2016. 64-70.

KIS KELEMEN, Bence – HOHMANN Balázs: Is There Anything New Under the Sun? A Glance at the Digital Services Act and the Digital Markets Act from the Perspective of

Digitalisation in the EU Authors. Croatian Yearbook of European Law & Policy 19(1), 2023. 225-248.

KLEIN Tamás: A DSA alapjogvédelmi mechanizmusa mint alkotmányjogi nívó. In: KOLTAY András – SZIKORA, Tamás – LAPSÁNSZKY András (szerk.): A vadnyugat vége? Tanulmányok az Európai Unió platformszabályozásáról. Budapest, ORAC Kiadó, 2024. 275. (2024a)

KLEIN Tamás: Az újmédia szabályozásának új iránya? – A Digital Services Act alapjogvédelmi mechanizmusa. In TÖRÖK Bernát – ZÓDI Zsolt (szerk.): Digitalizálódó társadalom – Tanulmányok az új technológiák társadalmi-jogi hatásairól. Budapest, Ludovika Egyetemi Kiadó, 2023. 122-124.

KLEIN Tamás: Platform Regulation and the Protection of Fundamental Rights. Symbolon 25(2), 2024. 18-20.

KLEIN Tamás: Új terület a jogtudomány horizontján? Jogtudományi Közlöny, 2024/3. 134-140.

KOLTAY András: Az új média és a szólásszabadság. A nyilvánosság alkotmányos alapjainak újragondolása. Budapest, Wolters Kluwer, 405-440.

KOVÁCS Ildikó: Az európai Bíróság „taxiítéletei”: az uberPop és a star taxi App. Fontes Iuris 7(1), 2021. 39-50.

Stefan KULK – Frederik ZUIDERVEEN BORGESIOUS: Filtering for copyright enforcement in Europe after the Sabam cases. European Intellectual Property Review, Forthcoming, 2013.

Teodora LALOVA-SPINKS, et al.: EU-US data transfers: an enduring challenge for health research collaborations. Digital Medicine 7(1), 2024. 215.

Tobias LOCK: Rights and principles in the EU Charter of Fundamental Rights. Common Market Law Review 56(5), 2019.

NÁDORI Péter: Úton a tömeges internetes szólás jogi megítélésének új megközelítése felé: A strasbourgi Nagykamara ítélete a Delfi-ügyben. In Medias Res 8(2), 2019. 343-366.

PAPP János Tamás. A közösségi média platformok szabályozása a demokratikus nyilvánosság védelmében. Budapest, Wolters Kluwer, 2022. 16-50.

Sanjana PARIKH: Defining the Market for Two-Sided Platforms. Berkeley Technology Law Journal 34(4), 2019. 1305-1336.

Edouard PIGNOT: Who is pulling the strings in the platform economy? Accounting for the dark and unexpected sides of algorithmic control. Organization 30(1), 2023. 140-167.

João Pedro QUINTAIS – Naomi APPELMAN – Ronan Ó. FATHAIGH: Using terms and conditions to apply fundamental rights to content moderation. German Law Journal 24(5), 2023. 881-911.

Katarina Knol RADOJA: Freedom of Expression on the Internet-Case 18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited. Balkan Social Science Review 15(15), 2020. 7-25.

Hadi RHONDA – Shiri MELUMAD – Eric S. PARK: The Metaverse: A new digital frontier for consumer behavior. *Journal of Consumer Psychology* 34(1), 2024. 142-150.

Poplett RYAN: Is content moderation a concern that is best left to platforms?. *Ethica* 2, 2022. 73.

SUZOR, Nicolas P., et al.: What do we mean when we talk about transparency? Toward meaningful transparency in commercial content moderation. *International Journal of Communication* 13, 2019. 18.

TELEKI Lóránt, GÖNCZÖL Tünde: A digitális kapuőrök az ex ante szabályozás, a versenyjog és az adatvédelem kerettüzeiben. *Verseny és Szabályozás* 1, 2022. 243.

Heather TILLEWEIN – Keely MOHON-DOYLE – Destiny COX: A Critical Discourse Analysis of Sexual Violence Survivors and Censorship on the Social Media Platform TikTok. *Archives of Sexual Behavior* 2024. 1-10.

Giovanni TRICCO: The New Transatlantic Data Agreement Placed in Context: Decoding the Schrems Saga Within the Digital Economy. *Journal of Law, Market & Innovation* 3(1), 2024. 82-110.

TÖRÖK Bernát: A szólásszabadság a közösségi platformokon és a Digital Service Act. In TÖRÖK Bernát – ZÓDI Zsolt (szerk.): *Az internetes platformok kora*. Budapest, Ludovika, 2022. 195-200.

Sergey V. VOLODENKOV – Sergey Nikolaevich FEDORCHENKO – Julia ARTAMONOVA: Sociotechnical reality of the digital space of contemporary politics: structure and features. *Political Expertise*, 18(3), 2022. 230-232.

Tatjana JOVANIĆ: Platform Regulation: Ex Ante Tools and Strategies in the Regulatory Toolkit. In Dušan V. POPOVIĆ – Rainer KULMS: *Repositioning Platforms in Digital Market Law*. Cham, Springer Nature Switzerland, 2024. 1-34.

Peggy VALCKE – Aleksandra KUCZERAWY – Pieter-Jan OMBELET: Did the Romans get it right? What Delfi, Google, eBay, and UPC TeleKabel Wien have in common. *The responsibilities of online service providers* 2017. 101-116.

Xie WENJING – Kavita KARAN: Consumers' privacy concern and privacy protection on social network sites in the era of big data: Empirical evidence from college students. *Journal of Interactive Advertising* 19(3), 2019. 187-201.

Folkert WILMAN: The Digital Services Act (DSA) – An Overview. Available at SSRN 4304586 (2022).

Zhou, ZIHAN, et al.: A Review of Gaps between Web 4.0 and Web 3.0 Intelligent Network Infrastructure. 2023 IEEE 9th World Forum on Internet of Things (WF-IoT). IEEE, 2023.

ZÓDI Zsolt: Átláthatósági és indokolási követelmények az európai platformjogban. *In Medias Res* 12(2), 2023. 5-24.

Internetes hivatkozások listája

A hivatkozások ellenőrzési időpontja egységesen: 2024. november 30.

<https://digital-strategy.ec.europa.eu/en/news/digital-services-act-commission-designates-first-set-very-large-online-platforms-and-search-engines>

The Commission sends request for information to X under the Digital Services Act | Shaping Europe's digital future

<https://digital-strategy.ec.europa.eu/en/news/commission-requests-information-x-decreasing-content-moderation-resources-under-digital-services>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-tiktok-under-digital-services-act>

<https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-tiktok-under-digital-services-act>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-0>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-aliexpress-under-digital-services-act>

<https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-aliexpress-under-digital-services-act>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-tiktok-and-youtube-under-digital-services-act>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-meta-and-snap-under-digital-services-act>

<https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-meta-under-digital-services-act-related-protection>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-amazon-under-digital-services-act>

<https://digital-strategy.ec.europa.eu/en/news/commission-requests-information-amazon-under-digital-services-act>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-17-very-large-online-platforms-and-search-engines-under>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-1>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-linkedin-potentially-targeted-advertising-based-sensitive-data>

<https://digital-strategy.ec.europa.eu/en/news/statement-commissioner-breton-steps-announced-linkedin-comply-dsa-provisions-targeted-advertisement>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-linkedin-potentially-targeted-advertising-based-sensitive-data>

<https://digital-strategy.ec.europa.eu/en/news/commission-compels-microsoft-provide-information-under-digital-services-act-generative-ai-risks>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-tiktok-regarding-launch-tiktok-lite-france-and-spain>

<https://digital-strategy.ec.europa.eu/en/news/commission-opens-proceedings-against-tiktok-under-dsa-regarding-launch-tiktok-lite-france-and-spain>

<https://digital-strategy.ec.europa.eu/en/news/statement-commissioner-breton-announcement-tiktok-suspend-tiktok-lites-reward-programme-eu>

<https://digital-strategy.ec.europa.eu/en/news/tiktok-commits-permanently-withdraw-tiktok-lite-rewards-programme-eu-comply-digital-services-act>

<https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-facebook-and-instagram-under-digital-services-act>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-2>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-illegal-content-and-protection-minors-pornhub-xvideos-and>

<https://digital-strategy.ec.europa.eu/en/news/commission-requests-information-under-digital-services-act-pornhub-stripchat-and-xvideos-their>

<https://digital-strategy.ec.europa.eu/en/news/commission-requests-information-online-marketplaces-temu-and-shein-compliance-digital-services-act>

<https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-temu-under-digital-services-act>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-youtube-snapchat-and-tiktok-recommender-systems-under-digital>

<https://digital-strategy.ec.europa.eu/en/news/commission-sends-additional-request-information-tiktok-under-digital-services-act>

<https://digital-strategy.ec.europa.eu/en/news/commission-requests-information-under-digital-services-act-temu-traders-selling-illegal-products>

<https://digital-strategy.ec.europa.eu/en/news/commission-publishes-guidelines-under-dsa-mitigation-systemic-risks-online-elections>

<https://digital-strategy.ec.europa.eu/en/library/digital-services-act-study-risk-management-framework-online-disinformation-campaigns>

Felhasznált jogszabályok és döntések listája

A Bizottság (EU) 2016/1250 végrehajtási határozata (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről. C/2016/4176 HL L 207.

A Bizottság (EU) 2018/334 ajánlása (2018. március 1.) az illegális online tartalom hatékony kezelésére irányuló intézkedésekről C/2018/1177

A Bizottság határozata (2000. július 26.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott biztonságos kikötő adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről. HL L 215.

A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Európa digitális jövőjének megtervezése. COM/2020/67 final

A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az Európai Demokráciára vonatkozó cselekvési tervről COM/2020/790 final

Az Európai Parlament 2019. február 12-i állásfoglalása az Európai Unió Alapjogi Chartájának végrehajtásáról az Unió intézményi keretében (2017/2089(INI))

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

Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet) HL L 277.

Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól. HL L 178. (a továbbiakban: e-kereskedelmi irányelv)

Az Európai Unió Alapjogi Chartája. HL C 326., 26/10/2012

Az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata. HL C 326., 2012.10.26.

Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata. HL C 326., 2012.10.26.

Lisszaboni Szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról, HL C 306. 2007.12.17.

Az Európai Unió Bíróságának ítélete (nagytanács), 2015. október 6. Maximilian Schrems kontra Data Protection Commissioner. (C-362/14) ECLI:EU:C:2015:650

Az Európai Unió Bíróságának ítélete (nagytanács), 2020. július 16. - Data Protection Commissioner kontra Facebook Ireland Limited és Maximillian Schrems. (C-311/18) ECLI:EU:C:2020:559

Az Európai Unió Bíróságának ítélete (nagytanács), 2014. május 13. – Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González (C-131/12) ECLI:EU:C:2014:317

Az Európai Unió Bíróságának ítélete (harmadik tanács), 2019. október 3. Eva Glawischnig-Piesczek kontra Facebook Ireland Limited (C-18/18) ECLI:EU:C:2019:821

A Bíróság ítélete (második tanács), 2019. július 29. Fashion ID GmbH & Co.KG kontra Verbraucherzentrale NRW eV. (C-40/17) ECLI:EU:C:2019:629

Az Európai Unió Bíróságának ítélete (harmadik tanács), 2012. február 16. Belgische Vereniging van Auteurs, Componisten en Uitgevers (Sabam) kontra Netlog NV (C-360/14) ECLI:EU:C:2012:85

Az Európai Unió Bíróságának ítélete (negyedik tanács), 2014. március 27. UPC Telekabel Wien GmbH kontra Constantin Film Verleih GmbH és Wega Filmproduktionsgesellschaft mbH (C-314/12) ECLI:EU:C:2014:192

Az Európai Unió Bíróságának ítélete (nagytanács), 2017. december 20. Asociación Profesional Elite Taxi kontra Uber Systems Spain, SL. (C-434/15) ECLI:EU:C:2017:981

Az Európai Unió Bíróságának ítélete (nagytanács) 2019. december 19 X elleni büntetőeljárás (C-390/18) ECLI:EU:C:2019:1112

Delfi AS v. Észtország, 64569/09 ítélet, EJEB, 2013.

Magyar Tartalomszolgáltatók Egyesülete és Index.hu Zrt. v. Magyarország, 22947/13 ítélet, EJEB, 2016.

Zeran v. America Online (1997)

Blumenthal v. Drudge (1998)

Doe v. America Online (2001)

Doe v. MySpace (2008)

Jones v. Dirty World Entertainment Recordings LLC (2014)