Adatvédelem és platformok a DSA tükrében

Liber Ádám – Bereczki Tamás

Tartalomjegyzék

Az Európai Unió (EU) digitális stratégiája[1] az elmúlt években egyre inkább a digitális tér átalakítására és szabályozására összpontosít és célja, hogy biztosítsa a technológiai fejlődés, a gazdasági versenyképesség és az alapvető jogok közötti egyensúlyt. Az EU komoly hangsúlyt és erőforrásokat fektet ezen stratégia végrehajtására, hogy a digitális jogok és elvek között garantálja a tisztességes, védett, biztos és biztonságos digitális környezetet[2]. Ennek megfelelően az EU digitális stratégiája végrehajtásának középpontjában a digitális szolgáltatásokat nyújtó platformok állnak, amelyek az információs társadalom gerincét alkotják, és amelyek a gazdasági és társadalmi élet minden területére kiterjedő hatással bírnak.

Az európai uniós jogalkotó a digitális szolgáltatások területén az uniós adatvédelmi szabályozással, az EU általános adatvédelmi rendelete[3] és az elektronikus hírközlési adatvédelmi irányelv[4] szabályaival párhuzamosan célul tűzte ki továbbá az alapvető jogok digitális térben történő biztosítását és ezen online folyamatok szabályozását, hogy biztosítsa a felhasználói jogok védelmét és a digitális tér átláthatóságát. Az online platformok átláthatóságának és a felhasználói kontroll erősítésének szükségessége az EU jogalkotási munkájának egyik fő iránya lett az EU 2020-as digitális stratégiájának megfelelően. Az ezzel kapcsolatos új szabályozás, a Digitális Szolgáltatásokról szóló jogszabály (*Digital Services Act*, „*DSA*"[5]) központi szerepet játszik ebben a jogalkotási folyamatban.

A jelen tanulmány célja, hogy áttekintést nyújtson az Európai Unió platformok adatkezelésével kapcsolatos szabályozási törekvéseiről a DSA tükrében, különös tekintettel az online megfigyelésre, a profilozásra, tartalommoderálásra, automatizált döntéshozatalra és az alapvető jogok és a felhasználók, különösen a kiskorúak és gyermekek védelmére a DSA kapcsolódó jogintézményei és garanciái adatvédelmi vonatkozásaira.

1. A DIGITÁLIS PLATFORMOK ADATKEZELÉSÉNEK SZABÁLYOZÁSI KÉRDÉSEI

A digitális platformok által végzett *kiterjedt adatgyűjtés, a felhasználói tevékenységek követése, felhasználók tevékenységének és magatartásuk megfigyelése, célzott hirdetések alkalmazása és ezen adatok együttes, mélyreható elemzése, illetőleg* napjainkban már mesterséges intelligencia rendszerek tanítása céljából történő értékesítése[6] az adatvédelmi és adatbiztonsági kérdéseket az EU egyik legfontosabb szabályozási területévé tette. A felhasználók online tevékenységeinek nyomon követése és profilozása komoly kihívást jelent

[1] Európai Bizottság - Európa digitális jövőjének alakítása; lehívás: 2024.09.15

[2] Európai nyilatkozat a digitális évtizedben érvényre juttatandó digitális jogokról és elvekről; (2023/C 23/01); lehívás: 2024. 09. 15

[3] 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 irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet, „*GDPR*")); HL L 119, 2016.5.4., 1. o

[4] Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv, „*ePrivacy irányelv*"); HL L 201., 2002.7.31

[5] A DSA az Európai Parlament és a Tanács (EU) 2022/2065 rendelete, amely 2022. október 19-én került elfogadásra, a digitális szolgáltatások egységes piacának szabályozásáról szól; European Commission: Shaping Europe's digital future - The Digital Services Act package; letöltés: 2024.09.15

[6] vö. FTC conducting inquiry into Reddit's AI data-licensing practices ahead of IPO; 2024. március 21; lehívás: 2024.09.15

az egyének magánéletének védelme szempontjából. A személyes adatok hatalmas mennyisége, amelyet ezek a platformok kezelnek, lehetőséget biztosítanak nemcsak a gazdasági haszonszerzésre, hanem a felhasználók viselkedésének és preferenciáinak befolyásolására, illetve fogyasztókat károsító *visszaélésszerű gyakorlatokra*[7] is.

A kiterjedt adatgyűjtések további aggasztó vonzata az álhírek és *deepfake terjesztése, politikai manipuláció (fake news) és a választási folyamatok befolyásolása*, amelyet az Európai Adatvédelmi Biztos (EDPS) is hangsúlyozott különböző állásfoglalásaiban, így a 2018-as online manipulációról szóló véleményében[8]. Kutatások szerint a felhasználók, választók hírfolyamának vagy keresési eredményeinek manipulálása befolyásolhatja a szavazási viselkedésüket és „véleménybuborékokba" tereli őket[9]. Ez a jelenség különösen fontos a mai digitális korban, ahol a közösségi média és a keresőprogramok jelentős szerepet játszanak az információhoz való hozzáférésben és az emberek véleményének formálásában, ami torzíthatja a valóságról alkotott képüket és befolyásolhatja a politikai döntéseiket[10]. Az *online manipuláció* politikai kommunikációt illető veszélyeivel kapcsolatosan az Európai Adatvédelmi Biztos a vonatkozó véleményében[11] szintén utalt a helyi és nemzeti adatvédelmi hatóságokat, valamint nemzetközi szervezeteket tömörítő Global Privacy Assembly (GPA) 2005-ös határozatára[12] a személyes adatok politikai kommunikáció céljából történő felhasználásáról.

Ezen magatartások szabályozásban különleges szerepet játszik *a GDPR*, amely 2018. május 25. napja óta a személyes adatok kezelésére szigorú szabályozási keretet biztosít, amely elengedhetetlen a digitális gazdaság és az online platformok működésének átláthatósága és biztonsága szempontjából. Az EU digitális stratégiája azonban nem korlátozódik pusztán a digitális platformok szabályozására. Szélesebb kontextusban az EU digitális stratégiája a társadalom digitális átalakulásának irányítását tűzte ki célul, amely magában foglalja a mesterséges intelligencia (AI) szabályozását, a digitális infrastruktúra fejlesztését, valamint a digitális készségek és a digitális gazdaság előmozdítását a digitális reziliencia és kiberbiztonság erősítése mellett. Az Európai Unió digitális startégiájának részeként számos jogszabályt fogadott el, melyek adatvédelmi relevanciával rendelkeznek, ideértve a digitális

[7] Az amerikai egyesült államokbeli Federal Trade Commission 2024. szeptember 19. napján tette közzé a közösségi média és videó streaming szolgáltatások adatvédelmi gyakorlataival kapcsolatos jelentését. A jelentés számos olyan megállapítást tesz az érintett szolgáltatók adatvédelmi gyakorlatairól, melyek komoly adatvédelmi, fogyasztóvédelmi és versennyel kapcsolatos piaci kudarcokat jeleznek a felhasználók személyes adatai kezelésével kapcsolatosan, mivel a vizsgált vállalatok olyan káros gyakorlatokat folytatnak, melyek az adatvédelem rovására törekednek profitmaximalizálásra és a piaci verseny korlátozására. vö. Federal Trade Commission - A Look Behind the Screens Examining the Data Practices of Social Media and Video Streaming Services; An FTC Staff Report, September 2024; lehívás: 2024.09.19

[8] vö. EDPS Opinion 3/2018 EDPS Opinion on online manipulation and personal data; lehívás: 2024.09.19

[9] Véleménybuborék élőben: az emberek többsége alig kerül kapcsolatba más pártállásúakkal; Az online platformok hatása a demokratikus nyilvánosságra - Kutatási trendek és eredmények; lehívás: 2024.09.07

[10] Dipayan Ghosh, Ben Scott - Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You; Time.com; March 19, 2018; 2024.09.15

[11] Opinion 3/2018 - EDPS Opinion on online manipulation and personal data; p. 7-9.; lehívás: 2024.09.15

[12] Global Privacy Assembly - Montreux (Switzerland), 14th to 16th September 2005 , Resolution on the Use of Personal Data for Political Communication, lehívás: 2024.09.15

szolgáltatásokról szóló jogszabályt, a digitális piacokról szóló jogszabályt (DMA[13]), az adatkormányzási rendeletet (DGA[14]), az adatmegosztási rendeletet (Data Act[15]) és a mesterséges intelligencia rendeletet (AI Act[16]), melyek mindegyike személyes adatok kezelésével kapcsolatos relevanciával is rendelkezik.

Az EDPS már 2017-ben aggodalmát fejezte ki a digitális területen hozott olyan európai uniós jogszabályok elfogadásával kapcsolatban, amelyek *átfedésben vannak* az akkoriban nemrég elfogadott GDPR-ral. Az EDPS digitális tartalom nyújtásáról szóló szerződésekről szóló irányelv javaslatáról szóló véleményében[17] írta, hogy „*Az EU-nak kerülnie kell minden új javaslatot, amely felboríthatja az EU jogalkotója által gondosan kialakított egyensúlyt az adatvédelmi szabályok tekintetében. Az átfedő kezdeményezések akaratlanul is veszélyeztethetik a digitális egységes piac koherenciáját, ami szabályozási széttöredezettséghez és jogbizonytalansághoz vezethet.*"[18] Az EDPS ezért javasolta azt, hogy az Európai Unió a GDPR-t alkalmazza a személyes adatok digitális gazdaságban való felhasználásának szabályozására. Ezeket az érveket azonban az Európai Bizottság részéről nem vették következetesen figyelembe az európai uniós digitális jogalkotási folyamat során[19], ami emiatt potenciálisan jogbizonytalansághoz vezethet, ha ezen új digitális jogszabályok és a GDPR együttes alkalmazásából származó szabályozási átfedéseket vesszük figyelembe.

A DSA alkalmazása tekintetében ezért merül fel a kérdés, amely jelen tanulmánynak is tárgya, hogy miként kell alkalmazni az uniós adatvédelmi szabályokat a DSA tükrében és a DSA alkalmazása milyen hatással jár az érintett felhasználók adatvédelmi jogaira, illetőleg milyen következményei vannak szabályozási átfedéseknek, ideértve e szabályok kikényszerítését is.

2. AZ UNIÓS ADATVÉDELMI SZABÁLYOK ALKALMAZÁSA PLATFORMOKRA

A GDPR célja, hogy biztosítsa a személyes adatok védelmét, megerősítse az érintettek adatvédelmi jogait, biztosítva számukra a hozzáférést, a helyesbítést és a törlést, valamint az automatizált döntéshozatali folyamatokkal szembeni védelmet. Ezen felül a GDPR előírja, hogy

[13] Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály); HL L 265., 2022.10.12, p. 1–66.

[14] Az Európai Parlament és a Tanács 2022. május 30-i (EU) 2022/868 rendelete az európai adatkormányzásról és az (EU) 2018/1724 rendelet módosításáról (adatkormányzási rendelet); HL L 152., 2022.6.3, p. 1–44.

[15] Az Európai Parlament és a Tanács (EU) 2023/2854 Rendelete (2023. december 13.) a méltányos adathozzáférésre és -felhasználásra vonatkozó harmonizált szabályokról, valamint az (EU) 2017/2394 rendelet és az (EU) 2020/1828 irányelv módosításáról (adatrendelet); HL L, 2023/2854, 2023.12.22

[16] Az Európai Parlament és a Tanács 2024. június 13-i (EU) 2024/1689 rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet); HL L, 2024/1689, 2024.7.12

[17] EDPS Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 14 March 2017, p. 3.; lehívás: 2024.09.13

[18] EDPS Opinion 4/2017, im. p. 3.

[19] Gabriela Zanfir-Fortuna, Follow the (personal) data: Positioning data protection law as the cornerstone of EU's 'Fit for the Digital Age' legislative package; Working Paper – Forthcoming in EDPS At 20 Anniversary Volume, June 2024; p. 4.; lehívás: 2024.09.15,

az adatkezelők átlátható módon tájékoztassák a felhasználókat az adatgyűjtés és adatkezelés céljairól, továbbá biztosítsák a hozzájárulásuk megszerzését, különösen a profilalkotás és a célzott hirdetések esetében. Mindezeken keresztül a GDPR kulcsfontosságú eleme az EU digitális stratégiájának, amely a digitális innováció és gazdasági növekedés fenntarthatóságát kívánja támogatni.

A digitális platformok, mint a közösségi média szolgáltatók, keresőprogramok és e-online piactér szolgáltatók a digitális gazdaság meghatározó szereplőivé váltak és nagy tömegben kezelnek személyes adatokat, – azaz azonosított vagy azonosítható természetes személyre vonatkozó bármilyen információ[20] -, ami ezzel az üzleti modellel rendszeresen együtt jár. Az online platformok működésének adatvédelmi relevanciája abból fakad, hogy *központi szerepet játszanak a személyes adatok gyűjtésében, kezelésében és felhasználásában*, ami közvetlen hatással van az egyének magánéletére és a személyes adatok védelmére online tevékenységekkel kapcsolatosan. A GDPR ezzel összefüggésben szigorú szabályokat és alapelveket[21] határoz meg, amelyek célja, hogy biztosítsák a felhasználók személyes adatainak megfelelő kezelését, és átláthatóvá tegyék a platformok adatvédelmi gyakorlatait. A releváns adatvédelmi alapelveket a GDPR 5. cikke rögzíti és ide tartozik *a jogszerűség, tisztességes adatkezelés elve, az átláthatóság, a célhoz kötöttség, adatminimalizálás, pontosság, integritás és bizalmas kezelés, valamint az elszámoltathatóság alapelve* és alapvetően határozzák meg a platformok működését a személyes adatok kezelésével kapcsolatosan. A GDPR előírja, hogy bármely személyes adat kezelése tiszteletben tartsa ezeket az adatkezelési elveket, amely a DSA hatálya alatt is irányadó maradt.

A GDPR rendelkezéseit az online térben az *ePrivacy irányelv* rendelkezései pontosítják[22] és kiegészítik[23]. Az ePrivacy irányelv számos rendelkezése „*pontosítja*" a GDPR rendelkezéseit a személyes adatoknak az elektronikus hírközlési ágazatban történő kezelése tekintetében, illetőleg az ePrivacy irányelv olyan rendelkezéseket is tartalmaz, amelyek „*kiegészítik*" a GDPR rendelkezéseit a személyes adatoknak az elektronikus hírközlési ágazatban történő kezelése tekintetében.[24] Az ePrivacy irányelv számos rendelkezése például a nyilvánosan elérhető elektronikus hírközlési szolgáltatások „előfizetőinek" vagy „felhasználóinak" védelmét célozza. Egy nyilvánosan elérhető elektronikus hírközlési szolgáltatás előfizetői természetes vagy jogi személyek lehetnek. A GDPR kiegészítéseként az ePrivacy irányelv a természetes személyek alapvető jogainak – különösen a magánélet tiszteletben tartásához való joguknak – védelme mellett a jogi személyek jogos érdekeinek védelmét is szolgálja. Ezt meghaladóan a GDPR (173) preambulumbekezdés megerősíti, hogy amikor a személyes adatok kezelésére nem vonatkoznak az ePrivacy irányelvben meghatározott különös kötelezettségek, akkor a GDPR alkalmazandó. Az ePrivacy irányelv többek között különös szabályokat állapít meg az elektronikus (online) kommunikáció bizalmasságának és biztonságának védelmére, beleértve

[20] Személyes adat fogalmáról lásd részletesen a 29. cikk szerinti adatvédelmi munkacsoport személyes adat fogalmáról szóló véleményét 4/2007 szám alatt (WP 136); lehívás: 2024.09.15

[21] vö. GDPR 5. cikke (1)-(2) bekezdése

[22] Vö. 5/2019. számú vélemény az elektronikus hírközlési adatvédelmi irányelv és az általános adatvédelmi rendelet közötti kölcsönhatásról, különösen az adatvédelmi hatóságok illetékessége, feladatai és hatásköre tekintetében; 4.1 pont; Az elfogadás időpontja: 2019. március 12.; lehívás: 2024.09.09

[23] A 2002/58 irányelv 1. cikke a következőket írja elő: (2) Ennek az irányelvnek a rendelkezései az (1) bekezdésben említett célok érdekében pontosítják és kiegészítik a [95/46] irányelvet. […]"

[24] Vö. 5/2019. számú EDPB vélemény; 4.2 pont;

az elektronikus direkt marketing szabályozását. 2009 óta[25] az ePrivacy irányelv előírja, hogy minden olyan fél, aki információt tárol vagy fér hozzá egy személy digitális eszközén, például nyomkövető cookie-k használatával, meg kell szereznie ezen felhasználó hozzájárulását. Az ePrivacy irányelv és annak nemzeti átültető rendelkezéseinek célja, hogy megvédjék a végfelhasználókat az illetéktelen információtárolástól vagy hozzáféréstől a végberendezéseiken harmadik felek által, így az ilyen technológiákat alkalmazó platform szolgáltatóktól, mellyel a felhasználó adatvédelmi jogait biztosítják. Az ePrivacy irányelv felülvizsgálat alatt van, és az eredeti tervek szerint a GDPR-ral együtt fogadták volna el rendeleti formában[26], azonban arra ezzel kapcsolatos viták és lobbitevékenységek miatt a mai napig sem került sor[27].

Az uniós adatvédelmi szabályok, így a GDPR és az ePrivacy irányelv tagállami átültető rendelkezései alkalmazása szempontjából lényeges az „*adatkezelő*" meghatározása, amely az európai adatvédelmi jog központi fogalma és azt rögzíti, hogy ki felel a személyes adatok kezeléséért és az uniós adatvédelmi jogszabályok betartásáért. Az adatkezelő ugyanis az a személy vagy szervezet, aki vagy amely akár önállóan, vagy másokkal együtt meghatározza a személyes adatok kezelésének céljait és eszközeit és ennél fogva felelős a GDPR adatvédelmi rendelkezéseinek betartásáért.[28] Lényeges különbség, hogy a DSA a „közvetítő szolgáltatókra" telepít kötelezettségeket, amely nem mindig azonos az adatkezelővel.

Az online platformok, mint például a közösségi média szolgáltatók, az online piacterek, és a keresőprogramok, jelentős mennyiségű személyes adatot kezelnek. Ezek a platformok adatkezelők lehetnek akkor, amikor önállóan vagy a platform felhasználóval közösen határozzák meg a személyes adatok kezelésének céljait és eszközeit, például amikor felhasználói profilokat hoznak létre vagy személyre szabott hirdetéseket jelenítenek meg, illetőleg az online platformok adatfeldolgozók is lehetnek, ha egy másik fél nevében és utasításai szerint kezelik az adatokat. Az online platformok *egyre komplexebb adatkezelési folyamatokat végeznek*, amelyek *több szereplő közös részvételét* igénylik, mely esetben az adatvédelmi felelősség megosztásában és általánosan a GDPR követelményeinek való megfeleléssel kapcsolatos kérdések merültek fel. Az adatkezelői státusz meghatározása nem mindig egyértelmű, ha adatkezelési folyamatok bonyolultak és gyakran több szereplő vesz részt az adatkezelési folyamatokban. Az európai uniós jogalkotói cél, hogy a bonyolult adatkezelési, több szolgáltatót magában foglaló láncolati struktúrák és kiszervezések ne puhíthassák fel, illetve ne csökkenthessék az ilyen adatkezelésben részt vevők adatvédelmi kötelezettségeit, illetve az érintettek vevők elszámoltathatóságát, és az érintettek magas szintű védelmét. Magasabb kockázatot jelent az érintett jogaira és szabadságaira nézve, ha több szervezet vagy

[25] Lásd az Európai Parlament és a Tanács 2009/136/EK irányelve (2009. november 25.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról; OJ L 337, 18.12.2009, p. 11–36

[26] Proposal for an ePrivacy Regulation; https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation; lehívás: 2024.09.15

[27] Captured states – e-Privacy Regulation victim of a "lobby onslaught" By EDRi · May 23, 2019; lehívás: 2024.09.15

[28] Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), Datenschutzrecht. DSGVO mit BDSG (Nomos 2019), 1. Auflage; Artikel 4. Nr 7.; p. 329

személy, mint adatkezelők, illetve adatfeldolgozók láncolata vesz részt az adatkezelésben és ez a magasabb kockázati szint szigorúbb felelősségi elvárásokat indukál az adatkezelésben közreműködőkkel szemben.[29]

Az EU Bíróság gyakorlata online platformokkal kapcsolatosan *a közös adatkezelés fogalmának kiterjesztő értelmezése* mellett tört lándzsát, tehát az, hogy az online platformok esetében, amelyek többszereplős, összetett rendszereknek minősülnek, valamennyi szereplő – beleértve gyakran a felhasználókat is – felelősséggel tartozik az adatkezelési kötelezettségek betartásáért. "Közös adatkezelőnek" minősül, ha több személy közösen határozza meg, hogy miért és hogyan kell kezelni a személyes adatokat. A közös adatkezelőket egyetemleges felelősség terheli az érintettnek (például a felhasználóiknak) esetlegesen okozott károkért. A GDPR 26. cikk értelmében a közös adatkezelőknek megállapodást kell kötniük a fennálló felelősségeik, feladataik megoszlása tekintetében. E megállapodás lényegét közölni kell azon érintettekkel, akiknek személyes adatait kezelik. A német DSK közös adatkezelésről szóló iránymutatása szerint a közös adatkezelés esetei nem ritkán növelhetik az érintett személyek jogaira és szabadságaira vonatkozó kockázatokat, így adott esetben indokolt lehet az adatvédelmi hatásvizsgálat lefolytatása a GDPR 35. cikk alapján[30], ez azonban minden esetben egyedi mérlegelést igényel.[31]

A közös adatkezeléssel kapcsolatosan kiemelendő így az EU Bíróság a *C-210/16. sz. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein kontra Wirtschaftsakademie Schleswig-Holstein GmbH ügyében*[32], illetve a *C-40/17. sz. Fashion ID GmbH & Co KG ügyben*[33] hozott döntése. Ezen EU bírósági gyakorlatból az következik, amikor több fél, így egy online platform üzemeltetője és a platformon hirdető vállalat közösen határozza meg a személyes adatok kezelésének céljait és eszközeit, *közös adatkezelőkké válnak* a GDPR értelmében. Az olyan helyzetek, mint a közösségi médiaplatformok és azok üzleti felhasználói (például egy vállalkozás, amely egy közösségi médiaplatformon hirdet), együttműködését jelentik, gyakran közös adatkezelésnek minősülnek. Ez azt jelenti, hogy mindkét fél felelősséget visel az adatvédelmi előírások betartásáért, és kötelesek tisztázni egymás között az adatkezeléssel kapcsolatos kötelezettségeket összhangban a GDPR 26. cikk (1) bekezdésével. A közös adatkezelők kötelesek egyértelműen és átlátható módon tájékoztatni[34] az érintetteket (adatokat szolgáltató személyeket) arról, hogy kik a közös adatkezelők, és hogyan történik az adatok kezelése. A közös adatkezelőknek világos megállapodást kell kötniük arról, hogy ki milyen szerepet tölt be az adatkezelési folyamat során. Ennek a megállapodásnak tartalmaznia kell az érintettek jogainak biztosítását szolgáló intézkedéseket is. Az érintettek jogainak megsértése esetén a közös adatkezelők mindegyike felelősségre vonható lehet, függetlenül attól, hogy a jogsértést ténylegesen melyik fél követte el. Az online platformok esetében ez jelentős jogi kockázatot jelent, különösen akkor, ha nem

[29] vö. Liber Ádám - Bereczki Tamás: Közreműködők adatvédelmi jogállása; JK, 2019/12., 506-507.
[30] DSK, Kurzpapier Nr. 16 (Fn. 27), S. 4:; lehívás: 2024.09.16
[31] Der Bayerische Landesbeauftragte für den Datenschutz Gemeinsame Verantwortlichkeit Orientierungshilfe; Version 1.0 | Stand: 1. Juni 2024; lehívás: 2024.09.15
[32] Európai Unió Bírósága - C-210/16 sz., Wirtschaftsakademie Schleswig-Holstein kontra Facebook Ireland Ltd ügyben 2018. június 5-én hozott ítélet (ECLI:EU:C:2018:388).
[33] Európai Unió Bírósága, C-40/17. sz., Fashion ID kontra Facebook Ireland ügyben 2019. július 29-én hozott ítélet (ECLI:EU:C:2019:629).
[34] vö. GDPR 26. cikk (2) bekezdése

egyértelmű a felek közötti felelősség megosztása és megoszlása, ami az érintetti jogok sérelmével járhat.

Az európai uniós adatvédelmi szabályozás tehát a GDPR és az ePrivacy irányelv alkalmazásával szigorú szabályozási rezsimet rögzít a platformok adatkezelésével kapcsolatosan és ennek megfelelően szigorúbb elszámoltathatósági kötelezettségek vonatkoznak rájuk, melyet az EU Bíróság gyakorlata a közös adatkezelés tág értelmezésével terjesztett ki online platformok tevékenységére.

3. A DSA KAPCSOLATA AZ ADATVÉDELMI SZABÁLYOKKAL ÉS EGYÜTTES ALKALMAZÁSUK PLATFORMOKRA

A DSA célja, hogy az online platformok szabályozása alapvető jogokon alapuló megközelítést biztosítson, amelyben a személyes adatok védelme is központi szerepet játszik.[35] A DSA modernizálja az online közvetítők felelősségét, biztosítva, hogy az online platformok megfelelően kezeljék a felhasználói tartalmakat, átlátható adatkezelési gyakorlatokat folytassanak, és védjék a felhasználók jogait. A DSA kiterjed a felhasználói jogok megerősítésére, beleértve a tájékoztatáshoz, a tartalmak moderálásához és az adatkezelés átláthatóságához való jogokat.

A DSA az elektronikus kereskedelemről szóló 2000-es irányelvre[36] épít, amelynek egyik központi szerepét a „közvetítő szolgáltatók" (ISP) fogalma adja. A szabályozás finomította az ezen fogalom alá tartozó szolgáltatásokat, és hármas felosztást alkalmazott: (i) egyszerű továbbítás, (ii) gyorsítótárazás és (iii) tárhelyszolgáltatás. A DSA ezt a struktúrát megtartotta, de új alkategóriákat vezetett be, például az „online platformokat" és „online keresőprogramokat", valamint ezek szigorúbb felügyeletét, különösen az „online óriásplatformok" és a „nagyon népszerű keresőprogramok" esetében. A DSA hierarchikus rendszert alkalmaz, amely eltérő kötelezettségeket ír elő a közvetítő szolgáltatások különböző típusaira, és egyes speciális szabályok vonatkoznak például a tárhelyszolgáltatókra és az online platformokra. Ennek megfelelően ha egy szolgáltató egyidejűleg többféle szolgáltatást nyújt, akkor ezek a szolgáltatások részben vagy egészben a DSA hatálya alá tartozhatnak, illetőleg a különböző szolgáltatások eltérő DSA követelmények hatálya alá eshetnek.[37] A szolgáltatás besorolása függ a technikai funkcióktól, a vállalkozás méretétől, és a technológia változása esetén is módosulhat.[38] A DSA 3. cikkének i) pontja meghatározza az „online platformok" fogalmát, amelyek olyan tárhelyszolgáltatások, amelyek nemcsak információt tárolnak a felhasználók kérésére, hanem ezeket a nyilvánosság számára is terjesztik. Ide tartoznak például az online piacterek, alkalmazásboltok és közösségi hálózatok. Az ilyen platformok tevékenysége nem lehet egy másik szolgáltatás kisebb vagy kiegészítő eleme. Az információk „nyilvános terjesztése" azt jelenti, hogy azokat potenciálisan korlátlan számú személy számára teszik

[35] vö. DSA (3) preambulumbekezdése; vö. Domingos Soares Farinho - Personal Data Processing by Online Platforms and Search Engines: The Case of the EU Digital Services Act; p. 38.; lehívás: 2024.09.15.

[36] 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 („elektronikus kereskedelemről szóló irányelv"); HL L 178., 2000.7.17, p. 1–16

[37] Domingos Soares Farinho - im p. 39.

[38] vö. ACM DSA Guidelines - Due diligence obligations for intemediary services - Netherlands Authority for Consumers and Markets, Case no. ACM/24/190334 / Document no. ACM/UIT/623178; 28. - 30. pontok; lehívás; 2024.09.15

elérhetővé, és ez akkor is megvalósul, ha a hozzáférés regisztrációhoz kötött, de automatikus. A DSA szigorúbb kötelezettségeket ír elő az online platformokra és keresőprogramokra, de mikro- vagy kisvállalkozásokra nem terjednek ki ezek a szabályok, kivéve, ha a vállalkozás mérete növekszik. Az online platformok üzleti modellje jelentős mértékben a felhasználók által generált személyes adatok gyűjtésén, kezelésén és monetizálásán alapul, melyet a felhasználók egy szolgáltatás fejében nyújtanak[39]. Az adatokat a felhasználók szolgáltatják a platformok számára, amelyek aztán elérhetővé teszik azokat más felhasználók számára. Az „igénybe vevő" fogalma tág, magában foglalja mind az üzleti, mind a magáncélból szolgáltatásokat használó személyeket.

A DSA javaslatról szóló EDPS vélemény szerint *nincs eredendő konfliktus az adatvédelemhez való jog és a DSA célkitűzései között*, amelyek az innovatív, átlátható és biztonságos online környezet biztosítását szolgálják. Az adatvédelem és a magánélet védelme elengedhetetlen összetevői egy élénk digitális gazdaságnak, beleértve az online platformokat is. Az adatvédelem és a magánélet védelme szükséges ahhoz, hogy az egyének szabadon kifejezhessék magukat, szabadon hozzáférhessenek az információkhoz és kreatívak lehessenek. Az EDPS szerint az online biztonság és az online platformok elszámoltathatóságának biztosítására szolgáló mechanizmusok tovább erősíthetik az alapvető jogok hatékony élvezetét.[40]

A DSA, a GDPR és az e-Privacy irányelv közötti kapcsolat *kiegészítő jellegű*. Ez azt jelenti, hogy a DSA nem módosítja vagy rontja le az uniós adatvédelmi szabályok alkalmazását, hanem azokat kiegészíti és velük összhangban kell működnie. A DSA világosan rögzíti, hogy nem érinti a GDPR által meghatározott adatvédelmi normákat, és minden személyes adatokkal kapcsolatos kérdést továbbra is a GDPR szabályai szerint kell kezelni. Az e-Privacy irányelv specifikus adatvédelmi szabályokat tartalmaz az elektronikus kommunikációra vonatkozóan, és kiegészíti és pontosítja a GDPR szabályait ezen a területen. A DSA ezzel kapcsolatosan rugalmas keretet biztosít, és lehetőséget ad a tagállamoknak, hogy nemzeti szabályozásukat az uniós célokkal összhangban alakítsák ki. Ennek alapján tehát a DSA egy integrált és harmonizált megközelítést kínál a digitális szolgáltatások szabályozására az adatvédelem területén, biztosítva, hogy a személyes adatok védelme továbbra is kiemelt prioritás maradjon az online környezetben.

A DSA számos utalást rögzít személyes adatok kezelésére és a GDPR szabályaira. Ezek az utalások különböző témakörök köré csoportosíthatók, így a GDPR, ePrivacy irányelv és a DSA közötti kapcsolatra[41]; profilalkotásra és célzott hirdetésekre vonatkozó korlátozásokra[42];

[39] Az Európai Adatvédelmi Testület (EDPB) a 2/2019. számú iránymutatásában a személyes adatoknak az általános adatvédelmi rendelet 6. cikke (1) bekezdésének b) pontja szerinti kezeléséről kijelenti, hogy „az adatvédelem az Alapjogi Charta 8. cikkében biztosított alapvető jog, és figyelembe véve, hogy az általános adatvédelmi rendelet egyik fő célja, hogy az érintettek számára biztosítsa, hogy az őket érintő információkkal saját maguk rendelkezhessenek, a személyes adatok nem tekinthetők forgalomképes árucikkeknek. Még akkor is, ha az érintett hozzájárulhat a személyes adatok kezeléséhez, e megállapodás révén nem mondhatnak le alapvető jogaikról."; 56. sarokpont, 16. oldal;

[40] vö. EDPS vélemény 15. sarokpontja

[41] DSA (10) preambulumbekezdés, illetve a DSA 2. cikk (4) g) pontja

[42] DSA (68)-(69) preambulumbekezdés és DSA 26. cikk (3) bekezdése

kiskorúak védelmére vonatkozó rendelkezésekre[43]; adatokhoz való hozzáférés és kutatás[44]; kockázatértékelés és átláthatósági követelményekre VLOP és VLOSE üzemeltető szolgáltatóknál[45]; vagy bejelentési és cselekvési mechanizmusokra[46]. Ebből a szempontból lényeges, hogy ezen szabályok alkalmazása hogyan viszonyul az európai uniós adatvédelmi szabályokhoz és a DSA és annak alkalmazása hogyan egészíti az európai uniós adatvédelmi szabályokat, mellyel kapcsolatosan a jogszerű adatkezelés, felelősség, és egyes DSA szabályozásához tartozó egyes specifikus adatvédelmi kötelezettségek alkalmazását vizsgáljuk meg a továbbiakban.

4. A JOGSZERŰ ADATKEZELÉS SZEREPE A DSA HATÁLYA ALATT

A DSA elsődleges célja a *jogellenes tartalom, az átláthatóság, és a platformok felelősségének szabályozása*, nem közvetlenül az adatkezelési jogalapok meghatározása, melyet adatvédelmi alapelvként a GDPR 5. cikk (1) bekezdés a) pontja rögzít. Ennek ellenére a DSA-ban foglalt kötelezettségek befolyásolják, hogy a szolgáltatók milyen adatkezelési jogalapokat alkalmazhatnak, és a megfelelő jogalap alkalmazása során emiatt figyelembe kell venni a DSA követelményeit is[47]. A DSA a közvetítő szolgáltatók részére több esetben meghatározza az alkalmazandó adatvédelmi jogalapot és az adott jogalap (így például a hozzájárulás) alkalmazásának korlátait, illetőleg számos esetben határoz meg kötelező adatkezeléseket (vö. GDPR 6. cikk (1)(c) és (e) pont) online platformok részére, amelyek nem biztosítanak mérlegelést a személyes adatok kezelésével kapcsolatosan a szolgáltatók részére és amely egyben korlátozza az érintett adatvédelmi jogait és az érintett információs önrendelkezési jogát a DSA alkalmazása során.

4.1 A HOZZÁJÁRULÁS ALKALMAZÁSA A DSA HATÁLYA ALATT

A hozzájárulás, mint adatkezelési jogalap alkalmazásával összefüggésben a DSA különös figyelmet fordít a célzott hirdetések és profilalkotás kérdésére. E tekintetben a DSA kifejezetten hivatkozik a GDPR-ra, különösen a hozzájárulás követelményére a személyes adatok hirdetési célú kezelésével kapcsolatban. A DSA (68) preambulumbekezdés kimondja, hogy a hirdetésekkel kapcsolatos tájékoztatásra vonatkozó követelmények *nem érintik a GDPR releváns rendelkezéseit, beleértve a hozzájáruláshoz való jogot és az automatizált döntéshozatalra vonatkozó szabályokat*. Ez azt jelenti, hogy az online platformoknak biztosítaniuk kell, hogy a felhasználók hozzájárulását megszerezzék, mielőtt személyes adataikat célzott hirdetések céljára felhasználnák. Ez a hozzájárulásnak *önkéntesnek, konkrétnak, tájékozottnak és egyértelműen kinyilvánítottnak* kell lennie a GDPR szerint[48].

A DSA 26. cikk (3) bekezdése tiltja a különleges kategóriájú személyes adatok (mint például az egészségügyi adatok, politikai vagy a vallási meggyőződés) kezelését profilalkotáson alapuló

[43] DSA (71) preambulumbekezdés és DSA 28. cikk (1)–(4) bekezdései
[44] DSA (97) preambulumbekezdés és DSA 40. cikk
[45] DSA (81) preambulumbekezdés; (94) preambulumbekezdés; DSA 34. cikk (1) bekezdése
[46] DSA (52) preambulumbekezdés
[47] vö. Domingos Soares Farinho - im p. 43.
[48] vö. EDPB 5/2020 Iránymutatás az (EU) 2016/679 rendelet szerinti hozzájárulásról 1.1 verzió Elfogadás időpontja: 2020. május 4.

ún. targetált hirdetések céljára. A vonatkozó DSA szerinti tilalom általános, ami azt jelenti, hogy *a felhasználó kifejezett hozzájárulása alapján sem* kezelhetők különleges kategóriájú adatok profilalkotáson alapuló ún. targetált hirdetések céljára[49]. Ezt a tilalom általános és a jogalkotó a Crambrige Analytica ügy[50] és egyéb egészségügyi adatokkal való célzott hirdetésekkel kapcsolatos visszaélésszerű adatkezelési gyakorlatok[51] miatt vezette be. Ez a tilalom bármely különleges kategóriájú személyes adatra vonatkozik, azaz a származtatott adatokra („inferred data"[52]) is kiterjed, ha annak alapján különleges kategóriájú személyes adatokra lehet következtetni.

Kiskorúak esetében a DSA 28. cikk (2) bekezdése szintén korlátozza a hozzájárulás, mint jogalap alkalmazását, mivel az online platformot üzemeltető szolgáltatók nem jeleníthetnek meg a szolgáltatás igénybe vevőinek adatait felhasználó profilalkotáson alapuló (targetált) hirdetéseket interfészeiken (mint a weboldaluk), ha kellő bizonyossággal tudatában vannak annak, hogy a szolgáltatás igénybe vevője kiskorú. Ez a tilalom szintén abszolút, ami azt jelenti, hogy a szülő, illetve törvényes képviselő hozzájárulása alapján sem, illetőleg akkor sem célozhatók meg profilozáson alapuló hirdetésekkel a kiskorúak, ha a GDPR 8. cikke alapján egyébként ehhez hozzájárulást adhatnának, mivel a DSA általános tilalmat rögzít a személyes adatok ilyen kezelésére, ami azt jelenti, hogy a jogszabály tiltja és jogellenessé minősíti ezt a típusú adatkezelést, ha a szolgáltató kellő bizonyossággal tudatában vannak annak, hogy a szolgáltatás igénybe vevője kiskorú. A DSA 28. cikk (3) bekezdése az adatminimalizálás elvének megfelelően pedig egyértelművé teszi, hogy az e cikkben foglalt kötelezettségek teljesítése nem kötelezi az online platformot üzemeltető szolgáltatókat arra, hogy további személyes adatokat kezeljenek annak értékelésére, hogy a szolgáltatás igénybe vevője kiskorú-e.

A hozzájárulás önkéntességével kapcsolatosan különös jelentősége van a platform méretének, és gazdasági erejének, ami online óriásplatformok esetében különösen releváns. Az Európai Adatvédelmi Testület Európai Adatvédelmi Testület 2024. április 17. napján véleményt[53] fogadott el a személyes adatoknak az online óriásplatformok által alkalmazott „hozzájárulási vagy fizetési" modellek keretében viselkedésalapú hirdetések céljából történő kezeléséről, ami az adatkezeléshez adott hozzájárulás érvényességével foglalkozott. A testület szerint az ilyen online platformoknak valódi választási lehetőséget kell biztosítaniuk a felhasználók számára a „hozzájárulási vagy fizetési" modellek alkalmazásakor. A vélemény szerint a legtöbb esetben a felhasználók számára csak a hirdetésekhez való hozzájárulás és a díjfizetés közötti választás nem felel meg az érvényes hozzájárulás követelményeinek. Ennek megfelelően az online óriásplatformoknak alternatív megoldásokat kell biztosítaniuk, amelyek között ingyenes lehetőség is szerepel, amely nem tartalmaz viselkedésalapú reklámot. A hozzájárulás megszerzése nem mentesít a GDPR alapelveinek betartása alól, és a szükségesség, arányosság elveit is figyelembe kell venniük. A Testület figyelmeztet arra is, hogy a díjak nem kényszeríthetik az egyéneket a hozzájárulás megadására, és a döntések negatív

[49] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 26. Rn 45; p. 320

[50] vö. Az Európai Parlament 2018. október 25-i állásfoglalása a Facebook-felhasználók adatainak a Cambridge Analytica általi felhasználásáról és az adatvédelemre gyakorolt hatásokról (2018/2855(RSP)); lehívás: 2024.09.11

[51] EDRI - Panoptykon Foundation, Algorithms of trauma: New case study shows that Facebook doesn't give users real control over disturbing surveillance ads (6 October 2021); lehívás: 2024.09.10

[52] A provided, observed és inferred data megkülönböztetésről lásd: Article 29 Working Party Guidelines on the right to data portability Adopted on 13 December 2016; p. 8-9.

[53] EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms Adopted on 17 April 2024; lehívás: 2024.08.20

következményeit is mérlegelni kell, mint például a szolgáltatások elvesztésének kockázata, ami azt jelenti, hogy ezek a platformok lehetőségeit a GDPR hozzájárulással kapcsolatos rendelkezései is korlátozzák a DSA rájuk irányadó szigorúbb szabályozási rezsimje mellett.

4.2 Kötelező adatkezelések

A DSA számos jogi kötelezettségeket rögzíti személyes adatok kezelésére. Ezek a rendelkezések jogkorlátozást rögzítenek és szükségszerűen korlátozzák az érintettek jogait, figyelemmel arra, hogy beavatkozást jelentenek az egyén magánszférájába.

A jogellenes tartalommal szembeni fellépést előíró DSA 9. cikk alapján (A jogellenes tartalom elleni fellépésre vonatkozó végzések) az online szolgáltatóknak biztosítaniuk kell a jogellenes tartalmak eltávolítására vonatkozó végzések végrehajtását, annak továbbítását, továbbá tájékoztatni kell a szolgáltatás érintett igénybe vevőjét a kapott végzésről és annak végrehajtásáról, ami azt jelenti, hogy ennek kapcsán kötelező a vonatkozó személyes adatok kezelése is. A DSA 10. cikke hasonló rendelkezéseket rögzít az információszolgáltatási kötelezettségekkel kapcsolatosan (Információszolgáltatásra vonatkozó végzések), ami kötelezi a szolgáltatókat, hogy az egyéni igénybe vevőre vonatkozó konkrét tájékoztatást előíró végzéseket végrehajtsák és azokról tájékoztatást adjanak az igénybe vevő részére. A DSA 16. cikke a jogellenes tartalomra vonatkozó bejelentési és cselekvési mechanizmusokat szabályozza, amelyek keretében a szolgáltatóknak biztosítaniuk kell az ilyen tartalmak jelentésére szolgáló rendszereket, és megfelelő intézkedéseket kell hozniuk az ilyen jelentések kezelése érdekében, beleértve az érintett személyes adatok törlését vagy korlátozását, amennyiben ez szükséges. A DSA 17. cikke szerint a szolgáltatóknak indokolniuk kell a tartalmak eltávolítására vagy korlátozására vonatkozó döntéseiket, amely során az adatkezelési kötelezettségek is megjelennek, mivel a döntés alapját képező adatokra vonatkozó tájékoztatást is biztosítani kell az érintett felhasználóknak. A DSA 18. cikke szerint, ha a szolgáltatók bűncselekmény gyanúját észlelik, kötelesek ezt jelenteni az illetékes hatóságok részére. Ez az adatkezelési kötelezettség magában foglalja a bűncselekményre utaló személyes adatok gyűjtését és továbbítását a megfelelő hatóságok felé. A DSA 30–32. cikkei a kereskedők nyomonkövethetőségével kapcsolatos adatkezelési kötelezettségeket határozzák meg az online piacokon. A szolgáltatóknak kötelességük biztosítani, hogy a kereskedők személyes adatai megfelelően nyomon követhetők és tárolhatók legyenek a jogellenes kereskedelmi tevékenységek azonosítása érdekében. A 40. cikk alapján a Bizottságnak vizsgálati és végrehajtási hatáskörei vannak az online óriásplatformok (VLOP) és nagyon népszerű online keresőprogramok (VLOSE) felett, amelynek keretében ezek a platformok kötelesek együttműködni és szolgáltatni az ehhez szükséges adatokat, beleértve a személyes adatokat is, ha azokra a vizsgálat során szükség van, tovább ebbe a körbe tartozik a kutatóknak biztosított hozzáférés is.

Mindezek a rendelkezések kötelező adatkezelési műveleteket fogalmaznak meg, ami azt jelenti, hogy a személyes adatok kezelésével kapcsolatosan nincs mérlegelési lehetősége a közvetítő szolgáltatónak és szükségszerűen korlátozzák az érintett információs önrendelkezési jogát, azonban ezekkel kapcsolatosan be kell tartani a célhoz kötött adatkezelés követelményét, melyet a szolgáltatók nem kerülhetnek meg. A szolgáltatók adatkezelőként a GDPR alapján felelősek érte, hogy betartsák az adatok kezelésével kapcsolatos jogalap követelményeket, mikor a fent megjelölt adatkezeléseket végzik.

5. A FELELŐSSÉG KÉRDÉSE AZ ADATVÉDELMI SZABÁLYOZÁS ÉS A DSA HATÁLYA ALATT

Az online platformok felelőssége eltér attól függően, hogy az adatvédelmi szabályok (GDPR, e-Privacy irányelvet átültető nemzeti rendelkezések) megsértéséért vagy a DSA megsértéséért fennálló felelősségről van-e szó, illetve az online platform által elkövetett jogsértésről van szó, ami a platformok által végzett tevékenységekre vonatkozik vagy az online platform felhasználója által elkövetett jogsértésről van szó, mikor a felelősség a felhasználók tevékenységeihez vagy a feltöltött jogellenes tartalomhoz kapcsolódó felelősségre vonatkozik.

5.1 Adatvédelmi jogsértésért való felelősség

Az online platform felelős az adatvédelmi szabályok megsértéséért, mikor a platform saját maga kezeli az adatokat és adatkezelőként (vagy adatfeldolgozóként) jár el, és az általa végzett adatkezelési műveletek nem felelnek meg a GDPR rendelkezéseinek, így a platform nem tartja be az adatvédelmi alapelveket (GDPR 5. cikk, 24. cikk (1)-(2) bekezdés), az adatbiztonsági rendelkezéseket (GDPR 32. cikk), a beépített és alapértelemzett adatvédelem elvét (vö. GDPR. 25. cikk) vagy akár az érintetti jogokat (GDPR 12. cikk, 15-22. cikkek). Ennek megfelelően egy online platform adatkezelőként teljes mértékben felelős a személyes adatok kezelése során történő jogsértésekért. A GDPR 82. cikke szabályozza a kártérítéshez való jogot és a felelősség kérdését. Amennyiben az online platform a szolgáltatásait felhasználó személy közös adatkezelőként jár el, ebben az esetben az online platform és a szolgáltatásait felhasználó személy egyetemlegesen felelnek az okozott kárért.

Az Európai Bíróság a *Google Spain*[54] és a *Wirtschaftsakademie* ügyben döntött arról, hogy a keresőprogramok működtetői, illetőleg a közösségi média platformok adatkezelőnek minősülnek a személyes adatok védelmére vonatkozó szabályozás alapján. Mindkét esetben a Bíróság kiemelte, hogy az "adatkezelő" fogalmát tágan kell értelmezni. A Google Spain ügyben a keresőprogramok működtetője esetében a Bíróság megállapította, hogy *„a keresőprogram működtetője az, aki meghatározza e tevékenység – és ezáltal az általa ennek keretében végzett személyesadat-kezelés – céljait és módját, és akit ebből következően […] ezen adatkezelés szempontjából „adatkezelőnek" kell tekinteni*". A Bíróság rámutatott, hogy az "adatkezelő" fogalmának széles értelmezése szükséges ahhoz, hogy az érintettek hatékony és teljes védelmet kapjanak, és nem lehet kizárni a keresőprogram működtetőjét az adatkezelői felelősség alól csak azért, mert nem gyakorol közvetlen ellenőrzést a harmadik fél weboldalain közzétett személyes adatok felett. A közösségi média platformok esetében az Európai Bíróság a Wirtschaftschakademie ügyben egyértelműen megállapította, hogy ezek a platformok elsődlegesen meghatározzák az adatkezelés célját és eszközeit a felhasználók és a platformon található rajongói oldalak látogatóinak személyes adatai tekintetében, így ők is adatkezelőnek és ezáltal az adatkezelésért felelős személynek minősülnek és felelnek a személyes adatok kezelésével kapcsolatos kötelezettségek betartásáért, mellyel kapcsolatosan elszámoltathatósági követelmények állnak fenn.

5.2 Szolgáltatók felelőssége és mentesülése

[54] A Bíróság ítélete (nagytanács), 2014. május 13. Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González. Az Audiencia Nacional (Spanyolország) által benyújtott előzetes döntéshozatal iránti kérelem. C-131/12. sz. ügy.

A közvetítő szolgáltatóként eljáró platformok általában automatikus adatkezelés útján kezelnek különböző tartalmakat és adatokat, melyeket nem maguk, hanem harmadik személyek szolgáltatnak. Amennyiben ezen tartalmak jogsértőek, az információ, illetve a tartalom szolgáltatója közvetlenül felel a jogsértés elkövetéséért, melyet Magyarországon az Elkertv. 7. § (1) bekezdése rögzít. Eszerint a szolgáltató felel az általa rendelkezésre bocsátott, jogszabályba ütköző tartalmú információért, amely felelősség az adatvédelmi jogszabályokat sértő jogellenes tartalmakra is kiterjed, melyet a szolgáltatást igénybe vevő felhasználók, kereskedők bocsátanak rendelkezésre. Ezzel kapcsolatosan lényeges a DSA hatályával kapcsolatos 2. cikk (2) bekezdése, ami azt rögzíti, hogy a DSA nem alkalmazandó az olyan szolgáltatásokra, amelyek nem közvetítő szolgáltatások, illetve az ilyen szolgáltatások tekintetében meghatározott követelményekre, függetlenül attól, hogy a szolgáltatás nyújtására közvetítő szolgáltatáson keresztül kerül-e sor.

A tartalomszolgáltatók, felhasználók online környezetben jellemzően valamely közvetítő szolgáltató eszközeinek felhasználásával valósítanak meg jogsértést, amelynek megtörténtéről a közvetítő szolgáltató a szolgáltatás műszaki jellemzőiből adódóan általában nem rendelkezik tudomással. A közvetítő szolgáltatók jogsértésért való felelősség alóli mentesülését – horizontális jelleggel – korábban az elektronikus kereskedelemről szóló irányelv, illetve a DSA alkalmazandóvá válása óta a DSA 4–6. cikke határozza meg[55]. A közvetítő szolgáltatók, akik automatikus adatkezelést végeznek harmadik féltől származó tartalmak révén, jogsértés esetén tehát *a tartalom szolgáltatóját* terheli a felelősség. Magyarországon az Elkertv. 7. § (1) bekezdése szerint a szolgáltató felelős a jogszabályba ütköző információkért, beleértve az adatvédelmi jogszabályokat sértő tartalmakat is. A közvetítő szolgáltatók általában nem tudnak a jogsértésekről. A felelősség kérdését, tehát azt, hogy a tartalomszolgáltató jogsértéséért a közvetítő szolgáltató egyáltalán felel-e, illetve felelőssége esetén ez közvetlen formában, járulékosan vagy más konstrukció alapján áll fenn – ideértve a polgári jogi, közigazgatási jogi és büntetőjogi felelősség kérdését – az egyes európai uniós tagállami jogok határozzák meg[56].

A DSA alkalmazása az információs társadalom szolgáltatásaira korlátozódik, amely megkülönbözteti a közvetítő szolgáltatásokat, így az egyszerű továbbítást, gyorsítótárazást és tárhelyszolgáltatást. A DSA lehetővé teszi a közvetítő szolgáltatók számára, hogy mentesüljenek a felhasználók által elkövetett jogsértésekért való felelősség alól, ideértve az adatvédelmi jellegű jogsértéseket is, amennyiben nem rendelkeznek tudomással a jogellenes tartalomról. A szolgáltatók tevékenysége tehát szigorúan *automatikus, technikai* és *passzív* kell, hogy maradjon, mely esetben nem vonhatók felelősségre, ha nincs tudomások a rendszereik útján elkövetett jogsértésről. Gyorsítótárazást, tárhelyszolgáltatást és online keresőprogram-szolgáltatás esetén továbbá annak van jelentősége, hogy a szolgáltató tudomást szerzett-e a jogellenes tartalomról és ezt követően haladéktalanul eltávolította, illetőleg hozzáférhetetlenné tette-e a jogellenes tartalmat[57]. A mentesülés mindazonáltal nem alkalmazandó, ha pusztán technikai és automatikus kezelésével megvalósuló semleges

[55] A DSA 89. cikk (1) bekezdése hatályon kívül helyezte az elektronikus kereskedelemről szóló irányelv 12-15. cikkeit, amit ezt a kérdést szabályozta.
[56] vö. Müller-Terpitz / Köhler: Digital Services Act: DSA - Gesetz über digitale Dienste; Kommentar; 2024; XXVII, 860 S. C.H.BECK. 60. o., 25. sarokpont
[57] vö. DSA 5. cikk (1) bek. e) és 6. cikk (1) bek. b) pontot, illetőleg Elkertv. 7. § (3) b) pontot

szolgáltatásnyújtás helyett – a közvetítő szolgáltató olyan aktív szerepet játszik, amely révén tudomást szerez az említett információkról vagy ellenőrzi azokat.[58]

Bár a közvetítő szolgáltató mentesülhet a felelősség alól, ennek ellenére követelhető tőle a jogsértés megelőzése vagy megszüntetése[59]. Ugyanakkor összhangban a DSA 8. cikkével általános nyomon követési kötelezettség nem írható elő számára, tehát nem kötelezhető arra, hogy általános felügyeletet gyakoroljon a rendszerein továbbított tartalmak felett és ezzel kapcsolatosan valamennyi felhasználó tevőleges nyomon követése keretében személyes adatok kezelését végezze. Az Elkertv. 7. § (5) bekezdése külön is szabályozza, hogy a közvetítő szolgáltatónak a DSA rendelet 4–6. cikk alapján történő mentesülése nem zárja ki azt, hogy az a személy, akit a jogellenes tartalmú információ révén sérelem ért, a jogsértésből fakadó igényei közül a jogsértés megelőzésére vagy abbahagyására irányuló követeléseit a jogsértő fél mellett a közvetítő szolgáltatóval szemben is bíróság útján érvényesítse.

5.3 Kellő gondossági követelmények megsértéséért való felelősség

A platformok felelősek azokért a cselekményekért, melyek a GDPR adatkezelőként (vagy adatfeldolgozóként) történő megsértéséből fakadnak. Egy olyan terület létezik azonban, ahol a GDPR és a DSA szerinti felelősség átfedésben[60] lehet, mégpedig akkor, ha az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók nem tesznek eleget a DSA-ban előírt ún. kellő gondossági kötelezettségeiknek a személyes adatok védelme tekintetében.

A DSA 34. cikke előírja, hogy az online óriásplatformoknak és népszerű keresőprogramoknak alaposan fel kell mérniük a szolgáltatásaik és rendszereik – beleértve az algoritmikus rendszereket – által generált rendszerszintű kockázatokat, különös figyelmet fordítva a személyes adatok védelmére. A DSA 35. cikke szerint a kockázatértékelés alapján a szolgáltatóknak arányos és hatékony kockázatcsökkentési intézkedéseket kell bevezetniük. Ha e szolgáltatók nem végzik el a szükséges kockázatértékelést vagy nem hajtanak végre megfelelő intézkedéseket, akkor a GDPR elszámoltathatósági követelményeit is megsérthetik, így a DSA és a GDPR közötti felelősség átfedésben állhat.[61] Ez a gyakorlatban és adatvédelmi szempontból azzal a kötelezettséggel jár, hogy az érintett szolgáltatóknak az ajánlórendszereiket, online hirdetéseiket, általános szerződési feltételeiket, adatkezelési gyakorlataikat (adatok felhasználását, adatok forrását, adatokkal való tanítást, címkézést) a szigorúbb elszámoltathatósági követelményekkel összhangban már tervezési szinten is úgy kell kialakítani, hogy az az azonosított szisztematikus kockázatokkal összhangban álljon, figyelemmel a belső és külső körülményekre, felhasználók magatartására is[62], mely kockázatkátokat a DSA 35. cikkében foglaltaknak megfelelően kell csökkenteni, melyhez a GDPR 35. cikke szerinti adatvédelmi hatásvizsgálatnak[63] és adott esetben 36. cikk szerinti

[58] lásd DSA (18) preambulumbekezdését
[59] vö. DSA rendelet 4. cikk (3) bekezdése; 5. cikk (2) bekezdése, 6. cikk (4) bekezdése
[60] vö. Domingos Soares Farinho - im p. 44.
[61] vö. Domingos Soares Farinho - im p. 44.
[62] vö. Müller-Terpitz / Köhler: Digital Services Act: DSA - Gesetz über digitale Dienste; Kommentar; 2024; XXVII, 860 S. C.H.BECK. Artikel 34, 403. o., 27-28. sarokpontok
[63] vö. Müller-Terpitz / Köhler: Digital Services Act: DSA - Gesetz über digitale Dienste; Kommentar; 2024; XXVII, 860 S. C.H.BECK. Artikel 35, 410. o., 5. sarokpontok

előzetes konzultációnak kell párosulnia, ha az azonosított magas kockázatok nem csökkenthetők elfogadható szintre.

6. PLATFORMOK SPECIFIKUS ADATVÉDELMI KÖTELEZETTSÉGEI A DSA HATÁLYA ALATT

A DSA számos specifikus adatvédelmi kötelezettséget rögzít platformok számára, amely személyes adatok kezelésével jár vagy ezzel kapcsolatos kötelezettséget rögzít és ez kiterjed a jogellenes tartalom kezelésére, tartalommoderálásra, ezzel kapcsolatos transzparencia kötelezettségekre, bejelentési és cselekvési mechanizmusokra, online interfész tervezéssel kapcsolatos követelményekre, melyekkel kapcsolatosan a DSA-ban több hivatkozás található az adatvédelmi szabályokra és azok fogalmaira.

6.1 Jogellenes tartalom kezelése és tartalommoderálás

A DSA szabályozza a jogellenes tartalom kezelését, a tartalommoderálás feltételeit és tisztázza a szolgáltatók általános monitorozási és aktív tényfeltárási kötelezettségeinek hiányát, illetőleg az önkéntes, saját kezdeményezésű vizsgálatok lehetőségét, amelynek lehetősége szorosan összefügg a szolgáltatók felelősségével és felelősség alóli mentesüléssel, melyet az előző bekezdésben tárgyaltunk. Figyelemmel arra, hogy ezek a tevékenységek felhasználói személyes adatok kezelésével járnak, azoknak közvetlen adatvédelmi implikációjuk van és bizonyos mérlegelést igényel a közvetítő szolgáltatók részéről.

6.1.1 A „jogellenes tartalom" és a „tartalommoderálás" fogalma

A DSA 3. cikk h) pontja értelmében „*jogellenes tartalom*" bármely olyan információ, amely önmagában vagy egy tevékenységgel kapcsolatban, beleértve a termékek értékesítését vagy a szolgálatások nyújtását, nem felel meg az uniós jognak vagy bármely tagállam – az uniós joggal összhangban álló – jogának, függetlenül az adott jog pontos tárgyától vagy jellegétől. A jogellenes tartalom a DSA számos rendelkezésének, így a felelősség alóli mentesülés és a DSA 9, 16. és 23. cikkek központi fogalma. A DSA 12. preambulumbekezdés rávilágít arra, hogy ezt a fogalmat tágan és úgy kell értelmezni, hogy az – formájától függetlenül – olyan információkra utal, amelyek az alkalmazandó jog értelmében vagy önmagukban is jogellenesek, melybe beleértendők a gyermekek szexuális bántalmazását ábrázoló képek megosztása, az adatvédelmi jogot sértő információk, mint például a magánjellegű képek jogellenes, hozzájárulás nélküli megosztása, az online követéses zaklatás, a nem megfelelő vagy hamisított termékek értékesítése, a fogyasztóvédelmi jogszabályokba ütköző termékek értékesítése vagy ilyen szolgáltatások nyújtása, a szerzői jogi védelemben részesülő anyagok engedély nélküli felhasználása, a szálláshely-szolgáltatások jogellenes kínálata vagy az élő állatok jogellenes értékesítése. Itt rögzítendő, hogy az Európai Bíróság a gyakorlatában a jogellenes tartalom fogalmát dinamikusan értelmezi, figyelemmel arra, hogy a *Glawischnig-Piesczek v. Facebook Ireland Limited* (C-18/18)[64] ügyben a blokkolási rendelkezések alkalmazási körét kiterjesztette az értelmileg azonos, hasonló tartalmakra is.

A DSA 3. cikk t) pontja meghatározza a „*tartalommoderálás*" fogalmát. Ez a közvetítő szolgáltató olyan automatizált vagy nem automatizált tevékenysége, amely különösen a

[64] Európai Unió Bírósága, 2019. október-3-i Eva Glawischnig-Piesczek kontra Facebook Ireland Limited-ítélet C 18/18, EU:C:2019:821

szolgáltatás igénybe vevője által közzétett *jogellenes tartalom* vagy *a közvetítő szolgáltató szerződési feltételeivel összeegyeztethetetlen információ* észlelésére, azonosítására és kezelésére szolgál, ideértve az ilyen jogellenes tartalom vagy információ elérhetőségét, láthatóságát és hozzáférhetőségét érintő intézkedéseket, például annak hátrasorolását, a demonetizálását, az ahhoz való hozzáférés megszüntetését vagy annak eltávolítását, vagy a szolgáltatás igénybe vevője általi információközlés lehetőségét érintő intézkedéseket, például a fiókja megszüntetését vagy felfüggesztését.

A tartalommoderálás szükségszerűen személyes adatok kezelésével jár, és a DSA szigorú transzparencia szabályok hatálya alá tereli ezt a tevékenységet, mivel a DSA 14-15. cikkei szerint a tartalommoderálás céljából alkalmazott valamennyi szabályra, eljárásra, intézkedésre és eszközre – beleértve az algoritmikus döntéshozatalt és az emberi felülvizsgálatot –, valamint a belső panaszkezelési rendszerük eljárási szabályzatára vonatkozó információt valamennyi közvetítő szolgáltató szerződési feltételeikben *transzparens tájékoztatást* kell nyújtani, mely kötelezettségek a GDPR transzparencia kötelezettségei mellett élnek.

Ezt meghaladóan VLOP és VLOSE szolgáltatóknak kockázatkezelés és kockázatcsökkentés részeként is kezelniük kell a tartalommoderálásukat (vö. DSA 35-36. cikkek), különösen „*a tartalommoderálási eljárások módosítása, beleértve a jogellenes tartalmak konkrét típusaira vonatkozó bejelentések feldolgozásának gyorsaságát és minőségét, valamint adott esetben a bejelentett tartalom mielőbbi eltávolítását vagy hozzáférhetetlenné tételét – különösen a jogellenes gyűlöletbeszéd vagy az online erőszak esetében –, továbbá a releváns döntéshozatali eljárások és a tartalommoderálásra szánt források módosítása*” tekintetében ha, a magán- és a családi élet tiszteletben tartásához való alapvető jogra, a Charta 8. cikkében foglalt, a személyes adatok védelméhez való alapvető jogra, a Charta 11. cikkében foglalt, a véleménynyilvánítás és a tájékozódás szabadságához való alapvető jogra vonatkozó kockázat merül fel a tartalommoderálás alkalmazásával kapcsolatosan.

A tartalommoderálás a GDPR, valamint az adatvédelem szempontjából vizsgálva, éppúgy a felhasználók alapvető jogainak védelmét szolgáló tevékenység más felhasználókkal és hatóságokkal szemben, mint ahogy eszköz arra, hogy a felhasználókat magától a platformtól is megvédje.[65] A tartalommoderálás magában foglalja a jogellenes tartalmak azonosítását, ezzel kapcsolatos felhasználói, megbízható bejelentői és hatósági értesítések kezelését, illetőleg ennek alapján megtett moderálási intézkedéseket, melyek ezzel személyes adatok kezelését foglalja magában és amellyel kapcsolatosan a közvetítő szolgáltatónak mérlegelnie kell a személyes adatok kezelésének jogszerűségét és a kapcsolódó automatizált eszközök igénybe vételének korlátait, és biztosítania kell az emberi felülvizsgálat kötelező biztosítását ennek igénybe vétele esetén. Ezek a tartalommoderációs tevékenységek személyes adatok kezelésével járó tevékenységek jogkorlátozást valósítanak meg az érintett viszonylatában, ezért a DSA ún. alapjogi teszt hatálya alá rendeli ezek alkalmazását.

6.1.2 Általános nyomon követés és egyéb proaktív intézkedések előírásának tilalma

A DSA szerint a közvetítő szolgáltatókat, kötelesek bizonyos lépéseket tenni a jogellenes tartalmak kezelésére, illetőleg a DSA kifejezetten kimondja, hogy az online platformok és

[65] vö. Domingos Soares Farinho - im p. 46.

közvetítő szolgáltatók *nem kötelesek általános jellegű monitorozást végezni vagy aktívan, az adott platformon jogellenes tevékenységeket felkutatni*. Ezen szabályoknak jelentős adatvédelmi relevanciája van, különösen a GDPR alkalmazása szempontjából, mivel szükségszerűen személyes adatok kezelésével jár a jogellenes tartalmak kezelése, illetve a tartalmak ezzel kapcsolatos moderálása. A szabályozás célja, hogy kiegyensúlyozza a jogellenes tartalom elleni fellépést és a felhasználók adatvédelmi jogainak tiszteletben tartását, különösen a GDPR elveivel összhangban. A DSA szerint tehát nem állapítható meg olyan általános kötelezettség, hogy a szolgáltatóknak az egyszerű továbbítás, gyorsítótárolás és tárhelyszolgáltatás nyújtása során a szolgáltatás tárgyát képező információkat nyomon kellene követniük. Ezt meghaladóan általánosan nem kötelezhetőek arra sem e szolgáltatók, hogy jogellenes tevékenységre utaló tényeket vagy körülményeket keressenek. Az általános monitorozási és aktív tényfeltárási kötelezettségek hiánya hozzájárul az adatkezelés minimalizáláshoz, a felhasználói jogok védelméhez, és biztosítja az adatvédelmi követelmények betartását a közvetítő szolgáltatók számára.

Az elektronikus kereskedelemről szóló irányelv közvetítő szolgáltatók felelősségéről szóló szabályozásának gyakorlati alkalmazása számos, az Európai Unió Bírósága előtti ügy tárgyát képezte. Ezen ügyekben a bíróságnak újszerű üzleti/reklámozási modellek alkalmazásáról – mint a Google AdWords szolgáltatása –, online piacterek felelősségéről, az általános nyomonkövetési kötelezettség, illetve szűrő- és blokkolórendszerek alkalmazásának határairól kellett állást foglalnia[66], melynek központi elemét képezte az ilyen intézkedések felhasználói személyes adatok védelmével való összeegyeztethetősége és ezen jogok alapjogi teszt keretében való összemérése a jogosultak polgári jogi igényeivel.

Az általános nyomonkövetési kötelezettség közvetítő szolgáltatókra irányadó tilalma az elektronikus kereskedelemről szóló irányelv 15. cikkén alapul, és a DSA 8. cikke ezt a rendelkezést gyakorlatilag változatlanul átvette. A tilalom fő oka, hogy egy általános szűrőrendszer bevezetése internetes cenzúrát eredményezne, és aránytalanul sértené a felhasználók magánélethez, adatvédelemhez fűződő jogait és technikailag is nehezen lenne kivitelezhető. A tilalom azonban nem vonatkozik specifikus nyomonkövetési kötelezettségekre, amelyeket bírósági vagy közigazgatási határozatok rendelhetnek el konkrét jogsértések megszüntetése vagy megelőzése érdekében.[67]

Az Európai Unió Bírósága több ügyben is foglalkozott a *szűrő- és blokkolórendszerek jogszerűségével,* például a L'Oréal v. eBay és a SABAM vs. Scarlet ügyekben. A Bíróság kimondta, hogy a közvetítő szolgáltatók nem kötelezhetők általános nyomonkövetésre, mert ez aránytalan intézkedés lenne, és sértené a vállalkozások szabadságát, valamint a felhasználók személyes adatainak és szólásszabadságának védelmét. A szűrőrendszerek kötelezővé tétele a

[66] Lásd különösen C-236-38/08 „Google v. Louis Vuitton, v. Viaticum & Luteciel & v. CNRRH, PierreAlexis Thonet, Bruno Raboin & Tiger"; C-237/08 „BDV"; C-238/08 „Eurochallenges"; C-558/08 „PORTAKABIN"; C-278/08 „BergSpechte"; C-91/09 „Bananabay"; C-323/09 „Interflora"; C-324/09 „L'Oréal v. eBay"; C-70/10. „SABAM v. Scarlet"; C-360/10 „SABAM v. Netlog" - lásd erről részletesen: Liber Ádám - Közvetítő szolgáltatók felelőssége szellemi tulajdon megsértéséért az Európai Unióban, in Iparjogvédelmi és Szerzői Jogi Szemle, 2013. június, pp. 5-42.; lehívás: 2024.09.15.

[67] Az elektronikus kereskedelemről szóló irányelv vonatkozó rendelkezésének értelmezésével és az általános, illetve egyedi megelőzésre vonatkozó kötelezettségek elhatárolásával az Európai Unió Bírósága a C-70/10. sz. SABAM vs. Scarlet, illetve a C-360/10. sz., SABAM vs. Netlog-ügyben foglalkozott.

felhasználók által tárolt fájlok és az összes adattevékenység folyamatos megfigyelését eredményezné, amely aránytalan beavatkozást jelentene az alapvető jogokba és ezért nem megengedett.

A személyes adatok védelme és a szellemitulajdon-jogok érvényesítése között az Európai Bíróság esetjoga szerint igazságos és méltányos egyensúlyt találni, amint azt a Promusicae[68] és Bonnier[69] ügyek is példázzák. Az uniós szabályozás lehetővé teszi a személyes adatok kiadását jogérvényesítési célokra, de ezt mindig *arányos módon* kell megtenni, *figyelembe véve a magánélet védelmét és más alapvető jogokat*. Az adatvédelmi jogszabályok, például az ePrivacy irányelv, szigorú feltételeket szabnak a személyes adatok kezelésére, különösen akkor, ha az a felhasználók magánéletéhez és adatvédelméhez fűződő jogokba ütközik.

6.1.3 Önkéntes vizsgálatok és jogi megfelelés lehetősége

Az önkéntes, saját kezdeményezésű vizsgálatok lehetőségét a DSA 7. cikke szabályozza és ez a rendelkezés azt rögzíti, hogy a közvetítő szolgáltatóktól nem tagadható meg a DSA 4., 5. és 6. cikkben említett, felelősség alóli mentesülés kizárólag azon az alapon, hogy jóhiszeműen és kellő gondossággal eljárva önkéntes, saját kezdeményezésű vizsgálatokat vagy egyéb, a jogellenes tartalom észlelésére, azonosítására és eltávolítására, illetve az ahhoz való hozzáférés megszüntetésére irányuló intézkedéseket hoznak, vagy az uniós jog és az uniós joggal összhangban álló nemzeti jog követelményeivel való megfeleléshez szükséges intézkedéseket hoznak. Ez a rendelkezés amiatt lényeges, mert biztosítja a közvetítő szolgáltatók számára, hogy nem jelenti a DSA szerinti immunitás elveszítését, ha önkéntes, saját kezdeményezésű, jóhiszemű vizsgálatok és jogi megfelelés keretében olyan intézkedéseket hoznak, melyek jogellenes tartalom észlelésére, azonosítására és eltávolítására vonatkoznak. Az elektronikus kereskedelemről szóló irányelv 15. cikke szerinti korábbi mentesülés ugyanis csak *technikai, automatikus és passzív* jellegű tevékenységek esetében állt fenn és önkéntes vizsgálatok esetére azzal a veszéllyel járt, hogy a közvetítő szolgáltatókat önkéntes intézkedések esetében felelőssé teszik a jogsértő tartalomért. Azon szolgáltatók tehát, akik önkéntesen ellenőrizték a szolgáltatásaik útján közvetített tartalmakat vagy szoftveres eszközökkel állandó megfigyelés alatt tartották azokat, „tudomást szereztek" e jogellenes tartalmakról, ami a felelősség alóli mentesülés alkalmazását akadályozta. Ezen a szolgáltatók számára hátrányos lehetett, akik igyekeztek önkéntesen feltárni és eltávolítani a jogsértő tartalmakat.[70]

A felelősség alóli mentesülés csak azoknak a szolgáltatóknak kedvez, akik „önkéntesen", „jóhiszeműen", „gondossággal" és a nemzeti jog, az uniós jog, különösen pedig a DSA rendelkezéseinek megfelelően járnak el. Ezen önkéntes vizsgálatok esetében szükségszerűen felmerülnek adatvédelmi kérdések, különösen azok jogalapjával, szükségességével és arányosságával kapcsolatosan. Ha az alkalmazott önkéntes intézkedések szükségtelenek, aránytalanok vagy nem megfelelőek, a felelősséget az általános szabályok alapján kell

[68] Európai Unió Bírósága, Promusicae-ügy, C-275/06, Productores de Música de España (Promusicae) vs. Telefónica de España SAU. (ECLI:EU:C:2008:54)
[69] Európai Unió Bírósága, C-461/10. – Bonnier Audio AB és társai v. Perfect Communication Sweden AB ügy (ECLI:EU:C:2012:219) (2012)
[70] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 7. Rn 1; p. 108.; vö. Koltay András, Szikora András, Lapsánszky András, Tóth András (szerk.) - Nagykommentár a DSA rendelethez, Wolters Kluwer, 2024; 7. cikk; 77. oldal

megítélni. A DSA (26) preambulumbekezdése kiemeli, hogy a DSA 7. cikk célja az, hogy elkerülje az önkéntes megfigyelési intézkedések hátrányait, hogy ne akadályozza meg a szolgáltatókat abban, hogy ilyen intézkedéseket hajtsanak végre. Az „*önkéntes*" megfigyelési intézkedések csak akkor minősülnek valóban önkéntesnek, ha azok végrehajtása nem jogszabályi, bírósági vagy hatósági kötelezettségen alapul, hanem a szolgáltató saját kezdeményezésére történik. A szolgáltatóknak meg kell adni a választási lehetőséget, hogy végrehajtják-e ezeket az intézkedéseket, amelyek a felhasználási feltételekben előre közölhetők, és a felhasználók hozzájárulását igénylik. Ezeket az intézkedéseket objektíven, arányosan, jóhiszeműen és nem diszkriminatív módon kell végrehajtani, biztosítva, hogy a jogszerű tartalmak indokolatlan eltávolítását elkerüljék. Amennyiben automatizált eszközöket alkalmaznak, a technológia megbízhatóságának biztosítania kell a minimális hibaarányt, a pontosság adatkezelési elvének megfelelően. A „*gondossági*" követelmény pedig azt várja el, hogy a szolgáltatók figyelembe vegyék az összes érintett fél jogait és érdekeit, mielőtt egy tartalmat jogellenesnek minősítenek és eltávolítanak. Az Európai Bíróság joggyakorlata szerint az ilyen intézkedések során *méltányos egyensúlyt kell biztosítani* a szellemi tulajdonjogok, a személyes adatok védelméhez való jog, a vállalkozás szabadsága és az információk szabad áramlásának jogai között. Ezen intézkedések jogszerűségének megítélése során hasonló elvek alkalmazandók, mint a kötelező szűrőszoftvereknél.

Az EDPS a DSA-val kapcsolatos véleménye 27. pontjában maga is emlékeztetett arra, hogy az önkéntes intézkedések is beavatkozást jelenthetnek az adatvédelemhez és a magánélethez való jogokba. További biztosítékok hiányában fennáll a kockázata annak, hogy közvetetten hozzájárulhat olyan személyes adatok kezeléséhez, amely *nem arányos* a kitűzött célokkal, különösen azáltal, hogy nem határozza meg pontosan azokat az illegális tartalomtípusokat, amelyek valóban indokolják a személyes adatok kezelésével járó automatizált észlelési technikák alkalmazását, illetve, ha nem rögzíti azokat a körülményeket, amelyek között ez önkéntesen a hatóságok tudomására hozhatók. Ezen önkéntes automatizált észlelési technikák alkalmazása és ennek jogszerűségi feltételeinek kialakítása az adatvédelmi felügyeleti hatóságok és a digitális szolgáltatási koordinátorok együttműködését fogja igényelni, ennek hiányában számolni lehet azzal, hogy nem fogja ösztönözni a szolgáltatókat arra, hogy önkéntes intézkedéseket hozzanak jogellenes tartalmakkal szemben.

6.1.4 Tartalommoderálási transzparencia

Tartalom moderálással kapcsolatos transzparencia különösen automatizált eszközök alkalmazása esetében releváns és a DSA rendelkezései ezzel kapcsolatosan tág tájékoztatási kötelezettségeket ír elő a szolgáltatók számára, ami többek között magában foglalja az ilyen eszközök alkalmazását és annak hatását a felhasználó jogaira. A DSA szerinti tájékoztatási kötelezettségek kiegészítik és nem érintik a szolgáltatók azon kötelezettségét, hogy tájékoztatást nyújtsanak az érintettek számára a GDPR 12-14. cikkeinek megfelelően. Ezek célja a tartalommoderálási gyakorlatok, beleértve a személyes adatok kezelésével járó intézkedések átláthatóságának további növelése.[71] Ezek a követelmények hozzájárulnak a felhasználói jogok védelméhez, az átláthatóság és az adatbiztonság előmozdításához, valamint az adatkezelési gyakorlatok adatvédelmi követelményeknek való megfeleléséhez, mivel a GDPR transzparencia követelményeit előíró 12-14. cikkei és a DSA transzparencia követelményei

[71] vö. EDPS DSA vélemény 33. sarokpontja

együttesen biztosítják, hogy az online platformok elszámoltatható módon kezeljék a személyes adatokat a tartalommoderáció során.

A DSA 14. cikke szerinti *szerződési feltételekre* vonatkozó szabályai előírják, hogy a platformoknak tájékoztatniuk kell a felhasználókat az általános szerződési feltételeken keresztül minden olyan szabályzatról, eljárásról, intézkedésről és eszközről, amelyet a tartalommoderáció céljából alkalmaznak, beleértve az algoritmikus döntéshozatalt és az emberi felülvizsgálatot, illetőleg a belső panaszkezelési rendszerük eljárási szabályzatára vonatkozó információkat és azok bármely jelentős változását is. Ez az előírás közvetlen adatvédelmi relevanciával bír, mivel az algoritmikus tartalommoderálás során személyes adatok kerülhetnek kezelésre. A szolgáltatóknak világos és átlátható információt kell nyújtaniuk arról, hogyan használják fel a felhasználók adatait a tartalommoderálási folyamat során, valamint arról, hogy az ilyen döntéshozatali eljárásokba milyen mértékben vonnak be emberi felülvizsgálatot. Ez biztosítja, hogy a felhasználók tisztában legyenek azzal, hogy adataik milyen módon kerülnek felhasználásra, és megértik a tartalommoderálási eljárások hatását a magánéletükre és személyes adataikra. A DSA 14. cikk (4) bekezdése ezzel kapcsolatosan előírja, hogy a szolgáltatónak *kellő gondossággal, objektíven és arányosan* kell eljárniuk a szerződési feltételeik alapján alkalmazott korlátozások alkalmazása és érvényesítése során, kellően figyelembe véve valamennyi érdekelt fél jogait és jogos érdekeit, beleértve a szolgáltatás igénybe vevőit megillető alapvető jogokat, melyekbe beleértendők a magánélet védelméhez tartozó jogok is. Az automatikus tartalommoderálás során gyakran kerül sor személyes adatok, például IP-címek vagy felhasználói tevékenységek kezelésére, amelyek a GDPR szerint személyes adatnak minősülnek. A GDPR 13. és 14. cikke előírja, hogy a személyes adatok kezelése során a felhasználókat részletesen tájékoztatni kell az adatkezelés céljáról, jogalapjáról, a kezelt személyes adatokról, az adatok forrásáról, valamint az érintettek jogairól és arról, ha személyes adataikat automatizált döntéshozatali folyamatokban használják fel, különös tekintettel azokra a helyzetekre, amikor az ilyen döntések jogi hatással bírnak vagy jelentős következményekkel járnak a felhasználókra nézve. Az illegális tartalmak felismerésére és eltávolítására szolgáló automatizált rendszerek különösen fontosak a felhasználók számára, mivel ezek befolyásolhatják hozzáférésüket egyes szolgáltatásokhoz, illetve tartalmakhoz.

Ezt meghaladóan a DSA 15. cikke arra kötelezi a szolgáltatókat, hogy átláthatósági jelentéseikben adjanak részletes tájékoztatást az automatikus tartalommoderációs eszközök alkalmazásáról, ideértve a panaszok számát, a panaszok alapját, az e panaszokra vonatkozó döntéseket, a döntések meghozatalához szükséges medián idő és azon esetek számát, amikor e döntéseket megváltoztatták. Az átláthatósági jelentések így kiegészítik a DSA 14. cikke és a GDPR 12-14. cikkei alapján a felhasználók részére nyújtott tájékoztatásokat, figyelemmel arra, hogy részletesen bemutatják a szolgáltató tartalommoderációs gyakorlatát.

A DSA 16. cikk azt is megköveteli, hogy a platformok könnyen hozzáférhető és felhasználóbarát *bejelentési és cselekvési mechanizmusokat* biztosítsanak, melyek alkalmazásáról indokolatlan késedelem nélkül értesíteni az adott magánszemélyt vagy szervezetet a bejelentés tárgyát képező információkkal kapcsolatos döntéséről, tájékoztatást nyújtva az e döntéssel kapcsolatos jogorvoslati lehetőségekről. Az ilyen döntésekben tárhelyszolgáltatók esetében

azt is fel kell tárni, ha az említett bejelentések kezeléséhez vagy döntéshozatalhoz automatizált eszközöket vesznek igénybe.[72]

A DSA 17. cikke előírja, hogy amikor egy platform korlátozásokat vezet be a felhasználókkal szemben – például egy tartalom eltávolításakor vagy egy fiók felfüggesztésekor, információ eltávolításakor, hozzáférhetőségének megszüntetésekor, hátrasorolásakor vagy láthatóságának korlátozásakor, vagy az adott információhoz kapcsolódó pénzkifizetések felfüggesztésekor vagy megszüntetésekor –, az indoklásnak tartalmaznia kell információkat az automatizált eszközök használatáról a döntéshozatal során. Az átláthatóság ezen követelménye biztosítja, hogy a felhasználók tisztában legyenek azzal, hogy döntések – például a hozzáférés megtagadása vagy a tartalom eltávolítása – részben vagy egészben automatizált módon történtek.

A DSA ezen tartalommoderálási transzparencia előírásai szorosan kapcsolódnak a GDPR által meghatározott tájékoztatási kötelezettségekhez, különösen a 12-14. cikkek szerinti követelményekhez. Ezek az előírások biztosítják, hogy a felhasználók részletes és átlátható információkat kapjanak a személyes adataik automatizált rendszerek általi kezeléséről, és megértsék, hogyan befolyásolják ezeket a rendszerek a jogaikat és lehetőségeiket. A DSA rendelkezései tehát további fontos adatvédelmi garanciákat biztosítanak a digitális térben a tartalommoderálási eljárások átláthatósága révén.

Az EDPS a DSA véleményében utalt arra[73], hogy GDPR 22. cikke szigorú feltételeket szab az automatizált döntéshozatali eljárásokra, különösen, ha ezek jogi hatásokkal járnak vagy jelentősen befolyásolják az érintettet. Ezen szakasz (1) bekezdése szerint ugyanis az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené, ami ezáltal egy általános tilalmat állapít meg a kizárólag automatizált adatkezelésen alapuló döntéshozatal tekintetében. [74] A GDPR (71) preambulumbekezdésével összhangban „megengedhető azonban az efféle adatkezelésen – ideértve profilalkotást is – alapuló döntéshozatal, ha azt (...) uniós vagy tagállami jog kifejezetten engedélyezi (...), vagy arra (...) szerződés megkötése vagy teljesítése érdekében van szükség, vagy ha az érintett ahhoz kifejezett hozzájárulását adta". Ilyen adatkezelés esetében a GDPR vonatkozó feltételeit szintén teljesítenie kell a szolgáltatónak, ezért az online platformoknak, amelyek automatizált eszközöket használnak a tartalommoderáció vagy a döntéshozatal során, tájékoztatniuk kell az érintetteket az eljárásról, a használt technológiáról, valamint a döntés alapját képező kritériumokról és érvekről, figyelembe véve a GDPR szerinti tájékoztatási kötelezettségeket.

A bejelentési és cselekvési mechanizmusok és a kapcsolódó indokolási kötelezettségek tartalommoderálás transzparenciáját segíti elő továbbá az a kötelezettség is, hogy az online platformot üzemeltető szolgáltatóknak a DSA 24. cikk (5) bekezdése alapján a tartalommoderálási döntéseiket és azok DSA szerinti indokolását fel kell tölteniük egy, az Európai Bizottság által kezelt, úgynevezett átláthatósági adatbázisba

[72] vö. DSA 15. cikk (6) bekezdése

[73] EDPS Opinion 1/2021 on the Proposal for a Digital Services Act, 42. pont, p.11

[74] vö. 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához; WP251rev.01, 21. oldal

(https://transparency.dsa.ec.europa.eu/), melynek útján nyilvánosságra kell hozniuk döntéseiket és azok indoklását egy nyilvánosan hozzáférhető adatbázisban, azzal a kitétellel, hogy ezek az információk nem tartalmazhatnak személyes adatokat.

6.1.5 Belső panaszkezelési rendszer

A DSA 20. cikk előírja, hogy az online platformoknak belső panaszkezelési rendszert kell biztosítaniuk, amely lehetővé teszi a felhasználók számára, hogy hat hónapon belül panaszt nyújtsanak be a platform döntései ellen, ha tartalommoderálás keretében eltávolítják vagy letiltják a hozzáférést egy tartalomhoz, vagy felfüggesztik vagy megszüntetik a szolgáltatást (vagy a felhasználói fiókot), figyelemmel arra, hogy a szolgáltatás igénybe vevői által rendelkezésre bocsátott információ jogellenes tartalomnak minősül vagy nem egyeztethető össze a szolgáltató szerződési feltételeivel. Ez a rendelkezés a felhasználók számára a tartalommoderációval kapcsolatosan az ún. „overblocking" intézményével szemben nyújt védelmet, ami adatvédelmi szempontból azért releváns, mivel, ha a platformok algoritmusai hibásan értelmezik a felhasználók viselkedését vagy tartalmát, az overblocking alapja lehet a pontatlan profilalkotásnak, ami sértheti a pontosság elvét és ezáltal a felhasználók adatvédelmi jogait, mellyel kapcsolatosan további biztosítékot jelent a DSA szabályozása.

A 20. cikk (6) bekezdése kimondja, hogy a platformoknak biztosítaniuk kell, hogy az ilyen panaszok elbírálása ne kizárólag automatizált eszközökkel történjen, azaz természetes személyt kell bevonni ebbe az eljárásba (Human-in-the-Loop)[75]. Az online platformot üzemeltető szolgáltatók indokolatlan késedelem nélkül tájékoztatják a panaszosokat a panasz tárgyát képező információkkal kapcsolatos indokolt döntésükről, és a peren kívüli vitarendezés 21. cikkben szabályozott lehetőségéről, valamint az egyéb elérhető jogorvoslati lehetőségekről. Ezzel kapcsolatosan rögzítendő, hogy a panaszkezelési mechanizmus létezése nem érinti az érintetteknek a GDPR és az ePrivacy irányelv szerinti jogait és jogorvoslati lehetőségeit, azaz a felhasználót nem zárhatja el attól, hogy egyéb (például adatvédelmi hatósági) úton érvényesítse az igényét, ha a panasz az adatvédelmi jogait érinti.

6.2 Profilalkotási korlátozások

A DSA részletes előírásokat tartalmaz a profilalkotással kapcsolatban, amelyek célja a felhasználók adatainak védelme és a transzparencia növelése az online platformokon. A „profilalkotás" fogalmát a GDPR 4. cikk 4. pontja határozza meg akként, hogy ez a személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják. A 29. cikk szerinti adatvédelmi munkacsoport automatizált döntéshozatallal és a profilalkotással kapcsolatban kiadott iránymutatás szerint a profilalkotás három elemből áll: (i) valamilyen formájú automatizált kezelésnek kell lennie, bár az emberi beavatkozás nem feltétlenül jelenti azt, hogy az adott tevékenységre nem alkalmazható a meghatározás.; (ii) személyes adatok tekintetében kell végezni; és (iii) a profilalkotás célja egy természetes személy személyes

[75] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 20. Rn 63; p. 244.

jellemzőinek értékelése, mikor a profilalkotás együtt jár a személyre vonatkozó valamilyen értékeléssel vagy megítéléssel. A természetes személyek ismert tulajdonságokon (pl. életkor, nem vagy magasság) alapuló egyszerű besorolása nem vezet szükségképpen profilalkotáshoz, mikor a cél nem az egyéni jellemzők értékelése. Ez függ az osztályozás céljától. A profilalkotás három különböző szakaszból állhat: adatgyűjtésből; automatizált elemzésből az összefüggések felismerésére; és az összefüggések alkalmazása adott természetes személyre a jelenlegi vagy jövőbeli viselkedés jellemzőinek azonosítására.[76] Ha ez a tevékenység személyes adatok *nagy számú*, illetve *módszeres értékelését* is magában foglalja, akkor az érintett jogaira és szabadságaira jelentett magas kockázatok miatt hatásvizsgálat köteles tevékenység GDPR 35. cikk (4) bekezdése alapján közzétett Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) hatásvizsgálati lista alapján.

29. cikk szerinti adatvédelmi munkacsoport iránymutatása szerint a profilalkotás különböző kockázatokkal járhat, mivel ráerősíthet a meglevő sztereotípiákra és társadalmi szegregációra, illetve személyeket bizonyos kategóriákba skatulyázhatja be, és a számukra javasolt preferenciákra korlátozhatja őket. Ez alááshatja az egyének választási szabadságát például bizonyos termékek vagy szolgáltatások – könyvek, zene vagy hírcsatornák – tekintetében. Bizonyos esetekben pedig a profilalkotás pontatlan előrejelzésekhez vezethet, más esetekben a szolgáltatások és áruk igénybevételének megtagadásához és indokolatlan megkülönböztetéshez vezethet, ezért megfelelő garanciákat igényel ennek alkalmazása.[77]

A platformok gyakran használják a személyes adatokat arra, hogy testreszabják a felhasználói élményt és javítsák a tartalommoderálást, ugyanakkor ezek az adatok jobb reklámszolgáltatásokat is lehetővé tesznek a hirdetők számára. A DSA ezzel kapcsolatosan különös figyelmet fordít három kulcsfontosságú területre: *online hirdetések,* a *kiskorúak online védelme*, és *ajánlórendszerek* alkalmazása. A profilalkotás tehát az egyik legfontosabb adatvédelmi kérdés, amelyet a DSA szabályoz. A DSA a GDPR előírásait továbbfejlesztve szigorítja a profilalkotáson alapuló célzott reklámokra vonatkozó szabályokat, különösen személyes adatok különleges kategóriáinak alkalmazása esetén és a kiskorúak védelmében. Az ajánlórendszerek esetében is fontos korlátozásokat vezet be, különösen online óriásplatformokra nézve, hogy a felhasználók választhassanak a profilalkotáson alapuló és nem alapuló ajánlások között. Ezek az intézkedések erősítik az online adatvédelem szintjét és elősegítik a transzparenciát a digitális szolgáltatások területén.

6.2.1 Online hirdetések

A DSA 26. cikk külön előírásokat tartalmaz az online hirdetésekre és azok transzparenciájára vonatkozóan. A DSA (68) preambulumbekezdése szerint az online hirdetések fontos szerepet játszanak az online környezetben, többek között az online platformok szolgáltatásnyújtásával kapcsolatban, ahol a szolgáltatásnyújtást olykor részben vagy egészben közvetlenül, vagy közvetve reklámbevételek révén ellentételezik. A DSA szabályozásának indoka az online platformok és az ott megjelenő hirdetések jelentősége (a Meta 2021-ben 115 milliárd USD-t

[76] vö. 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához; WP251rev.01, 7. oldal
[77] 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához; WP251rev.01, 2. oldal

forgalmazott, míg a YouTube 29 milliárd USD-t) és a több szolgáltatást is átfogó, személyes adatok tömeges és extenzív gyűjtésével járó jellege[78]. Az adatvédelmi követelmények teoretikus korlátját jelentik az ilyen típusú hirdetéseknek, figyelemmel az adatvédelmi jog és a célzás pontossága közötti konfliktusra, ezért az Európai Adatvédelmi Testület a 8/2020. sz. iránymutatásában[79] részletesen foglalkozott a közösségi média felhasználóinak megcélzásával és az egyes célzási módszerek elemzésével, az egyes szereplőkkel és azok felelősségével.

A „hirdetés" fogalmát a DSA 3. cikk r) pontja határozza meg és az valamely jogi vagy természetes személy üzenetének népszerűsítésére szolgáló információ*, függetlenül attól, hogy kereskedelmi vagy nem kereskedelmi célokat szolgál*, amelyet egy online platform megjelenít az online interfészén a *kifejezetten az ilyen információ népszerűsítéséért fizetett ellentételezés fejében*. Ez a fogalom egyrészről tágabb[80], mint a kereskedelmi kommunikáció fogalma, mivel politikai vagy társadalmi célú (fizetett) „hirdetése" is beletartozhat. Másrészről ez a fogalommeghatározás *szűkebb*[81], mivel a magában foglalja az (i) ellentételezés elemet, azt is, hogy azt (ii) kifejezetten az ilyen információ népszerűsítéséért adják és, hogy (iii) az ellentételezés online platformnál jelentkezik ezért.

A profilozáson alapuló célzott hirdetés a hirdetés olyan formája, amely specifikus közönségre irányul a reklámozó által népszerűsített termék vagy szolgáltatás alapján. A célzás különböző jellemzők figyelembevételével történhet, beleértve a demográfiai adatokat, mint például a gazdasági helyzet, nem, kor, iskolai végzettség vagy jövedelmi szint. Emellett alapulhat a felhasználók online viselkedésére, például a megtekintett oldalakra, a keresett kifejezésekre vagy a látogatások gyakoriságára. Az érdeklődési körök is fontos tényezők, mint például a felhasználói kedvelések, követések vagy megtekintett tartalmak. A célzott hirdetések lényege, hogy a megcélzott személy és az üzenet között feltételezett összhang alapján pontosan célzott, releváns üzeneteket továbbítsanak, ezzel növelve a reklám hatékonyságát és a konverzió esélyét. A célzott hirdetések létrehozásához különböző eszközöket használnak, amelyek segítségével a felhasználók online tevékenysége követhető és személyes adatok extenzív kezelésével jár. Ilyen eszközök a sütik és egyéb azonosítók, JavaScript kódok, közösségimédia-szolgáltatások, nyomkövető képpontok, valamint beépülő közösségi média modulok. A célzás során a készülékek, alkalmazások és online azonosítók, például internetprotokoll-címek és sütiazonosítók alapján követik a felhasználó tevékenységét. Ezen információk alapján eszközökön átívelő egyéni profilt hoznak létre, amely lehetővé teszi, hogy személyre szabott hirdetéseket küldjenek a felhasználó számára, figyelembe véve az eszköz-ujjlenyomat technológiáját is, amely a felhasználó egyedi online jelenlétét térképezi fel.

A targetált hirdetések számos *kockázatot* hordoznak magukban[82]. Ezek közé tartozik az adatkezelés, amely gyakran túlmutat az egyének észszerű elvárásain, valamint a célzáshoz kapcsolódó profilalkotás intruzív jellege. A felhasználók gyakran elveszítik az irányítást saját adataik felett, miközben az adatkezelés átláthatóságának hiánya tovább fokozza a problémát.

[78] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 26. Rn 1-2; pp. 311-312.
[79] Európai Adatvédelmi Testület 8/2020. sz. iránymutatása a közösségi média felhasználóinak megcélzásáról, 2.0. változat, elfogadás időpontja: 2021. április 13.; lehívás: 2024.09.14.
[80] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 3. Rn 125; p. 48.
[81] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 3. Rn 123; pp. 123.
[82] vö. EDPB 8/2020. sz. iránymutatása a közösségi média felhasználóinak megcélzásáról; 9.-18. sarokpontok.

További kockázatot jelent a megkülönböztetés és kirekesztés lehetősége, illetve a felhasználók manipulálása, ami aláássa az egyéni autonómiát és szabadságot. Az információs túlterheltség szintén veszélyeztetheti a felhasználók döntéshozatali képességét. Különösen kiszolgáltatott helyzetben lévő érintettek célzása etikai aggályokat vet fel, míg a politikai diskurzus befolyásolása és a dezinformáció terjedése hosszú távon destabilizáló hatással lehet a társadalomra[83]. Ezek a kérdések különösen a Cambridge-Analytica botrány ürügyén merültek fel és azzal a következménnyel jártak, hogy az online platformok korlátozni kezdték az egyes célzási opciókat.[84]

A 29. cikk szerinti adatvédelmi munkacsoport az automatizált döntéshozatallal és a profilalkotással kapcsolatos iránymutatása is rámutat arra, hogy az online hirdetések egyre inkább támaszkodnak automatizált eszközökre, és kizárólag automatizált egyedi döntéshozatalt foglalnak magukban, melyek alkalmazására a GDPR 22. cikkének szigorú feltételei irányadók, mivel az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené. Sok tipikus esetben a profilalkotáson alapuló célzott hirdetés bemutatására vonatkozó döntésnek nem lesz hasonlóan jelentős mértékű hatása a természetes személyekre, azonban elképzelhető, hogy lehet ilyen hatása az eset sajátos jellemzőitől függően. Így egy online hirdetéssel kapcsolatos adatkezelés, amely első ránézésre csak csekély hatással lehet az egyénekre, komolyabb következményekkel járhat egyes társadalmi csoportokra, például kisebbségekre vagy kiszolgáltatott felnőttekre nézve. Példaként említi a munkacsoport, ha valakit, aki feltételezhetően pénzügyi problémákkal küzd, rendszeresen magas kamatozású hitelek reklámjaival céloznak meg, és elfogadja ezeket az ajánlatokat, további adósságokat halmozhat fel. Az automatizált döntéshozatal, amely személyes adatokon vagy jellemzőkön alapuló megkülönböztető árazást alkalmaz, szintén jelentős hatással lehet, például, ha valakit túl magas árak miatt kizárnak bizonyos szolgáltatásokból vagy áruk igénybevételéből.[85]

A targetált hirdetések szereplői között *több különböző fél* található[86]. A felhasználók lehetnek regisztrált vagy nem regisztrált személyek, akiket a hirdetések célba vesznek, és ők egyben érintettnek minősülnek. A szolgáltatók olyan platformok vagy alkalmazások, amelyek megosztják a tartalmakat és információkat, és sok esetben több forrásból kombinálják az adatokat, platformon belül és kívül is. A célzók a reklámozók, akik az érintettek feltételezett jellemzői, érdeklődési körei és preferenciái alapján választják ki célközönségüket. Emellett egyéb szereplők is részt vesznek a folyamatban, mint például marketingszolgáltatók, hirdetési hálózatok, hirdetéscserélők (ad exchange), valamint keresleti és kínálati oldali platformok (SSP és DSP). Adatkezelési szolgáltatók (DMP-k) és adatelemzéssel foglalkozó vállalatok is kulcsszerepet játszanak a hirdetések hatékony célzásában. A különböző szereplőkkel és azok felelősségével kapcsolatosan az Európai Adatvédelmi Testület 8/2020. sz. iránymutatása

[83] EDRI - Sex, religion and race are advertising taboos, except for power-hungry politicians - By Civil Liberties Union For Europe · May 31, 2023; lehívás: 2024.09.14.
[84] Facebook: Removing Certain Ad Targeting Options and Expanding Our Ad Controls; Announcements; November 9, 2021; lehívás: 2024.09.14
[85] vö. 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához; WP251rev.01, 23-24. oldal
[86] vö. EDPB 8/2020. sz. iránymutatása; 19.-29. sarokpontok.

rámutat a EUB vonatkozó ítélkezési gyakorlatára és különösen a Wirtschaftsakademie (C-210/16. számú ügy), a Jehova tanúi (C-25/17. számú ügy[87]) és a Fashion ID (C-40/17. számú ügy) ügyekben hozott ítéletekre, hogy ezek minősülnek relevánsnak a célzók és a közösségimédia-szolgáltatók közötti kapcsolatot illetően és ezek a felek közös adatkezelőnek minősülnek annak valamennyi jogi következményével együtt és a GDPR 26. cikke alkalmazandó a kötelezettségeikre. Ezzel kapcsolatosan szintén releváns az IAB Europe C-604/22. számú ügy, mivel az Európai Unió Bírósága megállapította, hogy az IAB Europe által létrehozott „Transparency & Consent Framework" keretében közös adatkezelőként minősül, mivel a hozzájárulás megszerzésével és kezelésével kapcsolatosan befolyást gyakorolt a tagjai által kezelt személyes adatokra, még ha közvetlenül nem is fér hozzá ezekhez az adatokhoz és ezáltal a tagjaival osztozott a GDPR 26. cikkében meghatározott kötelezettségekben[88].

A DSA szabályozásának célja, hogy transzparenssé tegye az online hirdetéseket és az online platformot üzemeltető szolgáltatókat arra kötelezi, hogy a szolgáltatások igénybe vevőinek a rendelkezésére bocsátsanak bizonyos, annak megértéséhez szükséges egyedi információkat, hogy a hirdetés megjelenítésére mikor és kinek a nevében kerül sor.[89] A DSA 26. cikke alapján az online platformoknak világosan és egyértelműen fel kell tüntetniük minden egyes hirdetés esetében: (i) hogy az adott információ hirdetés, (ii) ki jeleníti meg a hirdetést (a hirdető személy vagy cég), (iii) ki finanszírozta a hirdetést (ha eltér a megjelenítőtől), és (iv) a hirdetés megcélzott felhasználói csoportjának meghatározására szolgáló paramétereket. Ezek a rendelkezések az elektronikus kereskedelemről szóló irányelv 6. cikk a)-b) pontjaiban meghatározott transzparencia szabályokat meghaladóan érvényesülnek, melyet Magyarországon az Elkertv. 14/A. § ültetett át a magyar jogba.

Az online óriásplatformoknak (VLOP) és nagyon népszerű online keresőprogramoknak (VLOSE) az online hirdetések transzparenciájával kapcsolatosan többletkötelezettségeik vannak, mivel a DSA 34. cikk (2) bekezdés d) pontja és a DSA 35. cikk (1) bekezdés e) pontja előírja, hogy az éves kockázatértékelés részeként a hirdetések kiválasztását és megjelenítését végző rendszereik esetében figyelembe kell venni, hogy azok befolyásolják-e a rendszerszintű kockázatok bármelyikét, ideértve a személyes adatok védelméhez való alapvető jogot és hogy ez a hirdetési rendszereik módosítását és az általuk kínált szolgáltatásokkal kapcsolatban a hirdetések megjelenítésének korlátozását vagy kiigazítására irányuló célzott intézkedések elfogadását teszi-e szükségessé. A DSA 39. cikk továbbá előírja, hogy egy publikus adattárat kell fenntartaniuk és egy évig archiválniuk, amely tartalmazza az összes hirdetéssel kapcsolatos információt, így a hirdetések megjelenítőjének és finanszírozójának nevét, valamint a célzásra használt paramétereket is. Ez az adattárt API-n keresztül kell elérhetővé tenni, és biztosítja az átláthatóságot az itt megjelenő online hirdetésekkel kapcsolatban. A DSA 44. cikk (1) bekezdés h) pontja önkéntes szabványok kidolgozását és végrehajtását, továbbá az online hirdetésekre vonatkozó magatartási kódexek kidolgozását támogatja.

A DSA-ban szabályozott hirdetéssel kapcsolatos transzparencia rendelkezések és tilalmak nem érintik a GDPR rendelkezéseit és azok alkalmazását, így a személyes adatok hirdetési célú kezelésének jogszerűségére vonatkozó rendelkezéseket, a személyes adatok kezelésével

[87] Európai Unió Bírósága a C-25/17. számú ügyben hozott 2018. július 10-ei Jehovan todistajat-ítélet, C-25/17, EU:C:2018:551

[88] vö. CJEU Judgement of 7 March 2024 in TCF Case: IAB Europe's Analysis; 23 April 2024, lehívás: 2024. 09. 23.

[89] vö. DSA (68) preambulumbekezdés harmadik mondatát

kapcsolatos átláthatósági, illetve tájékoztatási követelményeket, valamint az automatizált egyedi döntéshozatalt, beleértve a profilalkotást és a hatásvizsgálati kötelezettséget. Ezek a rendelkezések nem érintik az ePrivacy irányelv alkalmazását sem, különösen, amelyek az információk végberendezésben történő tárolására, valamint az ott tárolt információkhoz való hozzáférésre vonatkoznak.[90]

Bár a célzott hirdetések és a profilalkotás önmagában nem tilos a GDPR szerint, a DSA szigorúbbá tette a vonatkozó előírásokat, ha különleges kategóriájú személyes adatokról vagy kiskorúakról van szó. Korábban, a GDPR és az ePrivacy irányelv értelmében a felhasználók tiltakozhattak a profilalkotás ellen (vö. GDPR 21. cikk), vagy hozzájárulásukra volt szükség (vö. ePrivacy irányelv 6. cikke alapján). A DSA 26. cikk (3) bekezdése viszont megtiltja az online platformok számára, hogy profilalkotáson alapuló hirdetéseket jelenítsenek meg, ha ezek különleges kategóriájú személyes adatokon alapulnak (pl. egészségi állapot, politikai vélemény, vallás). Ez a rendelkezés egyértelműen a felhasználók adatvédelmének megerősítését szolgálja, és szigorúbb szabályokat vezet be, mint amilyeneket a GDPR vagy az ePrivacy irányelv előír. Ez az intézkedés fontos szerepet játszik a felhasználók védelmében, különösen az úgynevezett manipulatív technikák elleni harcban, amelyek célja a felhasználók kihasználása.[91] A DSA 69. preambulumbekezdése kiemeli, hogy különösen súlyos negatív hatásokkal járhatnak azok a célzott hirdetések, amelyek a felhasználók gyenge pontjait használják ki, és optimalizált technikákon alapulnak. Ezek a manipulatív módszerek egyes esetekben egész csoportokat érinthetnek, társadalmi károkat okozva, például dezinformációs kampányok vagy hátrányos megkülönböztetés révén. Az online platformok különösen érzékenyek ezekre a kockázatokra. Ez a tilalom nem befolyásolja az uniós adatvédelmi jogszabályok szerinti kötelezettségeket, amelyek a hirdetések terjesztésében részt vevő szolgáltatókra és hirdetőkre vonatkoznak.

6.2.2 Kiskorúak online védelme

A DSA (71) preambulumbekezdése hangsúlyozza, hogy a kiskorúak védelme az Unió egyik fontos szakpolitikai célkitűzése. A DSA szabályozása ezt transzparencia szabályokkal és a kiskorúakra kockázatot jelentő interfész kialakítások és profilozás tilalmával próbálja elérni, figyelemmel arra, hogy a kiskorúak különösen sérülékeny és kiszolgáltatott csoportnak tekinthetők online szolgáltatások igénybevételével kapcsolatosan és sötét tervezési minták áldozatául eshetnek, amely a személyes adataikat is érinti.

A DSA 28. cikke online platformot üzemeltető szolgáltatók vonatkozik és különös védelmet biztosít a kiskorúak számára a profilalkotáson alapuló célzott hirdetésekkel szemben. A cikk megtiltja az online platformoknak, hogy olyan „hirdetéseket”[92] jelenítsenek meg a kiskorú felhasználók számára, amelyek a GDPR 4. cikk 4. pontjában meghatározott profilalkotáson alapulnak. Ez a tilalom mindenféle személyes adat felhasználásán alapuló profilalkotásra vonatkozik, amennyiben kiskorúakról van szó. Ez a szabály akkor lép érvénybe, ha a platformok "kellő bizonyossággal" tudják, hogy a felhasználó kiskorú. A kiskorúak személyes adatait különösen védi, hiszen az online platformok nem gyűjthetnek külön adatokat annak

[90] DSA Guidelines - Due diligence obligations for intemediary services - Netherlands Authority for Consumers and Markets; 188. sarokpont.
[91] vö. Domingos Soares Farinho im. p. 51.
[92] vö. a „hirdetés” DSA fogalmával kapcsolatos fogalommeghatározást a 3. cikk r) pontban

érdekében, hogy meghatározzák, a felhasználó kiskorú-e, hanem más módon kell biztosítaniuk, hogy megfelelő védelmet biztosítsanak a kiskorúaknak.

A DSA és a GDPR között jelentős különbség van a terminológia tekintetében, mivel a GDPR a "gyermek" kifejezést használja, addig a DSA a "kiskorú" fogalmát, amely az uniós jogrendszerekben azoknak az adatalanyoknak a kategóriáját jelenti, akik még nem rendelkeznek teljes cselekvőképességgel[93]. A GDPR 8. cikke szerint a gyermekek 16 éves kortól (vagy ennél fiatalabb kortól, ha a nemzeti jog ezt megengedi) járulhatnak hozzá az információs társadalommal kapcsolatos szolgáltatások használatához. A DSA 28. cikke viszont megakadályozza, hogy a platformok célzott hirdetéseket jelenítsenek meg kiskorúaknak profilalkotás alapján, függetlenül attól, hogy a kiskorúak (vagy akár törvényes képviselő) a GDPR 8. cikke alapján egyébként hozzájárulhatnak-e a szolgáltatás használatához.

Gyermekek személyes adatainak kezelése *profilozás*, *automatikus döntéshozatal*, vagy *marketing céljából*, vagy *közvetlenül részükre kínált, információs társadalommal összefüggő szolgáltatások ajánlása* vonatkozásában a magyar adatvédelmi hatóság GDPR 35. cikk (4) bekezdése alapján hatásvizsgálat köteles tevékenység[94] azonban a gyermekek sérülékeny volta miatt a GDPR 35. cikk (1) bekezdése alapján a magas kockázatok miatt is indokolható ez. Az online óriásplatformoknak (VLOP) és nagyon népszerű online keresőprogramoknak (VLOSE) a DSA 34. és 35. cikke alapján az adatvédelmi hatásvizsgálatot meghaladó további kötelezettségei is vannak, mivel a DSA szerinti kockázatértékelésük részévé kell tenniük a gyermekek jogait érintő kockázatok felmérését is. A DSA (81) preambulumbekezdése szerint ilyenkor mérlegelniük kell, hogy mennyire könnyen érthető kiskorúak számára a szolgáltatás kialakítása és működése, valamint, hogy szolgáltatásuk révén a kiskorúak mennyire lehetnek kitéve olyan tartalmaknak, amelyek károsak egészségükre, valamint fizikai, szellemi és erkölcsi fejlődésükre. Ilyen kockázatok merülhetnek fel például az olyan online interfészek kialakítása kapcsán, amelyek akár szándékosan, akár nem szándékoltan kihasználják a kiskorúak gyengeségeit és tapasztalatlanságát, vagy amelyek függő viselkedésformákat eredményezhetnek.

6.2.3 Ajánlórendszerek

Az ajánlórendszerek azok az algoritmusok, amelyek tartalmakat javasolnak a felhasználóknak az online platformokon. A DSA 3. cikk s) pontja úgy határozza meg az „ajánlórendszert", hogy az teljes mértékben vagy részben *automatizált rendszer,* amelyet az online platform arra használ, hogy az online interfészén konkrét információkat javasoljon vagy ezeket az információkat rangsorolja a szolgáltatás igénybe vevője számára, többek között a szolgáltatás igénybe vevője által indított keresés alapján vagy egyéb módon meghatározva a megjelenített információk relatív sorrendjét vagy elsőbbségét.

Az ajánlórendszerek gyakran profilalkotáson alapulnak, és nagy szerepük van abban, hogy milyen információkat látnak a felhasználók a platformon. A DSA 70. preambulumbekezdése hangsúlyozza, hogy az online platformok üzleti működésének központi eleme az információk priorizálása és megjelenítése az interfészen, például algoritmusokkal végzett javaslások, rangsorolások révén. Ezek a rendszerek nagyban befolyásolják a felhasználók

[93] vö. Domingos Soares Farinho, im. p. 52.
[94] Lásd NAIH hatásvizsgálati lista 20. pontját.

információkeresési képességét és interakcióit, javítva a felhasználói élményt és megkönnyítve a releváns információkhoz való hozzáférést. Ugyanakkor elősegítik bizonyos üzenetek terjesztését és az online viselkedés befolyásolását. Ezért a platformoknak világosan és könnyen érthetően tájékoztatniuk kell a felhasználókat arról, hogyan működnek ezek az ajánlórendszerek, beleértve a javasolt információk meghatározásának kritériumait, különösen, ha azokat profilalkotás és online viselkedés alapján rangsorolják.[95]

Az ajánlórendszerek vagy online hirdetések kapcsán a profilalkotás és a mikro-célzás kockázatait az Európai Adatvédelmi Biztos már felvetette az online manipulációról és a személyes adatokról szóló véleményében[96]. Az ajánlórendszerek személyes adatok kezelésével kapcsolatos relevanciája abban rejlik, hogy ezek a rendszerek gyakran a felhasználók személyes adatait használják fel az információk rangsorolásához, javaslásához és testreszabásához.[97] Az egyes platformok is a személyes relevanciával írják le az ajánlórendszerek célját[98]. Az ilyen rendszerek alapvetően profilalkotáson alapulhatnak, amely során a felhasználók viselkedési adatait (például korábbi keresések, interakciók, kedvelések, megtekintések) elemzik és dolgozzák fel annak érdekében, hogy releváns tartalmakat, hirdetéseket vagy szolgáltatásokat jelenítsenek meg. Az ajánló rendszerek szabályozása a DSA-ban értintetlenül hagyja az ezzel kapcsolatos kötelezettségeket a GDPR hatálya alatt, ideértve a jogalappal, tájékoztatással és automatizált döntéshozatallal kapcsolatos kérdéseket.

A DSA 27. cikk (1)-(2) bekezdése előírja, hogy az online platformok szerződési feltételeikben világosan le kell írniuk az ajánlórendszerek fő paramétereit, továbbá a felhasználóknak lehetőséget kell biztosítani a paraméterek befolyásolására vagy módosítására (vö. DSA 27. cikk (1)-(2) bekezdése). A DSA 27. cikk (3) bekezdése szerint amennyiben több opció is rendelkezésre áll szolgáltatás igénybe vevői számára megjelenített információk relatív sorrendjét meghatározó ajánlórendszerek tekintetében, az online platformot üzemeltető szolgáltatók hozzáférhetővé tesznek egy olyan funkciót is, amely lehetővé teszi a szolgáltatás igénybe vevője számára, hogy bármikor kiválassza és módosítsa az általa előnyben részesített opciót. Ehhez a funkcióhoz közvetlen és könnyű hozzáférést kell biztosítani az online platform online interfészének azon külön része felől, ahol az információk prioritási sorrendjét meghatározzák.

A DSA tehát az ajánlórendszereket szabályozza az összes online platform esetében, azonban külön szabályokat vezet be online óriásplatformok (VLOP) és nagyon népszerű online keresőprogramok (VLOSE) esetében a személyes adatok védelme érdekében. A DSA 38. cikk előírja, hogy ezeknek a szolgáltatóknak legalább egy olyan ajánlórendszer-opciót kell biztosítaniuk, amely nem alapul profilalkotáson a GDPR 4. cikk 4. pontja alapján. Bár a

[95] vö. Müller-Terpitz / Köhler- DSA Kommentar – Artikel 27. Rn 13; p. 327.

[96] Lásd az EDPS 3/2018 sz. véleménye az online manipulációról és a személyes adatokról, 2018. március 19., p. 9., „*Manipulation also takes the form of microtargeted, managed content display which is presented as being most 'relevant' for the individual but which is determined in order to maximise revenue for the platform. This is akin to the 'secret menus' used to steer users of ecommerce sites and the 'dark patterns' used to dissuade decisions less desirable from the platform's perspective (such as declining to add additional items, like insurance, to a shopping cart*)."); lehívás: 2024.09.14

[97] vö. Marta Micheli, Modeling User Personality Traits for Recommender Systems, Conference Paper, January 2023; Conference: CHItaly 2023 - Crossing HCI and AI; lehívás: 2024.09.14

[98] vö. Facebook feed recommendations AI system; June 21, 2024; lehívás: 2024.09.14

profilalkotás önmagában nincs teljesen megtiltva, az a szabály, hogy a felhasználók ne legyenek kizárólag profilalkotáson alapuló ajánlórendszereknek kitéve, fontos lépés a profilozás káros hatásainak csökkentésére. Ez azt jelenti, hogy VLOP és VLOSE esetében nem lehet kizárólag profilozás alapján működő ajánlórendszereket használni. Megjegyzendő, hogy az Európai Adatvédelmi Biztos a DSA-ról szóló véleményében ezt a szabályt valamennyi online platformra javasolta kiterjeszteni és az opt-out helyett kizárólag opt-in alapján lehetővé tenni.[99] Ez a DSA szabály a személyes adatok felhasználásának korlátozását célozza, és összhangban van a GDPR 21. és 22. cikkeivel.[100] VLOP-k és VLOSE esetében a DSA 34. cikk szerinti kockázatértékelés dönti el, hogy az ajánlórendszerek szigorúbb alkalmazása indokolt-e a DSA 35. cikke alapján.

6.3 Online interfész design – sötét tervezési minták

A DSA 25. cikke egy újabb védelmi réteget, egy generálklauzulát[101] vezet be a manipulációs vagy megtévesztő tervezési elemekkel, az úgynevezett "dark patterns" gyakorlatokkal szemben. Ez a rendelkezés kapcsolatban áll a DSA 31. cikkével, amely a „beépített megfelelés a kialakítás által” cím alatt olyan online platformot üzemeltető szolgáltatók interfész kialakítására vonatkozó kötelezettségeit rögzíti, amely lehetővé teszi a fogyasztók számára, hogy távollevők közötti szerződéseket kössenek a kereskedőkkel.

Az Európai Adatvédelmi Testület a közösségimédia-platform interfészein található sötét megoldásokról szóló iránymutatása rámutat arra, hogy a GDPR rendelkezései a személyes adatok teljes kezelési folyamatára vonatkoznak, beleértve a közösségi média platformok interfészeinek tervezését és működését is.[102] Ezek a szabályok összhangban állnak a GDPR 25. cikke szerinti beépített és alapértelmezett adatvédelemre vonatkozó szabályaival. A sötét tervezési gyakorlatok gyakran sértik a GDPR tisztességes eljárásra vonatkozó követelményét, a tisztességtelen kereskedelmi gyakorlatokról szóló irányelv[103] és annak tagállami átültető rendelkezéseit, illetőleg a jóhiszemű és tisztességes eljárás polgári jogi követelményét, ezért jogellenesnek minősülnek.

A DSA nem vezet be külön szabályokat a GDPR-hoz képest, és ennek megfelelően a DSA 25. cikk (1) bekezdése kimondja, hogy online platformot üzemeltető szolgáltatók nem tervezhetik vagy működtethetik a felületüket úgy, hogy megtévesszék vagy manipulálják a felhasználókat, vagy torzítsák a döntéshozatali képességüket. Ez a szabály kiterjed minden felhasználói interakcióra. A DSA 25. cikk második bekezdése azonban kimondja, hogy ez a tilalom a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlatokról szóló 2005/29/EK irányelv vagy a GDPR hatálya alá tartozó gyakorlatokra nem alkalmazandó. A DSA alkalmazása kiegészíti az adatvédelmi szabályozási követelményeket azáltal, hogy lefedi azokat az eseteket, ahol a személyes adatok nem érintettek, vagy a GDPR, illetve a fogyasztókkal szembeni

[99] EDPS Opinion 1/2021 on the Proposal for a Digital Services Act; 73-74. sarokpontok; 16-17. oldal
[100] vö. Domingos Soares Farinho, im. p. 53.
[101] vö. Müller-Terpitz / Köhler- DSA Kommentar – Artikel 25. Rn 11; p. 308.
[102] Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them; p. 4.
[103] Az Európai Parlament és a Tanács 2005/29/EK irányelve (2005. május 11.) a belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól, valamint a 84/450/EGK tanácsi irányelv, a 97/7/EK, a 98/27/EK és a 2002/65/EK európai parlamenti és tanácsi irányelvek, valamint a 2006/2004/EK európai parlamenti és tanácsi rendelet módosításáról („Irányelv a tisztességtelen kereskedelmi gyakorlatokról”) (EGT vonatkozású szöveg); HL L 149., 2005.6.11, p. 22–39

tisztességtelen kereskedelmi gyakorlatokra vonatkozó szabályok nem védik a felhasználókat. A DSA hatálya alatt azonban sötét tervezési minták tilalma szélesebb körű, mint más jogszabályokban, mert tilalom kiterjed azokra az esetekre is, amikor üzleti felhasználóknak (üzletfeleknek) jelenítenek meg sötét mintákat. A DSA 25. cikk (3) bekezdése konkrétan nevesít is egyes sötét mintákat, így (a) egyes választási lehetőségek kiemelése a szolgáltatás igénybe vevőjének döntésre való felkérésekor; (b) a szolgáltatás igénybe vevőjének ismételt felkérése valamely választásra olyan kérdésben, amellyel kapcsolatban már döntést hozott, különösen a felhasználói élményt zavaró felugró ablak alkalmazásával; (c) a szolgáltatás megszüntetésére irányuló eljárásnak az előfizetési eljárásnál nehezebbé tétele és felhatalmazza a Bizottságot, iránymutatást adjon ki a DSA 25. cikk (1) bekezdés alkalmazását illető konkrét gyakorlatokól. A sötét megoldásokra vonatkozó szabályokat a rendelet tiltott gyakorlataira kell alkalmazni, amennyiben ezek nem tartoznak tisztességtelen kereskedelmi gyakorlatokról szóló irányelv vagy a GDPR hatálya alá (vö. DSA 25. cikk (2) bekezdése), ami ezáltal hatályában korlátozza a 25. cikk alkalmazhatóságát azokra a felhasználókra, akik nem minősülnek fogyasztóknak. Lényeges, hogy a DSA 25. cikk nem szabályozza e cikk megsértésére irányadó jogkövetkezményeket, ezért a DSA 52. cikke alapján a tagállami jog határozza meg ezt.[104]

6.4 Különös adatvédelmi kötelezettégek VLOP és VLOSE esetében

A DSA különleges adatvédelmi kötelezettségeket határoz meg online óriásplatformok (VLOP) és nagyon népszerű online keresőprogramok (VLOSE) számára, amely szabályozás azon online platformokra és online keresőprogramokra alkalmazandó, amelyek havonta átlagosan legalább 45 millió, a szolgáltatást aktívan igénybe vevővel rendelkeznek az Unióban[105], amely független a platform által generált nettó árbevétel összegétől és melyeket az Európai Bizottság a DSA 33. cikk (4) bekezdésében rögzített eljárásnak megfelelően határozattal ekként azonosít[106]. E szabályozás célja a felhasználók adatainak védelme és a platformok működésének nagyobb átláthatósága. Ezek a kötelezettségek több területre terjednek ki, és szoros kapcsolatban állnak a GDPR által meghatározott elszámoltathatósági követelményekkel.

Az érintett szolgáltatók a DSA 34. cikke alapján *magas kockázatú rendszerüzemeltetőnek* minősülnek[107] és ennek megfelelően legalább évente el kell végezniük egy kockázatértékelést, amely során azonosítják a rendszereik által jelentett potenciális rendszerszintű kockázatokat, ideértve a felhasználók személyes adatainak védelmével kapcsolatos kockázatokat is. Ezen túlmenően a DSA 35. cikkének megfelelően *kockázatcsökkentési intézkedéseket* kell hozniuk a felhasználók jogainak védelme érdekében, beleértve a személyes adatok kezelését is. Ez a GDPR alapján hatásvizsgálati kötelezettséget jelent ezen szolgáltatók számára. Az adatvédelmi hatásvizsgálat célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, valamint a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelésének elősegítése e kockázatok értékelésével és a kezelésükre szolgáló intézkedések meghatározásával. A GDPR 34. cikke és a DSA 35. cikke sem írja elő azonban a kockázat teljes elkerülését, mivel csupán kockázatcsökkentő intézkedések megtételére kötelezi az adatkezelőt. A DSA (86) preambulumbekezdése szerint minden elfogadott intézkedésnek tiszteletben kell tartania az ebben a rendeletben meghatározott kellő

[104] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 25. Rn 25; p. 309.
[105] vö. DSA 33. cikk (1) bekezdés
[106] Az eddig azonosított VLOP és VLOSE szolgáltatók listája itt elérhető; hozzáférés: 2024.09.15.
[107] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 35. Rn 5; p. 410.

gondossági követelményeket, illetve hatékonyan és megfelelően csökkentenie kell a konkrét és azonosított rendszerszintű kockázatokat. Az intézkedéseknek arányosnak kell lenniük az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatók gazdasági kapacitásával, valamint a szolgáltatásaik használatával kapcsolatos szükségtelen korlátozások elkerülésének szükségességével, és kellően figyelembe kell venniük az alapvető jogokra gyakorolt esetleges negatív hatásokat. A DSA 35. cikk (3) bekezdése értelmében az EU Bizottság iránymutatást adhat ki VLOP és VLOSE szolgáltatók által az egyes kockázatokkal kapcsolatban elfogadandó kockázatcsökkentő intézkedésekről. Az EU Bizottság eddig a választási folyamatokat érintő rendszerszintű kockázatok csökkentésére vonatkozó iránymutatásokról adott ki közleményt[108], amely szerint a kockázatcsökkentő intézkedéseknek figyelembe kell venniük a személyes adatok védelméhez való jogot, különös tekintettel a választási folyamatokkal kapcsolatos adatkezelésre és a dezinformáció kezelésére, illetőleg az adatokhoz való hozzáférésre.

Az *ajánlórendszerek átláthatósága* szintén kiemelt terület. A VLOP-ok és VLOSE-ok kötelesek legalább egy olyan ajánlórendszer opciót biztosítani, amely nem alapul profilalkotáson. Ennek a rendszernek világos és érthető információkat kell nyújtania a felhasználóknak arról, hogy milyen paraméterek alapján ajánlanak tartalmakat, és a felhasználók milyen lehetőségekkel rendelkeznek ezek módosítására. Az online hirdetések transzparenciája szempontjából a platformok kötelesek feltüntetni, hogy ki a reklám megrendelője, és milyen paraméterek alapján jelenítik meg a reklámokat a felhasználók számára. A VLOP-ok ezen kívül egy nyilvános hirdetési adattárat is létre kell hozniuk, amelyben dokumentálniuk kell minden reklámot, beleértve az adatokat, amelyeket a célzáshoz használnak.

A VLOP-oknak és VLOSE-oknak a DSA 37. cikke alapján saját költségükön és évente legalább egyszer független ellenőrzést (auditokat) kell végezniük, amelyek során felülvizsgálják a platformok által alkalmazott adatvédelmi intézkedéseket és a kockázatcsökkentési stratégiákat. Az audit eredményeit nyilvánosságra kell hozni, hogy biztosítsák a platformok működésének átláthatóságát. A VLOP-oknak és VLOSE-oknak ezt meghaladóan közzé kell tenniük átláthatósági jelentéseket, amelyek tartalmazzák az automatizált tartalommoderációs rendszerek, az ajánlórendszerek és a hirdetési tevékenységeik működésével kapcsolatos információkat.

A VLOP-oknak és VLOSE-oknak a DSA 41. cikke alapján létre kell hozniuk egy *független compliance funckiót*, azaz az operatív egységektől elkülönülő, a megfelelést támogató olyan szervezeti egységet, amely egy vagy több megfelelési tisztviselőből áll, beleértve a megfelelést támogató szervezeti egység vezetőjét is, amely a rendelkezik e feladatok ellátásához szükséges szakmai képesítéssel, ismeretekkel, tapasztalattal és képességgel. Ennek a megfelelést támogató egységnek megfelelő autoritással, státusszal és erőforrásokkal, valamint az online óriásplatformot vagy nagyon népszerű online keresőprogramot üzemeltető szolgáltató vezető testületéhez való hozzáféréssel kell rendelkeznie annak ellenőrzéséhez, hogy az adott szolgáltató megfelel-e a DSA követelményeinek, ideértve azt, hogy a VLOP és VLOSE esetében valamennyi kockázatot azonosítsanak és megfelelően beszámoljanak róluk, valamint hogy a DSA 35. cikkel összhangban észszerű, arányos és hatékony kockázatcsökkentési intézkedéseket hajtsanak végre, melynek ki kell terjednie a rendszerszintű adatvédelmi kockázatokra is.

[108] European Commission Guidelines for providers of VLOPs and VLOSEs on the mitigation of systemic risks for electoral processes, Publication 26 April 2024; lehívás: 2024.09.15

Általánosan kijelenthető, hogy a DSA alapján ezen kötelezettségek célja, hogy online óriásplatformok és nagyon népszerű online keresőprogramok működését átláthatóbbá tegyék, és magasabb szintű védelmet biztosítsanak a felhasználók személyes adatainak kezelése során, különös tekintettel a GDPR követelményeinek való megfelelésre, ami az elszámoltathatósággal kapcsolatos többletkövetelményt jelentenek ezen szolgáltatók számára, melyek jelentéstételi és transzparencia kötelezettségekkel párosulnak. Megjegyzendő, hogy az Európai Bizottság a DSA alkalmazandóvá válása óta számos eljárást indított VLOP és VLOSE szolgáltatókkal szemben[109] a DSA feltehető megsértése miatt.

6.5 ADATOKHOZ VALÓ HOZZÁFÉRÉS ÉS KUTATÓK HOZZÁFÉRÉSE

A DSA 40. cikke értelmében az online óriásplatformok (VLOP) és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók (VLOSE) kötelesek hozzáférést biztosítani a digitális szolgáltatási koordinátorok vagy a Bizottság számára a jogszabályoknak való megfelelés nyomon követéséhez szükséges adatokhoz. Ezen adatok kizárólag a jogszabályi előírások teljesítésének ellenőrzésére használhatók fel, miközben figyelembe kell venni az érintett felhasználók és szolgáltatók jogait, beleértve a személyes adatok védelmét, az üzleti titkok és a szolgáltatás biztonságának védelmét is. Ellenőrzött kutatók („vetted researcher"), és megfelelnek a meghatározott feltételeknek így kutatóhelyhez tartoznak és közérdekű tudományos kutatást végeznek, szintén hozzáférést kérhetnek a digitális szolgáltatási koordinátor útján a VLOP és a VLOSE platform adataihoz, hogy olyan kutatásokat végezzenek, amelyek hozzájárulnak a DSA 34. cikk (1) bekezdése szerint meghatározott, az Unióban felmerülő rendszerszintű kockázatok felderítéséhez, azonosításához és megértéséhez, valamint a 35. cikk szerinti kockázatcsökkentési intézkedések megfelelőségének, hatékonyságának és hatásainak értékeléséhez[110] és melyet ezt követően a szabályozó hatóságok a szolgáltatók ellenőrzésére felhasználhatnak.

Az ellenőrzött kutatók tevékenységének megértéséhez elengedhetetlen az általuk végzett tevékenység megértése és a tudományos kutatás fogalmának elemzése. A *tudományos kutatás fogalmát*[111] a GDPR mindazonáltal nem határozza meg, azonban az ilyen célú adatkezeléseket a GDPR szabályozza és privilegizálja, azaz bizonyos kivételeket és korlátozásokat ír elő az adatvédelmi követelmények alól. A GDPR 5. cikk (1) bekezdés b) pontja a célhoz kötöttség elvét rögzíti, és előírja, hogy a személyes adatokat csak meghatározott, egyértelmű és jogszerű célokra lehet kezelni. A személyes adatokat nem lehet olyan célokra tovább kezelni, amelyek nem egyeztethetők össze az eredeti célokkal. Azonban vélelmezhető, hogy a kutatás egy kompatibilis másodlagos cél (a „*kompatibilitás vélelme*"). A tagállami jog feltételeket szabhat ennek a vélelemnek a használatához. A korlátozott tárolhatósággal kapcsolatosan a GDPR 5. cikk (1) bekezdés e) pontja tartalmaz egy mentességet a kutatások számára, amely lehetővé teszi az adatok „hosszabb ideig" történő tárolását, ha azok minősített kutatási célokra kerülnek feldolgozásra. Az, hogy a „hosszabb idő" megfelelő-e, az adott tudományos kutatási projekt

[109] Supervision of the designated very large online platforms and search engines under DSA; lehívás: 2024.09.15

[110] vö. DSA 40. cikk (4) bekezdése

[111] vö. a tudományos kutatás fogalmáról lásd a német DSK iránymutatását - Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. September 2024 - DS-GVO privilegiert wissenschaftliche Forschung, Positionspapier zum Begriff „wissenschaftliche Forschungszwecke"; 11. September 2024, lehívás: 2024.09.19

sajátosságaitól függ. Átláthatósági kötelezettségekkel kapcsolatosan a GDPR 14. cikk (5) bekezdés b) pontja mentességet biztosít, ha az adatokat nem közvetlenül az érintettől szerzik be és a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne, különösen tudományos kutatási célból. Végül a GDPR 17. cikk (3) bekezdés d) pontja kimondja, hogy a törléshez való jog nem alkalmazandó, ha annak érvényesítése „lehetetlenné tenné vagy súlyosan akadályozná" a kutatási célkitűzések elérését, ha az adatkezelés a GDPR 89. cikk (1) bekezdésével összhangban történik. A GDPR 21. cikk (6) bekezdése mentességet biztosít a tiltakozáshoz való jog alól, ha az adatkezelés a közérdekű feladat ellátásához szükséges. A GDPR 89. cikk (1) bekezdése pedig tudományos kutatási célból folytatott adatkezelésre vonatkozó garanciákat és eltéréseket rögzíti. E garanciáknak biztosítaniuk kell, hogy olyan technikai és szervezési intézkedések legyenek érvényben, melyek biztosítják különösen az adattakarékosság elvének betartását. Ezen intézkedések közé tartozhat az álnevesítés, amennyiben az említett célok ily módon megvalósíthatók. Amennyiben e célok megvalósíthatók az adatok oly módon történő további kezelése révén, amely nem vagy már nem teszi lehetővé az érintettek azonosítását, a célokat ilyen módon kell megvalósítani.

Annak megállapításához, hogy egy kutatásra a fent bemutatott privilegizált szabályok alkalmazhatók-e, meg kell vizsgálni, hogy az adatkezelés valóban tudományos kutatási célból történik-e. Ez általában csak egyedi eseti értékelés alapján lehetséges. A GDPR (159) preambulumbekezdése szerint a GDPR alkalmazásában a személyes adatok tudományos kutatási célú kezelését tágan kell értelmezni, oly módon, hogy az magában foglalja többek között a technológiafejlesztési és demonstrációs tevékenységeket, az alapkutatást, az alkalmazott kutatást, és a magánfinanszírozású kutatást is. Ahhoz, hogy az adatkezelés megfeleljen a személyes adatok tudományos kutatási célú kezelésére vonatkozó jellemzőknek, speciális feltételeknek kell eleget tenni különösen a személyes adatok tudományos kutatási célok keretében történő közzétételére vagy egyéb nyilvánosságra hozatalát illetően. A DSA 40. cikke egyensúlyt kíván teremteni a kutatási célú adathozzáférés és a személyes adatok védelme között. A DSA kontextusában az ellenőrzött kutatók kutatóként és kvázi-ellenőrnek is tekinthetők: képesek új és felmerülő kockázatokat felfedezni, amelyek esetleg nem szerepeltek a vállalat kockázatértékelési jelentésében, valamint értékelni, hogy az önszabályozó kezdeményezések a gyakorlatban hatékonyak voltak-e a konkrét kockázatok mérséklésében.[112]

A DSA 40. cikk (7) bekezdése rögzíti az online óriásplatformot vagy nagyon népszerű online keresőprogramot üzemeltető szolgáltatók azon kötelezettségét elő kell segíteniük és biztosítaniuk kell az adatokhoz való, hozzáférést a kérelemben megadott megfelelő interfészeken keresztül, ideértve az online adatbázisokat vagy az alkalmazásprogramozási felületeket (API) is. A szabályozás lényege, hogy azon kutatóknak, akik kutatást kívánnak végezni az Európai Unióban felmerülő rendszerszintű kockázatok felderítése, azonosítása és megértése érdekében, a 40. cikk különböző hozzáférési lehetőségeket biztosít. A DSA 40. cikk (12) bekezdése alapján a kutatók, beleértve a nonprofit szervezetekhez, testületekhez és egyesületekhez kapcsolódókat is, ha megfelelnek a vonatkozó feltételeknek, hozzáférést kaphatnak a VLOP-ok és VLOSE-ok online interfészén nyilvánosan elérhető adatokhoz. A (4) bekezdés szerint a további feltételeknek megfelelő kutatók kérelmezhetik a VLOP-ok és VLOSE-ok nem nyilvános adatainak elérését, az erre vonatkozó adat-hozzáférési kérelmet benyújtva

[112] Mathias Vermeulen - Researcher Access to Platform Data: European Developments Journal of Online Trust and Safety, p. 3.; lehívás: 2024.09.15

az illetékes digitális szolgáltatási koordinátorhoz (DSC). A DSA előtt az ilyen típusú adatokhoz való hozzáférés, amely független kutatásokat tett lehetővé, eddig az online platformszolgáltatók önkéntes kezdeményezésein alapult. Ennek eredményeként azonban harmadik felek számára alapvetően korlátozottak voltak a kutatási lehetőségek a platformszolgáltatók döntéseinek az online ökoszisztémára gyakorolt hatásának elemzésére és nyomon követésére.[113]

Az ellenőrzött státusz megszerzésére vonatkozó feltételek teljesítését a digitális szolgáltatási koordinátor értékeli. A kutatók ellenőrzésére és az adatokhoz való hozzáférés biztosítására vonatkozó eljárások technikai részleteit egy felhatalmazáson alapuló jogi aktusban az Európai Bizottság fogja meghatározni, amelynek elfogadása jelenleg is folyamatban van[114]. A DSA (97) preambulumbekezdése egyértelművé teszi, hogy a szolgáltatók kereskedelmi érdekeinek figyelembevétele nem vezethet a konkrét kutatási célkitűzéshez a DSA szerinti kérelem alapján szükséges adatokhoz való hozzáférés megtagadásához.

A hozzáférési és adatszolgáltatási kötelezettségek szoros kapcsolatban állnak a személyes adatok védelmével, mivel az online platformok által gyűjtött és tárolt adatok gyakran tartalmazhatnak személyes adatokat a felhasználókról. A DSA tehát lehetőséget biztosít a kutatók számára, hogy platformadatokhoz férjenek hozzá, ugyanakkor megköveteli, hogy az adatkezelés során tiszteletben tartsák az érintettek adatvédelmi jogait, mivel előírja, hogy az adatkezelés során figyelembe kell venni a személyes adatok védelmére vonatkozó szabályokat. Ez azt jelenti, hogy a személyes adatokhoz való hozzáférés és azok felhasználása kutatók részéről csak a jogszabályoknak megfelelően történhet, például csak a jogszerű célok eléréséhez szükséges mértékben és időtartamban. A DSA ennek megfelelően kimondja, hogy az adatokhoz való hozzáférés nem veszélyeztetheti a személyes adatok védelmét vagy a felhasználók jogait, és az adatmegosztásnak meg kell felelnie a bizalmas információk, különösen az üzleti titkok és a szolgáltatás biztonságának védelmét szolgáló előírásoknak. A kutatói hozzáférés biztosítása során fontos a kutatás céljaival arányos adatkezelés. A VLOP-ok és VLOSE-ok nem akadályozhatják meg a kutatókat, akik megfelelnek bizonyos kritériumoknak, hogy nyilvánosan elérhető adatokat gyűjtsenek valós időben. Ez különösen fontos az algoritmikus rendszerek kutatásához szükséges automatikus adatgyűjtés szempontjából. A platformoknak megfelelő interfészeket, például API-kat kell biztosítaniuk a kutatók számára. A kutatóknak megfelelő adatvédelmi és biztonsági intézkedéseket kell alkalmazniuk, és az adatkezelésüknek az adatvédelmi és a bizalmas információk védelmére vonatkozó szabályoknak is meg kell felelnie. Emellett biztosítani kell, hogy az érintettek jogai ne sérüljenek, és hogy a kutatási célra használt adatok ne kerüljenek üzleti érdekek céljából felhasználásra. A szolgáltatóknak anonimizálniuk vagy álnevesíteniük kell a személyes adatokat, azon esetek kivételével, ha az elérni kívánt kutatási célt ez ellehetetlenítené.

A DSA hozzáférésre vonatkozó rendelkezéseit amiatt kritizálják[115], mivel az adathozzáférés csak olyan kutatás esetében lehetséges, amely „*hozzájárul az Unión belüli rendszerszintű kockázatok felderítéséhez, azonosításához és megértéséhez*” (vö. DSA 40. cikk (12) bekezdése),

[113] European Centre for Algorithmic Transparency - FAQs: DSA data access for researchers - lehívás: 2024.09.15
[114] European Commission - Delegated Regulation on data access provided for in the Digital Services Act; lehívás: 2024.09.15
[115] Iramina, Aline and Perel (Filmar), Maayan and Elkin-Koren, Niva, Paving the Way for the Right to Research Platform Data (June 19, 2023); p. 14.; lehívás: 2024.09.15

valamint a kockázatcsökkentő intézkedések hatékonyságának, megfelelőségének és hatásainak értékeléséhez. Bár a rendszerszintű kockázatok és a kockázatcsökkentő intézkedések tágan értelmezhetők, a DSA elsősorban a digitális platformok alapvető jogokra gyakorolt hatását vizsgáló kutatásokra koncentrál, nem pedig az általános kockázatokra, ami szűkíti a kutatási lehetőségeket.

7. Intézményi együttműködés a DSA hatálya alatt

Az európai uniós adatvédelmi szabályok (GDPR, ePrivacy irányelv) és a DSA végrehajtása, együttműködése, szankciói és ezek végrehajtása központi szerepet játszanak az európai digitális piac szabályozásában. Ezen jogszabályok egyaránt szigorú mechanizmusokat írnak elő az adatvédelem és a digitális platformok felelőssége és elszámoltathatósága terén. A GDPR és az ePrivacy irányelv az adatvédelmi szabályokat határozza meg, míg a DSA a digitális platformok működését és azok felelősségét szabályozza, biztosítva a biztonságos és átlátható digitális ökoszisztémát. A két szabályozás és annak végrehajtása közötti koordináció alapvető jelentőségű az uniós polgárok adatainak és jogainak védelme érdekében. Ezzel kapcsolatosan különös jelentősége van a Bundeskartellamt ügyben született EUB ítéletnek, amely kijelölte annak kereteit, hogy nem adatvédelmi hatóságok mennyiben vehetik figyelembe az adatvédelmi szabályozást a döntéseik során.

A GDPR végrehajtásáért a nemzeti adatvédelmi hatóságok és az Európai Adatvédelmi Testület (EDPB) felel, míg a DSA esetében a digitális szolgáltatási koordinátorok (DSC-k) és az Európai Bizottság látja el a felügyeleti feladatokat az online óriásplatformok (VLOP) és nagyon népszerű online keresőprogramok (VLOSE) felett. A szankciók súlyosak lehetnek, mivel a GDPR keretében éves globális árbevétel 2%-4%-ig terjedő bírságot lehet kiszabni, míg a DSA esetében pedig akár az éves globális árbevétel 6%-át is elérheti a bírság szankció, emellett egyéb jogkövetkezmények is alkalmazhatók, melyet a tagállami jog határoz meg a DSA 51. cikkének megfelelően, illetőleg adatvédelmi jogsértések esetében a GDPR 84. cikke alapján.

A DSA létrehozta a digitális szolgáltatási koordinátorok (DSC-k) intézményét, amelynek 2024. február 17. napjától kulcsfontosságú szerepe van a DSA végrehajtásában és amely hatáskörrel Magyarországon a Nemzeti Média- és Hírközlési Hatóságot (NMHH) nevezték ki és a Hatóságon belül, annak önálló hatáskörű szervei közül a Hatóság Elnöke gyakorolja az e hatáskörből eredő feladatokat. A digitális szolgáltatási koordinátor tevékenységére és eljárására vonatkozó általános szabályokat és az alkalmazható egyéb jogkövetkezményeket az internetes közvetítő szolgáltatások egyes szabályairól szóló 2023. évi CIV. törvény (Iszt.) rögzíti, ideértve a jogsértő magatartás tanúsításának megtiltását, a közvetítő szolgáltatót kötelezését a jogsértés megszüntetésére; közvetítő szolgáltató kötelezését közleménynek vagy a határozatnak az internetes honlapja nyitóoldalán való közzétételére a határozatban meghatározott módon és ideig, illetőleg bíróság döntése alapján szolgáltatáshoz való hozzáférés korlátozásának elrendelését, vagy a szolgáltatás felfüggesztésére kötelezést (vö. Iszt. 16. §).

A DSC-knek, illetőleg az Európai Bizottságnak a DSA adatvédelmileg releváns rendelkezései miatt az adatvédelmi hatóságokkal együttműködve kell eljárniuk, és emiatt indokolt a koordináció mind az egyes tagállamokon belül, mind azok között, valamint az Európai Bizottság és a tagállamok között a VLOP és VLOSE vonatkozásában, figyelemmel arra, hogy ezen együttműködés kereteit sem a DSA, sem a GDPR nem jelöli ki. Az uniós jogalkotó tehát új

intézményi keretet hozott létre, amely magában foglalja a DSC-ket, valamint egy független Digitális Szolgáltatások Európai Testületét (DSA Board, vö. DSA 61. – 63. cikkei)[116], ami a tagállamok digitális szolgáltatási koordinátoraiból áll, elnöke pedig az Európai Bizottság. Az Bizottság a DSA végrehajtó hatósága a VLOP és VLOSE szolgáltatók esetében, különösen a rendszerszintű kockázatok kezelésében, amelyek hatással lehetnek az alapvető jogok, például az emberi méltóság és a személyes adatok védelmére. A DSA előírja a kockázatértékelést, amely során ezeket az alapvető jogokat is figyelembe kell venni. Emellett a DSA 36. cikke válságreagálási mechanizmus bevezetését is lehetővé teszi, amely felhatalmazza a Bizottságot arra, hogy válsághelyzet fennállása esetén intézkedéseket írjon elő a platformok számára. A DSA szerinti új hatáskörök kiterjednek a tartalommoderálási eljárások ellenőrzésére, ami magában foglalhatja a személyes adatok kezelésének vizsgálatát is. Ez egy összetett intézményi rendszert eredményez, amely összehangolt együttműködést igényel a nemzeti adatvédelmi hatóságok és a DSC-k között. A Bizottság a VLOP és VLOSE esetében széleskörű vizsgálati és végrehajtási hatáskörökkel rendelkezik, és ezek az intézkedések szorosan kapcsolódnak a személyes adatok védelméhez.

A digitális szolgáltatásokról szóló csomagról és az adatstratégiáról szóló, 2021. november 18. napján kibocsátott nyilatkozatában[117] az Európai Adatvédelmi Testület kiemelte azokat a kockázatkatok, melyek a *felügyelet széttagoltságából* erednek a digitális szolgáltatások felügylete területén. Az Európai Adatvédelmi Testület emlékeztetett arra, hogy a személyes adatok védelmét és szabad áramlását illetően az EUMSZ 16. cikkének (2) bekezdése és az Európai Unió Alapjogi Chartája 8. cikkének (3) bekezdése előírja, hogy a személyes adatok kezelésének felügyeletét független adatvédelmi hatóságokra kell bízni. Így konkrétan a DSA esetében kiemelte, hogy az előírja az illetékes hatóságok számára, hogy felügyeljék az online óriásplatformok ajánlórendszereit (amelyek gyakran a GDPR értelmében vett érintettekről történő profilalkotást foglalják magukban); valamint a rendszerszintű kockázatok értékelése és mérséklése érdekében hozott intézkedéseket, beleértve a magánélet tiszteletben tartásához való jogot érintő kockázatokat is. Ugyanez tartalmaz olyan magatartási kódexekre vonatkozó rendelkezéseket is, amelyek személyes adatok kezelésére vonatkozhatnak. Ugyanakkor nem írja elő az illetékes hatóságok számára, hogy hivatalosan konzultáljanak vagy együttműködjenek az Európai Adatvédelmi Testülettel, vagy annak tagjaival. Ez azzal a kockázattal jár, hogy *egymásnak ellentmondó iránymutatás vagy akár eltérő eredmények születnek* a felügyeleti hatóságok jogérvényesítési intézkedéseiben. A jogalkotási folyamat során benyújtott módosítások azonban nem enyhítették a jogbizonytalansággal kapcsolatos aggodalmakat, mivel jelentős átfedési lehetőség van a DSA alkalmazási köre és a meglévő adatvédelmi jogszabályok között, azaz a felügyelet széttagoltsága továbbra is megmaradt. Másrészről az Európai Adatvédelmi Testület nyilatkozata azt is kiemelte, hogy egyes DSA rendelkezések ugyanazt a terminológiát használják, mint GDPR vagy az ePrivacy irányelv, a fent említett jogszabályokra való kifejezett hivatkozás nélkül. Ez azzal a kockázattal jár, hogy befolyásolja a GDPR alapfogalmainak (például a „hozzájárulás" vagy az „érintett" kulcsfogalmainak) értelmezését. Azzal a kockázattal is jár, hogy bizonyos rendelkezések a GDPR-tól vagy az ePrivacy irányelvtől eltérő rendelkezésekként értelmezhetők. Következésképpen egyes rendelkezések könnyen értelmezhetők a meglévő jogi kerettel

[116] Digitális Szolgáltatások Európai Testülete; legívás: 2024.09.15

[117] Európai Adatvédelmi Testület - Nyilatkozat a digitális szolgáltatásokról szóló csomagról és az adatstratégiáról - Az elfogadás időpontja: 2021. november 18., lehívás: 2024.09.15

összeegyeztethetetlen módon, és ebből következően jogbizonytalansághoz vezethetnek.[118] Annak ellenére, hogy a DSA rögzíti, hogy az adatvédelmi szabályok alkalmazását nem érinti, nem lesz könnyű feladat elkerülni az eltéréseket ezen új jogszabályok és a GDPR, valamint más adatvédelmi jogszabályok együttes értelmezésében és alkalmazásában.[119]

A DSA és a GDPR (és az ePrivacy irányelv) együttes alkalmazásával és a hatóságok együttműködésével kapcsolatosan lényeges megállapításokat rögzít az Európai Bíróság a *Meta Platforms Inc. és társai kontra Bundeskartellamt* ügyben hozott 2023-as ítélete[120]. Ez az ítélet azért lényeges, mert kijelölte annak kereteit, hogy nem adatvédelmi felügyeleti hatóságok mennyiben játszhatnak szerepet az európai uniós adatvédelmi követelmények érvényesítésében, figyelemmel arra, hogy sem az általános adatvédelmi rendelet, sem más uniós jogi aktus nem ír elő konkrét szabályokat a nemzeti versenyhatóság és az érintett nemzeti felügyeleti hatóságok vagy a fő felügyeleti hatóság közötti együttműködésre vonatkozóan, ezért az ítélet megállapításai a digitális szolgáltatási koordinátorok eljárására is alkalmazandó, amennyiben személyes adatok kezelésével kapcsolatos kérdéseket szükséges vizsgálniuk hatósági eljárás során. Az Európai Bíróság ebben a döntésében elismerte, hogy az adatvédelmi és versenyhatóságok különböző feladatokat látnak el, de a versenyhatóság vizsgálhatja, hogy egy vállalkozás magatartása megfelel-e a GDPR-nak, amennyiben ez szükséges az erőfölénnyel való visszaélés megállapításához.

A Bíróság hangsúlyozta, hogy a nemzeti versenyhatóságok nem helyettesíthetik az adatvédelmi felügyeleti hatóságokat, és együttműködésre van szükségük velük a GDPR egységes alkalmazásának biztosítása érdekében. A versenyhatóság nem térhet el az adatvédelmi hatóság döntéseitől, és konzultálnia kell az érintett felügyeleti hatóságokkal, ha kétségei vannak a GDPR alkalmazásával kapcsolatban. Ez a döntés példaértékű az adatvédelmi hatóságok és egyéb felügyeleti hatóságok közötti együttműködés tekintetében. A GDPR és a DSA közötti szoros kapcsolat miatt szükség lehet arra, hogy a digitális szolgáltatásokat felügyelő hatóságok (DSC-k) együttműködési megállapodásokat kössenek az adatvédelmi hatóságokkal az egységes jogalkalmazás érdekében. A DSA intézményi keretei a fentiek fényében fontos szerepet játszanak nemcsak a digitális platformok szabályozásában, hanem az adatvédelem biztosításában is, mellyel kapcsolatosan az adatvédelmi felügyeleti hatóságokkal való együttműködés az elvárás, figyelemmel a lojális együttműködés e kötelezettségére. Az újonnan létrehozott DSC-k tehát szabályozó hatóságként csak úgy működhetnek, ha figyelembe veszik az Európai Bíróság joggyakorlatában megállapított követelményeket, ami fokozott együttműködést igényel a tagállamok és az Európai Bizottság, az Európai Adatvédelmi Testület és a tagállami felügyeleti hatóságok között.

8. VÉGKÖVETKEZTETÉSEK ÉS SZAKMAI JAVASLATOK

A kutatásunkban bemutattuk, hogy egyrészt a DSA *lex specialis* szerepet tölt be a GDPR-ral és az ePrivacy irányelv szabályaival szemben, másrészt kiegészíti annak rendelkezéseit. Ezért elemeztük a platformok adatkezelésével szabályozásával kapcsolatos szabályozási igényt; az

[118] Európai Adatvédelmi Testület - Nyilatkozat a digitális szolgáltatásokról szóló csomagról és az adatstratégiáról, A következetlenségből fakadó kockázatok, 6. oldal

[119] vö. Zanfir-Fortuna, Gabriel im p 11.

[120] Európai Unió Bírósága, C-252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság (ECLI:EU:C:2023:537); lehívás: 2024.09.15

adatvédelmi jogszabályok és a DSA alkalmazását ezekre; (3) azt, hogy a DSA milyen új adatvédelmi követelményeket támaszt platformok részére és (4) az új intézményi keretet, amely az adatvédelmi hatóságokkal a lojalitás elve alapján szorosan együttműködve szabályozza az online platformok adatkezelését.

A DSA szerint az online platformok és keresőprogramok adatkezelők (és esetenként adatfeldolgozók) a GDPR értelmében, ezért a GDPR 6. cikk (1) bekezdése alapján jogszerű adatkezelést kell folytatniuk. A DSA új jogi kötelezettségeket határoz meg, különösen a tartalommoderáció és eljárási szabályok tekintetében, a kiskorúak jogai védelmében, és együtt alkalmazandó az adatvédelmi jogszabályokkal. A DSA kifejezetten szabályozza a sötét tervezési minták tilalmát, amely megerősíti az adatvédelmet, és elősegítheti vagy éppen korlátozhatja a személyes adatok védelmét a GDPR-ral összhangban. A DSA továbbá szigorítja a profilalkotás és célzott hirdetések szabályozását, különösen a kiskorúak és különleges kategóriájú személyes adatok használata esetén. A legnagyobb online platformok (VLOP) és keresőprogramok (VLOSE) számára pedig kötelezővé teszi, hogy nem csak profilalkotáson alapuló ajánlórendszert kínáljanak, hanem profilozás nélküli alternatívát is biztosítsanak, továbbá VLOP és VLOSE üzemeltetők esetében biztosítja azt, hogy kutatók is ellenőrizhessék és azonosíthassák a rendszerszintű kockázatokat.

Az *intézményi együttműködés* szempontjából a DSA új intézményi keretet is kialakít, amely a tagállamokban a digitális szolgáltatási koordinátorainak szerepét erősíti, amelyek adatvédelmi felügyeleti hatáskörbe tartozó kérdésekkel is találkozhatnak. Ez az új keret koordinációt igényel a GDPR felügyeleti hatóságai és a digitális szolgáltatási koordinátorok között. A tanulmány arra is rámutat, hogy további elemzések szükségesek, különösen a sötét tervezési minták, jogok gyakorlása és intézményi együttműködés területén a GDPR és a DSA összefüggéseiben.

Az *európai uniós adatvédelmi szabályozás és a DSA közötti kölcsönhatás* vizsgálata során lényeges, hogy harmonikus és koherens szakpolitikai ajánlások szülessenek, amelyek erősítik az adatvédelmet, valamint előmozdítják az átláthatóságot és a felhasználói jogokat a DSA területén. Az együttműködés javítása érdekében elengedhetetlen, hogy a digitális szolgáltatási koordinátorok és az adatvédelmi hatóságok közötti kapcsolatok világos keretek között működjenek, ezáltal lehetőség szerint elkerülve a párhuzamos eljárásokat. A kötelezettségek összehangolására vonatkozó iránymutatások megalkotása segíthet az adatvédelmi szabályozás és a DSA közötti átfedések pontosabb kezelésében, különös figyelmet fordítva a személyes adatok védelmére és az algoritmikus döntéshozatal átláthatóságára.

A DSA előírja az *algoritmikus átláthatóság* biztosítását, míg a GDPR kifejezetten a személyes adatok kezelésének átláthatóságára helyezi a hangsúlyt. Ezen szabályok átfedik egymást és az ennek való megfelelés érdekében a platformoknak világosan kell kommunikálniuk, hogyan kezelik a személyes adatokat a döntéshozatali algoritmusok alkalmazása és fejlesztése során. A felhasználóknak jogot kell biztosítani arra, hogy megértsék az automatizált döntéshozatal logikáját és az adatvédelmi következményeket, így javasolt lenne harmonizált iránymutatások kibocsátása ezzel kapcsolatosan e két szabályozás keretein belül.

A *kockázatértékelés* mindkét jogszabályban középpontban áll, ami lehetővé teszi a rendszerszintű és adatvédelmi kockázatok holisztikus kezelését. A DSA rendszerszintű kockázatkezelési kötelezettségei és a GDPR adatvédelmi hatásvizsgálatok közötti kapcsolat

tisztázása elősegítené a megfelelést, valamint hozzájárulna a kockázatok hatékonyabb csökkentéséhez. Ezen kívül a tartalommoderálás és az adatvédelmi jogok egyensúlyának megteremtése érdekében hatósági iránymutatásokra van szükség, amelyek biztosítják, hogy a platformok tiszteletben tartsák a felhasználói jogokat, miközben megfelelnek a DSA előírásainak is.

A *hirdetések átláthatósága és a célzott hirdetések szabályozása* terén a DSA és a GDPR közötti kapcsolat megerősítése is elengedhetetlen. A platformoknak ösztönözniük kell az adatminimalizálás elveit, különösen a viselkedési adatok gyűjtése és felhasználása terén.

Végül, a tudatos felhasználói szokások kialakítása érdekében javasolt lenne a digitális szolgáltatási koordinátorok és adatvédelmi felügyeleti hatóságok általi közös *tudatosságnövelő kampányok* megfontolása mind a felhasználók, mind az online platform üzemeltetők felé hangsúlyozva az egyes kötelezettségeket és felhasználói jogokat.

Felhasznált szakirodalom

- Müller-Terpitz / Köhler: Digital Services Act: DSA - Gesetz über digitale Dienste; Kommentar; 2024; XXVII, 860 S. C.H.BECK. ISBN 978-3-406-79878-8
- Koltay András, Szikora András, Lapsánszky András, Tóth András (szerk.) - Nagykommentár a DSA rendelethez, Wolters Kluwer, 2024; 7. cikk; 77. oldal
- Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), Datenschutzrecht. DSGVO mit BDSG (Nomos 2019), 1. Auflage
- Domingos Soares Farinho: Personal Data Processing by Online Platforms and Search Engines: The Case of the EU Digital Services Act; Public Governance, Administration and Finances Law Review Vol. 9. No. 1. (2024) •37–58.; Online: https://folyoirat.ludovika.hu/index.php/pgaf/article/view/7134/5939
- Kurtz, C., Wittner, F., Semmann, M., Schulz, W. & Böhmann, T. (2022). Accountability of Platform Providers for Unlawful Personal Data Processing in Their Eco-Systems – A Socio-Techno-Legal Analysis of Facebook and Apple's iOS According to the GDPR. Journal of Responsible Technolog y, 9. Online: https://www.sciencedirect.com/science/article/pii/S2666659621000111?via%3Dihub
- Mathias Vermeulen: Researcher Access to Platform Data : European Developments; Journal of Online Trust and Safety, September 2022, page 1-9; Stanford Internet Observatory , 2022 Online: https://tsjournal.org/index.php/jots/article/view/84/31
- Zanfir-Fortuna, Gabriela, Follow the (personal) Data: Positioning Data Protection Law as the Cornerstone of EU's 'Fit for the Digital Age' Legislative Package (March 15, 2024). EDPS at 20 Anniversary Volume, Forthcoming June 2024 , Online: http://dx.doi.org/10.2139/ssrn.4794182
- Dergacheva, Daria and Katzenbach, Christian and Schwemer, Sebastian Felix and Quintais, João Pedro, Improving Data Access for Researchers in the Digital Services Act (June 1, 2023). Online: http://dx.doi.org/10.2139/ssrn.4465846
- Kollnig, Konrad and Shadbolt, Nigel, How Decisions by Apple and Google obstruct App Privacy (January 31, 2023). Technology and Regulation (TechReg), Online: http://dx.doi.org/10.2139/ssrn.4343640
- Iramina, Aline and Perel (Filmar), Maayan and Elkin-Koren, Niva, Paving the Way for the Right to Research Platform Data (June 19, 2023). Online: http://dx.doi.org/10.2139/ssrn.4484052
- Liber Ádám - Bereczki Tamás: Közreműködők adatvédelmi jogállása; JK, 2019/12., 506-507.
- Liber Ádám - Közvetítő szolgáltatók felelőssége szellemi tulajdon megsértéséért az Európai Unióban, in Iparjogvédelmi és Szerzői Jogi Szemle, 2013. június, pp. 5-42.