Károli Gáspár Református Egyetem Állam-
és Jogtudományi Doktori Iskola

dr. Liber Ádám

Adatvédelem és platformok a DSA tükrében

PhD értekezés

A doktori iskola vezetője:	Prof. Dr. Jakab Éva DSc., egyetemi tanár
Felelős témavezető:	Dr. habil. Tóth András PhD tanszékvezető, egyetemi docens

Kézirat lezárásának időpontja: 2024. október 26. napja

BUDAPEST 2024

Témavezetői nyilatkozat

Dr. Liber Ádám: Adatvédelem és platformok a DSA tükrében

c. értekezés-tervezetével kapcsolatosan

Liber Ádám kérése alapján készséggel ajánlom figyelembe az „Adatvédelem és platformok a DSA tükrében" című értékezés tervezetét, amely a digitális szolgáltatásokról szóló rendelet (DSA), valamint az Európai Unió adatvédelmi szabályozásának- különösen az EU Általános Adatvédelmi Rendeletének (GDPR) és az elektronikus hírközlési adatvédelmi irányelvnek (ePrivacy irányelv) - egymásra hatását vizsgálja. Az alábbiakban röviden összefoglalom az értekezés-tervezet főbb tartalmi elemeit és annak szakmai jelentőségét.

Az értekezés átfogóan elemzi az online platformok adatkezelési gyakorlataival kapcsolatos szabályozási kérdéseket, különös figyelmet fordítva a DSA hatálya alá tartozó új szabályokra és azok hatásaira. Különösen értékes, hogy részletesen tárgyalja az adatvédelmi és digitális szabályozás közötti szinergiákat és átfedéseket DSA tükrében, figyelembe véve a modern digitális környezet összetettségét és az online platformok felelősségi rendszerének átalakulását.

Az értekezés-tervezet hat területet emel ki:

- **Digitális platformok adatkezelési szabályozása:** Az adatvédelmi alapelveknek való megfelelés az online platformok gyakorlatában és ennek a megjelenése az esetjogban. Az online platformok által alkalmazott profilalkotás, célzott hirdetések és a felhasználók viselkedésének követése kapcsán felmerülő adatvédelmi kockázatok és azok kezelése.
- **Adatvédelmi szabályok és DSA kapcsolata:** A GDPR és ePrivacy irányelv szabályainak kiegészítése és pontosítása a DSA rendelkezései révén, különös tekintettel a személyes adatok kezelésére, profilalkotásra és a kiskorúak védelmére.
- **Jogszerű adatkezelés szerepe:** A DSA hatása az adatkezelési jogalapokra, például a hozzájárulás fontosságára célzott hirdetések esetében, valamint az adatkezelési korlátozások speciális aspektusaira.
- **Felelősségi kérdések:** A GDPR és a DSA szerinti felelősségi keretek különbségei és átfedései az online platformok által elkövetett jogsértések kapcsán.

- **Platformspecifikus adatvédelmi kötelezettségek:** Automatizált döntéshozatal, tartalommoderálás és felhasználói jogok átláthatósági követelményei; az online óriásplatformokra (VLOP) és nagyon népszerű online keresőprogramot üzemeltető szolgáltatókra (VLOSE) vonatkozó specifikus követelmények és a kutatók hozzáférése.
- **Intézményi együttműködés és szakpolitikai javaslatok:** A GDPR és a DSA végrehajtásához kapcsolódó hatósági koordináció szükségessége, valamint a jogharmonizációra vonatkozó javaslatok.

Liber Ádám értekezés-tervezete nemcsak aktuális digitális szabályozási problémákra világít rá, hanem átfogó elemzést nyújt a DSA és az adatvédelmi szabályozás közötti kapcsolódási pontokról. Külön értéke, hogy az elméleti megközelítést gyakorlati példákkal és szakpolitikai javaslatokkal egészíti ki, ami különösen releváns az adatvédelem és az online platformok működésének szabályozása terén. Az értekezés-tervezet további kutatások alapjául is szolgálhat, különösen a szabályozási átfedések és a sötét mintázatok alkalmazásának kérdéseiben.

Liber Ádám értekezés-tervezete átfogó megközelítése alapján javaslom a tervezetet műhelyvitára, amely értékes hozzájárulást jelenthet az adatvédelmi jog és a digitális szolgáltatások szabályozása terén. Az értekezés-tervezet érdemben hozzájárul a digitális platformok szabályozásának aktuális kérdéseihez és az adatvédelem fejlődéséhez az Európai Unióban.

Budapest, 2024. december 10.

Dr.habil. Tóth András, tanszékvezető egyetemi docens

Témavezető

Tartalomjegyzék

1. BEVEZETÉS - A DIGITÁLIS PLATFORMOK ADATKEZELÉSÉNEK SZABÁLYOZÁSI KÉRDÉSEI

Az Európai Unió (EU) digitális stratégiája[1] az elmúlt években 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 digitális jogok és elvek között garantálja a tisztességes, védett, biztos és biztonságos digitális környezetet[2]. Ennek megfelelően az EU digitális stratégiája középpontjában a digitális szolgáltatások és az online platformok állnak, melyek az információs társadalom gerincét alkotják, és a gazdasági és társadalmi élet minden területére kiterjedő hatással bírnak. Ezen szolgáltatók szerepe azonban nem csupán gazdasági, hanem mélyreható társadalmi és politikai következményekkel is jár. Ez érinti a digitális nyilvános térben való részvétellel összefüggő alapvető jogok védelmét, illetőleg az adatvédelem, kibervédelem, digitális reziliencia és a felhasználói jogok biztosítását.

1.1 A digitális platformok adatkezelése és az online manipuláció jelentősége

A digitális platformok által végzett kiterjedt adatgyűjtés, felhasználói tevékenységek követése, felhasználók tevékenységének és magatartásuk megfigyelése, célzott hirdetések alkalmazása és ezen adatok együttes, mélyreható elemzése, továbbá a gyűjtött adatok mesterséges intelligencia rendszerek tanítása céljából történő értékesítése[3] az adatvédelmi kérdéseket az EU egyik legfontosabb szabályozási területévé tette. A felhasználók online tevékenységeinek nyomon követése és profilozása komoly kihívást jelent 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. Ennek különösen aggasztó vonzata az álhírek és deepfake terjesztése, politikai manipuláció és a választási folyamatok befolyásolása,

[1] Európai Bizottság - Európa digitális jövőjének alakítása; https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_hu; lehívás: 2024.08.19

[2] Európai nyilatkozat a digitális évtizedben érvényre juttatandó digitális jogokról és elvekről; (2023/C 23/01); https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32023C0123(01); lehívás: 2024. 09. 02

[3] FTC conducting inquiry into Reddit's AI data-licensing practices ahead of IPO; 2024. március 21; https://www.cnbc.com/2024/03/15/ftc-investigating-reddit-over-ai-data-licensing-practices-ahead-of-ipo.html; lehívás: 2024.09.02

amelyet az Európai Adatvédelmi Biztos (EDPS) is hangsúlyozott különböző állásfoglalásaiban, így a 2018-as online manipulációról szóló véleményében[4].

Az EU digitális stratégiája 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.

Mérvadó kutatások[5] szerint a felhasználók, választók hírfolyamának vagy keresési eredményeinek manipulálása befolyásolhatja a szavazási viselkedésüket és „véleménybuborékokba" tereli őket. 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. Amikor a választók hírfolyamát vagy keresési eredményeit az óriás keresőprogramot üzemeltető szolgáltatók, vagy szociális háló platform szolgáltatók szándékosan megváltoztatják, az torzíthatja a valóságról alkotott képüket és befolyásolhatja a politikai döntéseiket[6].

Az *online manipuláció* politikai kommunikációt illető veszélyeivel kapcsolatosan az Európai Adatvédelmi Biztos a vonatkozó véleményében[7] szintén utalt a helyi és nemzeti adatvédelmi hatóságokat, valamint nemzetközi szervezeteket tömörítő Global Privacy Assembly (GPA) 2005-ös határozatára[8] a személyes adatok politikai kommunikáció céljából történő

---

[4] EDPS Opinion 3/2018 on online manipulation and personal data; https://www.edps.europa.eu/sites/default/files/publication/18-03-19_online_manipulation_en.pdf, lehívás: 2024.08.19

[5] Véleménybuborék élőben: az emberek többsége alig kerül kapcsolatba más pártállásúakkal - https://telex.hu/belfold/2021/11/02/politikai-homofilia-velemenybuborek-fideszesek-es-ellenzekiek-ismeretsegi-kore-idea-kutatas; Az online platformok hatása a demokratikus nyilvánosságra Kutatási trendek és eredmények; https://onlineplatformok.hu/files/30f0f0a7-34ee-4215-8982-42a14f650251.pdf; lehívás: 2024.09.07

[6] Dipayan Ghosh, Ben Scott - Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You; Time.com; March 19, 2018; https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/; 2024.09.15

[7] EDPS Opinion 3/2018 - EDPS Opinion on online manipulation and personal data; pp. 7-9.; https://www.edps.europa.eu/sites/default/files/publication/18-03-19_online_manipulation_en.pdf lehívás: 2024.09.07

[8] Global Privacy Assembly - Montreux (Switzerland), 14th to 16th September 2005 , Resolution on the Use of Personal Data for Political Communication; https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Personal-Data-for-Polictical-Communication.pdf, lehívás: 2024.09.09

felhasználásáról. Ennek a határozatnak az volt a célja, hogy meghatározza a személyes adatok felhasználásának alapelveit és követelményeit politikai kommunikációs tevékenységek során. A határozat kimondta, hogy minden politikai kommunikációs tevékenységnek, beleértve a választási kampányokat is, tiszteletben kell tartania az érintett személyek alapvető jogait és szabadságait, különösen a személyes adatok védelméhez való jogot. A határozat célja az volt, hogy megakadályozza a személyes adatokkal való visszaélést a politikai célú kommunikáció során, és hogy elősegítse a demokratikus folyamatok integritásának megőrzését az adatvédelmi előírások szigorú betartásával.

Az online manipuláció folyamatát az Európai Adatvédelmi Biztos *három szakasszal írja le*[9], amelyek együtt egy összetett és gyakran láthatatlan ciklust alkotnak, és a modern digitális környezetben egyre nagyobb jelentőséggel bírnak. Az *első szakasz* az adatgyűjtés, amely során a platformok vagy az ott jelen lévő harmadik felek és szolgáltatók az egyének online tevékenységeiből, preferenciáiból és viselkedéséből származó adatokat gyűjtik össze *A második szakasz* a profilalkotás, amely az összegyűjtött adatok extenzív elemzését és felhasználását jelenti annak érdekében, hogy részletes profilokat hozzanak létre az egyénekről. Ezek a profilok az egyének érdeklődési köreit, szokásait és viselkedési mintáit tükrözik, amelyek alapján a platformok képesek személyre szabott ajánlásokat, hirdetéseket vagy tartalmakat megjeleníteni. A profilalkotás révén a platformok nemcsak a felhasználói élményt tudják finomítani, hanem potenciálisan befolyásolhatják is az egyének döntéseit, beleértve a fogyasztói és politikai viselkedést is. A *harmadik szakasz* a mikrocélzás vagy személyre szabás, amely során az elkészült profilok alapján célzott, egyénre szabott üzeneteket vagy tartalmakat küldenek a felhasználóknak, amelyek kifejezetten az ő érdeklődési körükre és viselkedési mintáikra szabottak. Az ilyen típusú adatkezelés különösen érzékeny, mivel komoly hatással lehet az egyének autonómiájára és magánéletére, különösen akkor, ha az érintettek nem kapnak megfelelő tájékoztatást a profilalkotás céljáról és következményeiről.

A leginvazívabb online hirdetési módszerek, mint a viselkedésalapú célzás és a webhelyek közötti nyomon követési technikák adatgyűjtési stratégiákon alapulnak, amelyek során a platformok adatokat gyűjtenek a felhasználókról, profilokat készítenek, és ezeket felhasználva manipulálják őket. Bár ezek a profilok személyre szabott szolgáltatásokat nyújtanak, gyakran

[9] vö. EDPS Opinion 3/2018 - Opinion on online manipulation and personal data; pp. 7-9.;

megsértik a magánélethez, adatvédelemhez való jogot, befolyásolják a személyes autonómiát és a véleménynyilvánítás szabadságát.[10]

Ebben a szabályozásban különleges szerepet játszik *a GDPR*[11], 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. E rendelet célja, hogy megerősítse az egyének adatvédelmi jogait, biztosítva számukra a hozzáférést, a helyesbítést és a törlést, valamint az automatizált döntéshozatali folyamatokkal szembeni védelmet. Ezen felül a GDPR előírja, hogy 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. A nemzetközi adattovábbításra vonatkozó szigorú szabályok biztosítják, hogy az uniós polgárok adatai világszerte megfelelő védelemben részesüljenek, hozzájárulva a digitális térbe vetett bizalom növeléséhez. Mindezeken keresztül a GDPR kulcsfontosságú eleme az EU digitális stratégiájának, amely a digitális innováció és gazdasági növekedés fenntarthatóságát támogatja.

A GDPR rendelkezéseit az online térben a 2002/58/EK irányelv[12] („*ePrivacy irányelv*") rendelkezései konkretizálják és egészíti ki. Ez utóbbi irányelv felülvizsgálat alatt van, és az eredeti tervek szerint a GDPR-ral együtt fogadták volna el rendeleti formában[13], azonban arra ezzel kapcsolatos viták és lobbitevékenységek miatt a mai napig sem került sor[14].

Az Európai Unió digitális startégiájának részeként számos jogszabályt fogadott el, melyek adatvédelmi relevanciával rendelkeznek, ideértve a digitális szolgáltatásokról szóló jogszabályt

[10] vö. Access Now, Raising the alarm: online tracking harms human rights; February 2 2020; https://www.accessnow.org/online-tracking-harms-human-rights/, lehívás: 2024.09.10

[11] 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) (EGT-vonatkozású szöveg); *HL L 119., 2016.5.4,* pp. 1–88.

[12] 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); HL L 201., 2002.7.31, pp. 37–47

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

[14] Captured states – e-Privacy Regulation victim of a "lobby onslaught" By EDRi · May 23, 2019; https://edri.org/our-work/coe-eprivacy-regulation-victim-of-lobby-onslaught/; lehívás: 2024.09.15

(Digital Services Act, DSA[15]), a digitális piacokról szóló jogszabályt (DMA[16]), az adatkormányzási rendeletet (DGA[17]), az adatmegosztási rendeletet (Data Act[18]) és a mesterséges intelligencia rendeletet (AIA[19]), melyek mindegyike személyes adatok kezelésével kapcsolatos szabályokat is rögzít. Az Európai Adatvédelmi Biztos 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 Európai Adatvédelmi Biztos digitális tartalom nyújtásáról szóló szerződésekről szóló irányelv javaslatáról szóló véleményében[20] írta, hogy „*Az alapvető jogokat, mint például a személyes adatok védelméhez való jogot, nem lehet egyszerű fogyasztói érdekekre redukálni, és a személyes adatokat nem lehet csupán árucikknek tekinteni*." Ugyanez a vélemény szintén rögzítette, 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.*"[21] Az Európai Adatvédelmi Biztos 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 a jogalkotási folyamat során[22], ami emiatt potenciálisan jogbizonytalansághoz vezethet, ha ezen

[15] 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; https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32022R2065; European Commission: Shaping Europe's digital future - The Digital Services Act package: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package; https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en; letöltés: 2024.08.19

[16] 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, pp. 1–66.

[17] 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, pp. 1–44.

[18] 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

[19] 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

[20] 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.; https://www.edps.europa.eu/sites/default/files/publication/17-03-14_opinion_digital_content_en_1.pdf; lehívás: 2024.09.13

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

[22] Gabriela Zanfir-Fortuna, Follow the (personal) data: Positioning data protection law as the cornerstone

új digitális jogszabályok és a GDPR együttes alkalmazásából származó szabályozási átfedéseket vesszük figyelembe.

A digitális szolgáltatásokról szóló jogszabály alkalmazása tekintetében ezért merül fel a kérdés, amely jelen értekezésnek 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 és milyen következményei vannak e szabályozási átfedéseknek és hogyan lehet kezelni ezeket.

1.2 A DSA szabályozási rendszere és a szolgáltatás minősítés jelentősége

Az Európai Unió a digitális szolgáltatások területén tehát *az uniós adatvédelmi szabályozással 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 DSA központi szerepet játszott ebben a jogalkotási folyamatban. A DSA célja, hogy az online platformok szabályozása alapvető jogokon alapuló megközelítést biztosítson, amelyben a személyes adatok védelme is központi szerepet játszik.[23] 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 kulcsszerepet játszik abban, hogy megteremtse az egyensúlyt a szabad és tisztességes digitális gazdaság, valamint a személyes adatok és az egyéni felhasználói jogok védelme között.

of EU's 'Fit for the Digital Age' legislative package; Working Paper – Forthcoming in EDPS At 20 Anniversary Volume, June 2024; p. 4.; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4794182; lehívás: 2024.09.13,

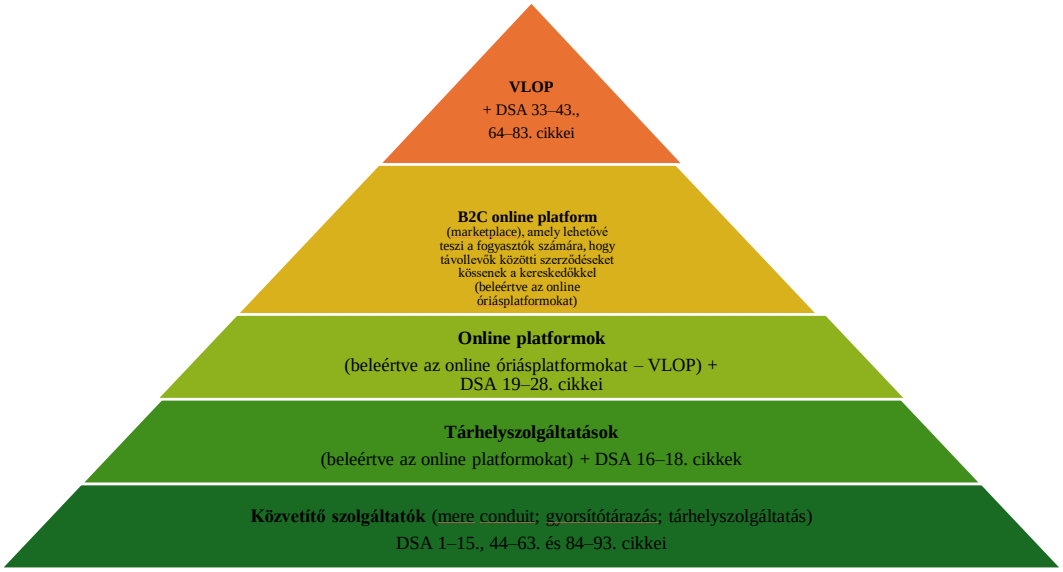
[23] vö. DSA (3) preambulumbekezdése; vö. Domingos Soares Farinho - Personal Data Processing by Online Platforms and Search Engines: The Case of the EU Digital Services Act, https://folyoirat.ludovika.hu/index.php/pgaf/article/view/7134/5939; lehívás: 2024.09.11. p. 38.

A DSA a 2000-ben elfogadott elektronikus kereskedelemről szóló irányelv[24] korábbi rendelkezéseire épít, amelyben már központi szerepet játszott a „közvetítő szolgáltatás" (ISP) fogalma, azonban a szabályozás tovább finomította e fogalom hatálya alá tartozó szolgáltatásokat. Az irányelv az ún. közvetítő szolgáltatók között az általuk végzett tevékenység alapján hármas felosztást végzett, amelyek a következők voltak: 1. *Egyszerű továbbítás* (mere conduit, azaz access provider vagy network provider), 2. *Gyorsítótárazás* (caching szolgáltatások nyújtói, és 3. *Tárhelyszolgáltatás* (hoszting), mint a cloud computing szolgáltatók; web hoszting szolgálatók; szociális hálók / közösségi platformok vagy a video-megosztóplatformok. Miközben a DSA-ban ez a hármas megkülönböztetés megmaradt és a „szolgáltatókat" immár „*közvetítő szolgáltatás*"-ként nevesítik (vö. DSA 3. cikk g) pont), a DSA két további új alkategóriát különít el a tárhelyszolgáltatásokon belül, amely az „online platform" és „online keresőprogram", és mindkét kategórián belül egy további alkategóriát, így az „*online óriásplatformokat*" (VLOP) és „*nagyon népszerű online keresőprogramokat*" (VLOSE). Mindezen új kategóriákra további szabályok vonatkoznak, ami a szabályozás szigorítását eredményezi a hierarchia csúcsán szereplő szolgáltatókra. Így az online platformok és az online keresőprogramok a DSA tárgykörébe tartozó, információs társadalommal kapcsolatos közvetítő szolgáltatások széles körén belüli specifikus alkategóriákra utalnak. Az említett tevékenységek sokféleségét figyelembe véve a DSA egy hierarchikus rendszert alkalmaz, amely eltérő, illetőleg szigorúbb kötelezettségeket ír elő az egyes közvetítő szolgáltatások kategóriái számára. Míg egyes általános kötelezettségek valamennyi ISP-re vonatkoznak, addig különös kötelezettségek a tárhelyszolgáltatókra; online platformokra (B2C online piacterekre), online keresőszolgáltatásokra vonatkoznak.

A DSA különböző szolgáltató típusokat leíró szabályozási „piramisa"[25] az alábbiakban látható:

[24] 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); A dokumentum eredetije megtekinthető CELEX: 32000L0031 - https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32000L0031&locale=hu Utolsó elérhető, magyar nyelvű konszolidált változat CELEX: 02000L0031-20240217 - https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:02000L0031-20240217&locale=hu

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



Ha egy adott szolgáltató egyidejűleg több szolgáltatást nyújt, akkor részben vagy egészben a DSA hatálya alá tartozhat, vagy eltérő szolgáltatások a DSA különböző követelményeinek hatálya alá tartozhatnak[26]. A szolgáltatás minősítés a nyújtott szolgáltatások és technikai funkciók elemzését igényli és adott esetben függhet a vállalkozás méretétől, hogy a szolgáltató mikro- vagy kisvállalkozás minősül-e; továbbá a funkciók és technológia változása is alapot adhat a szolgáltatásminősítés módosításra.

A DSA 3. cikk i) pontja meghatározza az „*online platformok”* fogalmát, melyek gyakorlatilag olyan szolgáltatásokra vonatkoznak, mint az online piacterek, alkalmazásboltok, közösségi hálózatokra vonatoznak. Az „online platform” olyan tárhelyszolgáltatás, amely nem csak azért tárol információt, mert azt a szolgáltatás igénybe vevői kérik, hanem a szolgáltatás igénybe vevőinek kérésére a nyilvánosság számára is terjeszti az információt. E tevékenység nem lehet egy másik szolgáltatás kisebb vagy kizárólag kiegészítő eleme, vagy a fő szolgáltatás kisebb funkcionalitása, amely objektív és technikai okokból nem használható az említett másik szolgáltatás nélkül (pl. online újság komment szekcióval, ami csak kiegészítő elem), kivéve, ha az ilyen elem vagy funkcionalitás másik szolgáltatásba való integrációja a DSA

[26] 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. - 29. pontok; lehívás: https://www.acm.nl/system/files/documents/guidelines-dsa-due-diligence-obligations-for-intermediary-services.pdf; 2024.09.15

alkalmazhatóságának elkerülésére szolgál[27]. A DSA 3. cikk i) pontja a „*nyilvános terjesztés*” fogalmát akként határozza meg, hogy az információkat potenciálisan korlátlan számú személy számára teszik elérhetővé. A DSA 14. preambulumbekezdése szerint, ha az információkhoz való hozzáféréshez regisztrációra vagy a szolgáltatás igénybe vevőinek egy csoportjához való csatlakozásra van szükség, csak akkor, ha az információkhoz hozzáférni kívánó igénybe vevők automatikusan – tehát emberi döntés vagy a hozzáférésre jogosultak emberi kiválasztása nélkül – regisztrálásra kerülnek vagy felvételt nyernek. Ha a szolgáltatás igénybe vevői csak regisztrációval vagy hozzájárulás megszerzése után férhetnek hozzá az információhoz, a „nyilvánossághoz való terjesztés” akkor is megvalósul, ha a regisztráció automatikus. Ez azt jelenti, hogy nincs szükség emberi döntésre vagy hozzáférés kiválasztására.[28] A DSA 19. cikke értelmében mikro- vagy kisvállalkozásokra nem terjednek ki az online platformokra irányadó kötelezettségek. Ha a szolgáltató nő forgalom vagy alkalmazott szám tekintetében, és már nem felel meg ezeknek a feltételeknek, akkor a státusz elvesztését követő tizenkét hónapon belül köteles megfelelni az online platformszolgáltatókra vonatkozó kötelezettségeknek.

Az online platformok üzleti modellje teljes mértékben a személyes adatokon alapul, mint amelyet a felhasználók által generált tartalom jelent. Ezek a platformok személyes adatokat gyűjtenek, kezelik és monetizálják azokat egy szolgáltatásért cserébe[29]: lehetővé téve a személyes adatok alanyainak, azaz a felhasználóknak, hogy megosszák tartalmukat online. A személyes adatok az online platformok és keresőszolgáltatók üzleti modelljén belül egy sajátos típusú tartalomként tekinthetők, amelyet ezekre a platformokra és szolgáltatás nyújtása céljából nyújtanak. A tartalom ezért legtöbb esetben a szolgáltatás igénybe vevője által létrehozott

[27] lásd Európai Unió Bírósága Uber France ügy (C-321/16.), ahol az Uber szolgáltatását nem közvetítő szolgáltatásként, hanem személyszállítási szolgáltatásként értékelték, illetőleg az Airbnb Ireland ügyet (C-390/18), ahol a Bíróság elhatárolta egymástól a platformon nyújtott szolgáltatást a bérléstől. vö. Koltay András, Szikora András, Lapsánszky András, Tóth András (szerk.) - Nagykommentár a DSA rendelethez, Wolters Kluwer, 2024; 19. oldal; Erion Murati - Airbnb and Uber: two sides of the same coin; Case note to CJEU of 19 December 2019 C-390/18 (AHTOP v. AIRBNB Ireland); September 8, 2020; https://www.medialaws.eu/airbnb-and-uber-two-sides-of-the-same-coin/; lehívás: 2024.09.15.

[28] vö. ACM DSA Guidelines - Due diligence obligations for intemediary services - Netherlands Authority for Consumers and Markets; 38. sarokpont.

[29] 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; https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_hu.pdf, lehívás: 2024.09.15

személyes adatnak minősül, amelyet a szolgáltatás igénybe vevői online platformok részére szolgáltatnak és azok teszik hozzáférhetővé változó számú felhasználó számára[30]. Ebben a tekintetben a „*szolgáltatás igénybe vevője*" (felhasználó) fogalmát tág értelmében[31] kell használni, amely nemcsak a regisztrált aktív vagy passzív felhasználókat jelenti, hanem azokat a természetes és jogi személyeket is, akik a szolgáltatást akár üzleti, akár magáncélból veszik igénybe annak érdekében, hogy információkhoz jussanak, amelyeket a platformok vagy online keresőprogramok tárolnak és jelenítenek meg. Továbbá, mivel az online keresőprogramokat jogi szempontból ugyanúgy kezelik, mint az online platformokat, az itt használt online platformokra való hivatkozások utalások az online keresőprogramokra is vonatkoznak[32], hacsak másként nincs meghatározva.

1.3 A digitális platformok adatkezeléseinek szabályozási kihívásai

A digitális platformok, különösen a nagy technológiai vállalatok, mint a Google (Alphabet), a Facebook (Meta), a Microsoft, a Tencent, az Amazon és az Apple által működtetett digitális közösségi terek központi szerepet játszanak a digitális tartalmak elérhetőségének és terjedésének szabályozásában. Ezek a vállalatok hatékony kapuőrökké váltak, mivel uralják azokat a platformokat és szolgáltatásokat, amelyeken keresztül a felhasználók hozzáférnek az információkhoz, szórakozáshoz és egyéb digitális tartalmakhoz. Az általuk alkalmazott algoritmusok és adatkezelési technikák révén képesek meghatározni, hogy mely tartalmak jelennek meg a felhasználók előtt, és melyek maradnak láthatatlanok. Ezen kapuőr szerepük révén jelentős befolyást gyakorolnak arra, hogy a felhasználók milyen információkkal találkoznak nap mint nap.

Ezen vállalatok által végzett adatgyűjtés és profilalkotás a digitális gazdaság egyik alapköve, mivel ezek a vállalatok hatalmas mennyiségű adatot gyűjtenek a felhasználóikról, beleértve a keresési előzményeiket, vásárlási szokásaikat, közösségi média tevékenységeiket, az adott platform mely tartalmát vagy weboldalának a részét találták érdekesnek és sok más adatpontot.

---

[30] vö. Domingos Soares Farinho im p. 39.;
[31] vö. DSA 3. cikk (b), (p) és (q) pontjait
[32] DSA 3. cikk j) pontja szerint „online keresőprogram": olyan közvetítő szolgáltatás, amelynek segítségével a felhasználók kéréseket vihetnek be azzal a céllal, hogy elvileg az összes weboldalon vagy egy adott nyelvhez tartozó összes weboldalon kulcsszó, hangalapú kérés, kifejezés vagy egyéb formában megadott lekérdezés alapján bármilyen témában kereséseket végezzenek, és amely bármilyen formátumban olyan eredményeket ad meg, amelyekben megtalálhatók a keresett tartalommal kapcsolatos információk;

Az így szerzett információkat arra használják fel, hogy részletes profilokat készítsenek az egyénekről, fejlesszék a saját algoritmusaikat és platformjuk design-ját, amelyek alapján célzott hirdetéseket és tartalmakat jelenítenek meg. Ez a folyamat lehetővé teszi a vállalatok számára, hogy maximalizálják hirdetési bevételeiket, miközben növelik a felhasználói élményt és elkötelezettséget. Ugyanakkor felveti a kérdést, hogy ezek az adatalapú döntések mennyire etikusak és hogyan befolyásolják a felhasználói autonómiát?

A nagy technológiai vállalatok *pénzügyi ereje* és *piaci dominanciája* szintén kulcsszerepet játszik a digitális ökoszisztéma alakításában. Ezek a vállalatok nemcsak a saját technológiáik folyamatos fejlesztésére képesek, hanem rendszeresen felvásárolják azokat a kisebb, innovatív vállalkozásokat is, amelyek potenciális versenytársaikká válhatnának[33]. Ez a koncentráció lehetővé teszi számukra, hogy tovább erősítsék pozíciójukat a piacon, és növeljék befolyásukat a digitális világban. Az ilyen mértékű hatalom azonban komoly szabályozási kihívásokat is felvet, mivel a szabályozó hatóságok és a közvélemény is nyugtalansággal figyeli, hogy ezek a vállalatok vajon tisztességesen és átláthatóan működnek-e, valamint, hogy mennyire korlátozzák a piaci versenyt és a véleménynyilvánítás szabadságát, illetve sértik a felhasználók magánéletét.

Az amerikai egyesült államokbeli Federal Trade Commission (FTC) 2024. szeptember 19. napján tette közzé a közösségi média és videó streaming szolgáltatások adatvédelmi gyakorlataival kapcsolatos jelentését[34]. Az FTC piacelemzés alapján olyan szolgáltatások adatkezelési gyakorlatait vizsgálta a 2019–2020 közötti időszak vonatkozásában, mint az Amazon, Facebook, YouTube, Twitter, Snap, ByteDance (TikTok), Discord, Reddit, and WhatsApp. A jelentésben foglaltakkal kapcsolatosan aggasztó, hogy a GDPR alkalmazandóvá válása utáni gyakorlatokat vizsgál globális szolgáltatók esetében és 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. Az FTC megállapítása szerint az érintett vállalatok

[33] Marc Ivaldi, Nicolas Petit, Selçukhan Ünekbaş - Killer acquisitions in digital markets may be more hype than reality - Centre for Economic Policy Research; 15 Sep 2023 - https://cepr.org/voxeu/columns/killer-acquisitions-digital-markets-may-be-more-hype-reality; lehívás: 2024.09.21

[34] 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 („FTC Staff Report"); https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf; lehívás: 2024.09.19

olyan fogyasztókat megkárosító gyakorlatokat folytatnak, melyek az *adatvédelem rovására* törekednek profitmaximalizálásra és a *piaci verseny korlátozására*.[35]

Az FTC jelentés megállapítja, hogy számos vizsgált szolgáltató *a felhasználókról és a nem felhasználókról egyaránt tömegesen gyűjtött adatokat*, amely számos káros és megkérdőjelezhető gyakorlat forrása. A gyűjtött adatok magában foglalta a felhasználók által megadott információkat, a passzívan gyűjtött adatokat vagy levont következtetéseket, valamint azokat az információkat, amelyeket egyes vállalatok adatbrókerektől és másoktól vásároltak a felhasználókról, ideértve olyan adatokat, mint a háztartás jövedelme, lakóhelye és érdeklődési köre, közöttük érzékeny személyes adatok[36]. A legtöbb vállalat harmadik felekkel is megosztotta a felhasználók személyes adatait[37], és nem tudták teljes körben felsorolni, hogy kik kapják meg ezeket az adatokat és milyen célból, illetve nem alkalmaztak megfelelő garanciákat erre[38]. A szolgáltatók, amelyek harmadik felektől származó adatokat gyűjtöttek, nem ismerték, hogy milyen adatokat kezelnek. A jelentés kockázatként azonosította a nemzetközi adattovábbításokat olyan országokba, mint Kína, Egyesült Arab Emírségek vagy Ukrajna[39]. A szolgáltatók az általuk gyűjtött adatokat határozatlan időtartamig és a fogyasztók elvárásaival ellentétesen őrizték meg, mivel az adatgyűjtési, adatminimalizálási és adatmegőrzési gyakorlatuk nem volt megfelelő[40]. Az adatokat több esetben a felhasználó kérése ellenére sem törölték, hanem csupán inaktiválták (soft deletion) vagy csak pszeudonimizálták azokat[41], amely adatkezelési gyakorlat adatvédelmi kockázatot jelentett a felhasználók és a nem felhasználók adatainak védelmére egyaránt. A jelentés komoly problémákat azonosított az érintetti jogok kezelésével, és a felhasználó adatvédelmi jogainak (privacy choices) betartásával kapcsolatosan.[42] A szolgáltatók adatkezelési tájékoztatói hosszúak, nem átláthatók, nem érthetőek, és nem megállapítható belőlük, hogy milyen adatkezelési gyakorlatokat folytatnak.[43]

[35] Statement of Commissioner Alvaro M. Bedoya On the 6(b) Report Examining the Data Practices of Social Media and Video Streaming Services; https://www.ftc.gov/system/files/ftc_gov/pdf/bedoya-statement-social-media-6b-report.pdf; lehívás: 201.09.19
[36] vö. FTC Staff Report, pp. 21-24.
[37] vö. FTC Staff Report, p. 27.
[38] vö. FTC Staff Report, p. 28-29.
[39] vö. FTC Staff Report, p. 28.
[40] vö. FTC Staff Report, pp. 30-31.
[41] vö. FTC Staff Report, p. 31
[42] vö. FTC Staff Report, p. 36.
[43] vö. FTC Staff Report, p. 38.

A jelentés szintén megállapítja, hogy a *targetált hirdetések* komoly kockázatot jelentenek az érintettek adatai védelmére, ideértve a megnövekedett csalás kockázatot, az adatvédelmi incidensekből eredő rendszerszintű kockázatokat és a gazdasági lehetőségekből való potenciális kirekesztés lehetőségét.[44] Számos szolgáltató támaszkodott arra, hogy reklámszolgáltatásokat értékesítsen más vállalkozásoknak, amelyek nagyrészt a felhasználók személyes adatai extenzív felhasználásán alapultak.[45] Ezen ökoszisztémát működtető technológia a színfalak mögött és a fogyasztók számára *láthatatlanul* működik, ami jelentős adatvédelmi kockázatot jelent. Egyes vállalatok például számos olyan adatvédelemi szempontból invazív nyomonkövető technológiákat alkalmaznak, mint például a pixelek, amelyek képesek a felhasználók tevékenységére vonatkozó érzékeny információkat továbbítani. Egyes vállalatok érzékeny adatokon alapuló reklámcélzási gyakorlata szintén komoly adatvédelmi aggályokat vet fel, ideértve a felhasználó hátrányos megkülönböztetését, érzelmi sérelem okozását, a megbélyegzést, a jó hírnévnek a sérelmét és a magánélet megsértését.[46] Mivel a hirdetési ökoszisztéma összetett és a működése a felszíne alatt zajlik, a felhasználók számára kihívást jelent annak megértése, hogy a róluk gyűjtött információkat hogyan használják fel a hirdetések célzására – és számos felhasználónak egyáltalán nincs is tudomása erről.[47]

A jelentés kitér az *algoritmusok, az adatelemzés, vagy a mesterséges intelligencia (AI) széles körű alkalmazására* a felhasználók és a nem felhasználók személyes adatainak kezelésével kapcsolatosan[48]. Ezek a technológiák lehetővé teszik a tartalomajánlást, a keresést, a reklámozást, az automatizált döntésen alapuló tartalommoderálást és a felhasználók személyes adataiból következtetések levonását is[49]. A felhasználók azonban nem rendelkeznek érdemi ellenőrzéssel a személyes adataik mesterséges intelligenciával (inkább gépi tanulással) működő rendszerek általi felhasználása felett. Ez különösen igaz azokra a személyes adatokra, amelyek származtatott adatok, amelyeket harmadik féltől vásároltak, vagy amelyeket a felhasználók és nem felhasználók platformon kívüli tevékenységeiből származtattak. Ezen rendszerek alapbeállítása, hogy gyűjtik az adatokat és ezzel kapcsolatosan nem biztosítják a hozzájárulás vagy a tiltakozás lehetőségét.[50] Ez igaz azokra a nem felhasználókra is, akik nem rendelkeztek

[44] vö. FTC Staff Report, p. 38.
[45] vö. FTC Staff Report, p. 40.
[46] vö. FTC Staff Report, p. 44.
[47] vö. FTC Staff Report, p. 46.
[48] vö. FTC Staff Report, p. 48.
[49] vö. FTC Staff Report, p. 50.
[50] vö. FTC Staff Report, p. 59.

fiókkal, és akik esetleg soha nem használták az adott szolgáltatást. A felhasználók és a nem felhasználók nem jogosultak ellenőrizni ezen rendszerek által kezelt adatokat vagy azok eredményeit, hogy helyesbítsék a hibás adatokat vagy megállapításokat, vagy hogy megértsék, hogyan születtek az ezzel kapcsolatos döntések.[51] A vállalatok automatizált rendszereinek használatával kapcsolatban hiányzott a hozzáférés, a döntés, az ellenőrzés, az átláthatóság, a megmagyarázhatóság és az értelmezhetőség, illetve az emberi felülvizsgálat lehetősége[52]. Az automatizált rendszerek használatának ellenőrzésére és tesztelésére vonatkozóan is eltérő, következetlen és nem megfelelő eljárásokat használtak[53]. Ezen vállalatok olyan algoritmusokat használtak, amelyek előnyben részesítenek káros tartalmak bizonyos formáit, melyek a kiskorúak mentális egészségére káros hatást gyakorolnak. A közösségi média és videó streaming szolgáltatók többsége azt állította, hogy nincsenek gyermek felhasználóik, annak ellenére, hogy valójában gyermekek is használják ezeket a platformokat, és úgy kezelték őket, mintha felnőtt felhasználók lennének[54]. Ezek a szolgáltatók nem biztosítottak megfelelő védelmet a kiskorúak számára.[55]

Az FTC szerint az adatokkal való visszaélések hozzájárulhatnak a *piaci erőfölényhez*, ami viszont tovább erősítheti az adatvisszaéléseket és a fogyasztóknak káros gyakorlatokat[56]. A digitális piacokon a felhasználói adatok megszerzése és fenntartása erőfölényhez vezethet, amely kizárja a versenytársakat és belépési korlátként akadályozza a piacra lépésüket. A felhasználói adatok versenyértéke ösztönözheti a vállalatokat arra, hogy az adatok gyűjtését az adatvédelem rovására helyezzék előtérbe.[57] Ezen túlmenően egy vállalat adatvédelmi gyakorlatai, adatgyűjtése, adatfelhasználása és automatizált rendszerei fontos részét képezhetik a termékminőségnek a digitális piacokon. A piaci verseny hiánya miatt a felhasználóknak *nincs valós választási lehetőségük* a szolgáltatások között, és kénytelenek elfogadni egy erőfölényben levő vállalat adatkezelési gyakorlatait. Ennek eredményeként a vállalatok nem versenyeznek ezeken a területeken, így a fogyasztók elveszítik a választási szabadságukat és autonómiájukat.

[51] vö. FTC Staff Report, pp. 60-61.
[52] vö. FTC Staff Report, pp. 68-69.
[53] vö. FTC Staff Report, pp. 65-67.
[54] vö. FTC Staff Report, p. 63., p. 75.
[55] vö. FTC Staff Report, p. 63., p. 72.
[56] vö. FTC Staff Report, p. 78.
[57] vö. FTC Staff Report, p. 79.

Összességében a verseny korlátozottsága súlyosbíthatja azokat a fogyasztói károkat, melyet a jelentés is leír[58].

Az FTC a jelentésében kitér arra, hogy az önszabályozás nem működik és nem is opció[59], mert az *kudarcot vallott*, ezért az FTC olyan *szabályozási lépésekre* tett javaslatot, amely a felhasználók személyes adatai védelmével, kiskorúak védelmével és a versenyellenes hatások megszüntetésével kapcsolatosak.

Az FTC jelentésében jelzett diszfunkciók és piaci kudarcok arra utalnak, hogy a platformok adatvédelmi és adatkezelési gyakorlatainak *szigorú szabályozása indokolt*, melynek az Európai Unió a GDPR, a DMA és a DSA elfogadásával tett kísérletet, azonban a végrehajtás területén érzékelhetően további lépések indokoltak, különösen határokon átnyúló ügyekben.[60]

1.4 Az értekezés módszertani megközelítése

A jelen értekezés célja, hogy átfogó képet nyújtson az EU adatvédelmi és platformszabályozási 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 és a DSA jogintézményeinek az adatvédelmi vonatkozásaira. Ennek keretében lefedi a digitális platformok adatkezelési gyakorlatait, különös tekintettel a GDPR, az ePrivacy irányelv és a DSA rendelkezéseire, követelményeire, valamint a vonatkozó szabályozási követelmények együttes alkalmazására és érvényesülésére a platformok adatkezelési folyamataiban.

Az értekezés első, *bevezető részében* bemutatásra kerültek a digitális platformok adatkezelésével kapcsolatos alapvető problémák, különösen az online manipuláció, az adatok tömeges gyűjtése, az ebből adódó piaci kudarcok és az ebből származó kockázatok. Ez a rész felvázolta a digitális platformok által generált főbb adatvédelmi kihívásokat, amelyek az elemzés alapjául szolgáltak.

[58] vö. FTC Staff Report, p. viii.
[59] vö. FTC Staff Report, p. 80.
[60] Data protection: Commission adopts new rules to ensure stronger enforcement of the GDPR in cross-border cases; https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3609; lehívás: 2024.09.15

Az értekezés *második része* a GDPR adatvédelmi alapelveinek érvényesülését vizsgálja digitális platformok esetében. Itt elemzi a jogszerűség, átláthatóság, tisztességes adatkezelés, célhoz kötöttség, adattakarékosság, pontosság, korlátozott tárolhatóság, adatbiztonság és elszámoltathatóság elveit, és bemutatja, hogyan alkalmazhatóak ezek a platformok adatkezelési gyakorlatában. Ebben a fejezetben különös hangsúlyt kap a platformok adatkezelői státuszának meghatározása, valamint a közös adatkezelés kérdései. A legnagyobb platformok – például a Facebook, Google és Amazon – komplex adatkezelési láncok mentén működnek, amelyben több szereplő vesz részt. Az elemzés az Európai Bíróság és a nemzeti adatvédelmi hatóságok gyakorlatára is támaszkodik, hogy teljes képet nyújtson a joggyakorlatról és az adatvédelmi alapelvek gyakorlati alkalmazásáról.

A *harmadik rész* a DSA szabályozási kereteit elemzi. A DSA új jogszabályként különösen a közvetítő szolgáltatásokra koncentrál, és számos specifikus adatvédelmi kötelezettséget vezet be, amelyek szigorúbbak és kiegészítik a jelenlegi adatvédelmi jogszabályokat. Ez a fejezet bemutatja a DSA által előírt adatvédelmi kötelezettségeket, különös tekintettel a jogellenes tartalom kezelésére, a tartalommoderálásra, a transzparencia követelményeire, a profilozás korlátozásaira és a felhasználói jogok védelmére. Külön elemzés részét képezi a DSA és a GDPR közötti összefüggések és átfedések, mivel ezek a szabályok együttesen határozzák meg a platformok jövőbeni adatvédelmi gyakorlatait. Ezenkívül bemutatásra kerül, hogy a DSA milyen új, szigorúbb elszámoltathatósági kötelezettségeket vezet be az online óriásplatformokok (VLOP) és nagyon népszerű online keresőprogramok (VLOSE) számára, valamint az, hogy ezek a kötelezettségek hogyan érintik ezek a felhasználók személyes adatait. Ezzel kapcsolatosan kitér a kutatók adatokhoz való hozzáférésére is, amely fontos ellenőrzési eleme a VLOP és VLOSE szolgáltatók gyakorlatainak és elszámoltathatóságának.

Az értekezés *utolsó része* az európai adatvédelmi jog és a DSA végrehajtásának gyakorlati szempontjait elemzi. Ez a fejezet a szabályok betartatásának eszközeire és az érintett hatóságok – mint az Európai Adatvédelmi Testület, a nemzeti adatvédelmi hatóságok, az Európai Bizottság, a Digitális Szolgáltatások Európai Testülete és a digitális szolgáltatási koordinátorok – szerepére fókuszál. Emellett bemutatom, hogy milyen kihívásokkal szembesülnek a hatóságok és a platformok, amikor a DSA és a GDPR követelményeit együttesen kell alkalmazniuk.

Ez a módszertani megközelítés lehetővé teszi a digitális platformok adatkezelési gyakorlatainak elemzését mind az adatvédelmi követelmények, mind a DSA alkalmazása szempontjából. Kiemeli a két jogszabály közötti összefüggéseket és gyakorlati kihívásokat, ezzel átfogó képet nyújtva a platformok adatvédelmi kötelezettségeiről, a szabályok tényleges végrehajtásáról és a gyakorlat fejlesztési lehetőségeiről.

2. PLATFORMOK ADATVÉDELMI GYAKORLATAI - AZ UNIÓS ADATVÉDELMI SZABÁLYOK ALKALMAZÁSA PLATFORMOKRA

2.1 Platformok működésének adatvédelmi relevanciája

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[61] -, ami ezzel az üzleti modellel rendszeresen együtt jár. Az online közvetítők működésének adatvédelmi relevanciája abból fakad, hogy központi szerepet játszanak a személyes adatok gyűjtésében, kezelésében és felhasználásában és tevékenységük közvetlen hatással van az egyének magánéletére és a személyes adatok védelmére online tevékenységekkel kapcsolatosan. A legnagyobb online platformok hatalmas mennyiségű személyes adatot gyűjtenek a felhasználókról, beleértve demográfiai adatokat, viselkedési mintázatokat, preferenciákat és online tevékenységeket[62]. Ezek az adatok lehetővé teszik a platformok számára, hogy részletes profilokat alkossanak az érintettekről, amelyeket később célzott hirdetésekhez, szolgáltatások testre szabásához vagy akár automatizált döntéshozatali folyamatokhoz használjanak fel. A profilalkotás és az automatizált döntéshozatali folyamatok alkalmazása lehetővé teszik, hogy a platformok előre meghatározott algoritmusok alapján döntéseket hozzanak a felhasználókkal kapcsolatban, például milyen tartalmakat, hirdetéseket vagy ajánlásokat lássanak vagy hogyan szegmentálják őket.

A GDPR ezzel összefüggésben szigorú szabályokat és alapelveket[63] 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 határozza meg és ide tartozik a *jogszerűség, tisztességes adatkezelés elve, az átláthatóság, a célhoz kötöttség, adatminimalizálás, pontosság, integritás és bizalmas kezelés, valamint az*

[61] vö. GDPR 4. cikk 1. pontja - „személyes adat” meghatározása; lásd erről részletesen a 29. cikk szerinti adatvédelmi munkacsoport személyes adat fogalmáról szóló véleményét 4/2007 szám alatt (WP 136); https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, lehívás: 2024.09.15

[62] Aisling Redden: Companies are collecting your personal data. Here's what you need to know; Euronews, https://www.euronews.com/next/2023/08/14/companies-are-collecting-your-personal-data-heres-what-to-know; lehívás: 2024.09.13

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

elszámoltathatóság alapelve és alapvetően meghatározzák a platformok működését a személyes adatok kezelésével kapcsolatosan. A személyes adatok kezelésére vonatkozó, a GDPR 5. cikkében foglalt elvek együttesen alkalmazandók.[64] A GDPR előírja, hogy bármely személyes adat kezelése tiszteletben tartsa az adatkezelési elveket, mellyel kapcsolatos bizonyítási teher az elszámoltathatóság elve alapján az adatkezelő online közvetítőt terheli.

A GDPR rendelkezéseit az online térben az ePrivacy irányelv rendelkezései pontosítják[65] és kiegészítik[66]. Az ePrivacy irányelv számos rendelkezése „pontosítja" a GDPR rendelkezéseit a személyes adatoknak az elektronikus hírközlési ágazatban történő kezelése tekintetében. A *lex specialis derogate legi generali elvvel* összhangban a különös rendelkezések elsőbbséget élveznek az általános elvekkel szemben azokban a helyzetekben, amelyeket kifejezetten szabályozni kívánnak. Azokban a helyzetekben, amikor az ePrivacy irányelv „pontosítja" (azaz konkrétabbá teszi) a GDPR-ban foglalt szabályokat, az ePrivacy irányelv (különös) rendelkezései – mint „*lex specialis*" – elsőbbséget élveznek a GDPR (általánosabb) rendelkezéseivel szemben.[67] Az ePrivacy irányelv olyan rendelkezéseket is tartalmaz, amelyek egyrészről „*kiegészítik*" a GDPR rendelkezéseit a személyes adatoknak az elektronikus hírközlési ágazatban történő kezelése tekintetében.[68] Így 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. preambulumbekezdése megerősíti, hogy amikor a személyes adatok kezelésére nem vonatkoznak az ePrivacy irányelvben meghatározott különös kötelezettségek, akkor a GDPR

[64] vö. Európai Unió Bírósága, 2022. október 20-i Digi ítélet, C-77/21, EU:C:2022:805, 47. pont

[65] 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.; https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_hu.pdf; lehívás: 2024.09.09

[66] Az ePrivacy 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. […]"

[67] A 29. cikk alapján létrehozott adatvédelmi munkacsoport 2010. június 22-i, 2/2010. számú véleménye az online viselkedésalapú reklámról, WP171, 10. o.

[68] Vö. 5/2019. számú EDPB vélemény az elektronikus hírközlési adatvédelmi irányelv és az általános adatvédelmi rendelet közötti kölcsönhatásról, különösen az adatvédelmi hatóságok illetékessége, feladatai és hatásköre tekintetében; 4.2 pont;

alkalmazandó. Tehát amennyiben léteznek különös rendelkezések valamely konkrét adatkezelési műveletre vagy műveletekre vonatkozóan, akkor a különös rendelkezéseket kell alkalmazni (*lex specialis*), minden egyéb esetben (vagyis amikor nem vonatkoznak különös rendelkezések az adott adatkezelési műveletre vagy műveletekre) pedig az általános szabály alkalmazandó (*lex generalis*). Az ePrivacy irányelv többek között különös szabályokat állapít meg az elektronikus (online) kommunikáció bizalmasságának és biztonságának védelmére, beleértve az elektronikus direkt marketing szabályozását. 2009-es felülvizsgálata óta[69] 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 magyarországi átültetését részben az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Elkertv.) végezte el. Ezen szabályok célja, hogy a személyes adatok kezelésével kapcsolatosan a GDPR rendelkezéseit „*pontosítsa és kiegészítse*" az elektronikus hírközlési szektor tekintetében. Az információs társadalommal összefüggő szolgáltatások, például weboldalak működtetése kapcsán bizonyos folyamatok kizárólag az egyik szabályozási keret hatálya alá tartozhatnak. Például, ha az adott technológia alkalmazása nem jár személyes adatok kezelésével, akkor csak az Elkertv. követelményeit kell betartani, és a GDPR szabályai nem alkalmazandók. Azonban olyan folyamatok és technológiák alkalmazása esetében, mint a csalásfelderítés és -megelőzés, szolgáltatásfejlesztés, tartalom személyre szabása, felhasználói élmény optimalizálása, biztonsági folyamatok monitorozása és incidenskezelés, felhasználói támogatás és ügyfélszolgálat, adat-elemzés és jelentéskészítés, piackutatás és versenyelemzés, termékfejlesztés, viselkedés-elemzés, ellátási lánc és készletgazdálkodás, ügyfél-szegmentálás, árazási optimalizálás stb. céljából történő sütik alkalmazásához kapcsolódik, ami személyes adatok kezelésével jár, úgy az ePrivacy irányelv / Elkertv. és a GDPR egyaránt alkalmazandó. Erre az esetre a GDPR 95. cikke irányadó, mely szerint az adatkezelők nem kötelesek további kötelezettségeket teljesíteni a GDPR alapján, amennyiben már eleget tesznek az ePrivacy irányelvben megfogalmazott, azonos célt szolgáló

[69] 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, pp. 11–36

kötelezettségeknek.[70] Ez a szabály az irányelv nemzeti végrehajtási rendelkezéseire, például az Elkertv-re is vonatkozik, amely releváns az információs társadalommal összefüggő szolgáltatásokat nyújtó, Magyarországon letelepedett szolgáltatók esetében. Ezért az Elkertv. 13/A. §-ának speciális rendelkezései *elsőbbséget élveznek* a GDPR rendelkezéseivel szemben, így ezek a szabályok alkalmazandók, amennyiben egy platform személyes adatokat kezel a végfelhasználói eszközökön történő információ tárolása és ahhoz történő hozzáférés során. A személyes adatok ezt követő kezelésére, amely csak az eszközről történő adatlekérés révén válik lehetővé, és amelyet semmilyen különös szabályozás nem fed le, ismét a GDPR általános követelményei vonatkoznak. 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.

2.2 Az adatkezelői státusz és ennek meghatározása

Az „*adatkezelő*” az európai adatvédelmi jog központi fogalma, az személy, aki a személyes adatok kezelésének céljait és eszközeit meghatározza. A GDPR 4. cikk 7. pontja értelmében „*adatkezelő*" az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog írja elő, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is kijelölheti. A GDPR 4. cikkének 8. pontja szerint az „*adatfeldolgozó*” olyan természetes vagy jogi személy, hatóság, ügynökség vagy más szerv, amely az adatkezelő nevében személyes adatokat kezel.

Az adatkezelő az a személy vagy szervezet, aki fogva felelős a GDPR adatvédelmi rendelkezéseinek betartásáért.[71] Az adatkezelő „az adatok ura”, akinek az elsődleges érdekében történik a személyes adatok kezelése.[72] Az adatkezelő tehát a GDPR szerinti kötelezettségek címzettje és annak kijelölése az adatvédelmi kötelezettségekkel kapcsolatos *felelősség telepítését* szolgálja. Az adatkezelő azonosítása, kijelölése és az ezzel kapcsolatos

[70] Vö. 5/2019. számú EDPB vélemény; 4.3 pont;
[71] Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), Datenschutzrecht. DSGVO mit BDSG (Nomos 2019), 1. Auflage; Artikel 4. Nr 7.; p. 329
[72] Knyrim (Hrsg), Praxishandbuch Datenschutzrecht, 4. Auflage; Manz; Rn. 3.38, p. 36.

kötelezettségek telepítése *nem a felek szabad megállapodásának tárgya*, hanem az adatvédelmi jogszabályok közjogi jellegét figyelembe véve *a felek tényleges tevékenységét* szükséges ehhez figyelembe venni.

Az adatkezelői státusz meghatározása nem mindig egyértelmű, különösen az online platformok esetében, ahol az adatkezelési folyamatok bonyolultak és gyakran több szereplő vesz részt az adatkezelési folyamatokban. 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, 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. Ezen komplexitás oka a digitális tér architektúrájából fakad, azaz hiába óriásiak ezek az online platformok, több, a működésükhöz szükséges szolgáltatások, mint pl. CDN-ek [content delivery network], fraud detection megoldások vagy éppen célzott hirdetés szolgáltatók [pl. ad networks] tőlük független, vagy a cégcsoportjukba tartozó, de önálló harmadik felek. Az adatvédelmi szabályozás célja, 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 személy, mint adatkezelők, illetve adatfeldolgozók láncolata vesz részt az adatkezelésben és ez a magasabb kockázati szint szigorúbb felelősségi elvárásokat indukál az adatkezelésben közreműködőkkel szemben[73], amely különösen releváns online platformok bonyolult adatkezelési láncait és kiszervezéseit figyelembe véve. A német DSK közös adatkezelésről szóló iránymutatása szerint a közös adatkezelés esetei nem ritkán növelhetik az érintett személyek jogaira és szabadságaira

[73] vö. Liber Ádám - Bereczki Tamás: Közreműködők adatvédelmi jogállása; JK, 2019/12., 506-507.

vonatkozó kockázatokat, így adott esetben indokolt lehet az adatvédelmi hatásvizsgálat lefolytatása a GDPR 35. cikke alapján[74], ez azonban minden esetben egyedi mérlegelést igényel.[75]

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 95/46 irányelv szerinti "adatkezelő" fogalmának értelmezése tekintetében az EU Bíróság a *C-210/16. sz. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein kontra Wirtschaftsakademie Schleswig-Holstein GmbH ügyében*[76] döntött úgy, hogy meg kell vizsgálni, hogy az Facebook-on nyilvánosan elérhető rajongói oldal üzemeltetője (jelen esetben a Wirtschaftsakademie) az Facebook Ireland és az Facebook Inc. társaságokkal együtt hozzájárul-e és milyen mértékben a rajongói oldal látogatóinak személyes adatai kezelésének céljairól és módjáról szóló döntéshez, és így „adatkezelőnek” tekinthető-e (31. pont). Az eset tényállása szerint a Wirtschaftsakademie Schleswig-Holstein oktatással foglalkozó, németországi társaság, aki a Facebookon hozott létre egy rangói oldalt, amely bárki számára nyilvánosan hozzáférhető volt az interneten. Mivel az oldalt a Facebook platformján üzemeltették, a Facebook által kínált cookie-kal és egyéb technológiai megoldásokkal, így a Facebook által kínált adminisztrátori, analitikai szolgáltatásokhoz fért hozzá a Wirtschaftsakademie Schleswig-Holstein. A Wirtschaftsakademie a szolgáltatással

[74] DSK, Kurzpapier Nr. 16 (Fn. 27), S. 4: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf; lehívás: 2024.09.16

[75] Der Bayerische Landesbeauftragte für den Datenschutz Gemeinsame Verantwortlichkeit Orientierungshilfe; Version 1.0, Stand: 1. Juni 2024; p. 58; https://www.datenschutz-bayern.de/infothek/OH_Gemeinsame_Verantwortlichkeit.pdf; lehívás: 2024.09.15

[76] 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).

kapcsolatosan nem fért hozzá érintett rajongók személyes adataihoz, mivel kizárólag statisztikai, aggregált adatokat kapott a Facebook-tól. A Wirtschaftsakademie arra hivatkozott, hogy ő maga nem adatkezelő, mivel kizárólag a Facebook kezeli a személyes adatokat. Az adatkezelő fogalmát ezzel szemben az EU Bíróság *kiterjesztően értelmezte* és kimondta, hogy a Wirtschaftsakademie Schleswig-Holstein GmbH és a Facebook Ireland Ltd. közös adatkezelők a rajongói oldal üzemeltetésének vonatkozásában. Kimondta a Bíróság, hogy a Facebook által felkínált platform létrehozásával és használatával a Wirtschaftsakademie Schleswig-Holstein GmbH lényegében a Facebookkal közösen döntött az adatkezelés eszközéről és céljáról, tehát arról, hogy a Facebook a rajongói oldal látogatóinak végfelhasználói berendezésére cookie-kat helyezhessen. A Wirtschaftsakademie meghatározhatta azokat a paramétereket (különösen a Facebook által rendelkezésre bocsátott filterek felhasználásával), melyek alapján a látogatókat reklámokkal célozhatta, amely ezzel befolyásolta a személyes adatok analitikai célú kezelését a Facebook részéről. Ezen szempontok mérlegelésekor a Bíróság figyelembe vette, hogy a használt platform mellett lehetősége volt az interneten bárkinek megtekintenie a Wirtschaftsakademie Schleswig-Holstein GmbH oldalát akár Facebook regisztráció nélkül is.

A Wirtschaftsakademie döntés összhangban volt a 29. cikk szerinti adatvédelmi munkacsoport az „adatkezelő" és az „adatfeldolgozó" fogalmáról szóló 1/2010 számú véleményével, ami szintén megerősítette, hogy "*... egyrészt az adatokhoz való hozzáférés önmagában nem jár adatkezeléssel, az adatokhoz való hozzáférés nem elengedhetetlen feltétele az adatkezelői minőségnek. Így a többszereplős, összetett rendszerekben a személyes adatokhoz való hozzáférést és az érintettek egyéb jogait különböző szinteken különböző szereplők is biztosíthatják*."[77] Az adatkezelő fogalom-meghatározásának ugyanis nem része az adatok birtoklása. Ezért nem lehet azzal érvelni, hogy a közös adatkezelők valamelyike nincs az adatok birtokában és nem fér hozzá az adatokhoz, ha az adatkezelés céljának és (vagy) eszközeinek meghatározásában mindkét fél részt vállal. Mint az Európai Unió Bírósága is megerősítette ebben az ügyben, a közös adatkezelők felelőssége nem feltétlenül ugyanaz az adatkezelésért. A különböző adatkezelők sok esetben különböző szakaszokban és különböző mértékben lehetnek felelősek a személyes adatok kezeléséért. Az adatvédelemi jogi szabályozás célja, hogy többes

[77] 29. cikk szerinti adatvédelmi munkacsoport 1/2010. számú véleménye az „adatkezelő" és az „adatfeldolgozó" fogalmáról (WP 169); 22. o.; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_hu.pdf; lehívás: 2024.09.09

adatkezelési szituációkban is egyértelmű legyen az adatvédelmi szabályok betartásáért és az e szabályok esetleges megszegéséért való felelősséget, annak elkerülése érdekében, hogy *csökkenjen a személyes adatok védelmi szintje* a többes adatkezelés okán.[78]

Egy másik ítéletben, a *C-40/17. sz. Fashion ID GmbH & Co KG ügyben*[79] az EU Bíróságnak egy olyan esetet kellett értékelnie, amelyben egy Facebook oldal üzemeltetője azáltal, hogy az Facebook Ireland „Like" gomb modulját beépítette a weboldalába, lehetővé tette a weboldalára látogatók személyes adatainak gyűjtését. Az adatok gyűjtése az ilyen oldalra való belépés pillanatától kezdve megkezdődött, függetlenül attól, hogy ezek a látogatók tagjai-e az Facebook közösségi hálózatnak, hogy rákattintottak-e az Facebook „Like" gombra, vagy hogy egyáltalán tudomásuk van-e erről a folyamatról (EUB C-40/17. sz. ügy, 75. pont). Azok a személyesadat-kezelési műveletek, amelyek céljait és módját a Facebook Irelanddel együtt a Fashion ID határozhatja meg, a „személyes adatok kezelése" fogalmának a 95/46 irányelv 2. cikkének b) pontjában szereplő meghatározására tekintettel a Fashion ID honlapjára látogatókra vonatkozó személyes adatok gyűjtésének és továbbítás általi közlésének minősül. Az említett információk alapján azonban első látásra kizártnak tűnik, hogy a Fashion ID határozná meg azoknak a későbbi személyesadat-kezelési műveleteknek a céljait és módját, amelyeket a Facebook Ireland végez el a személyes adatok Fashion ID általi továbbítását követően, és ezért a Fashion ID e műveletek tekintetében nem minősíthető a 2. cikk d) pontja értelmében vett adatkezelőnek. Azzal kapcsolatban, hogy milyen módot használt a Fashion ID a honlapjára látogatók személyes adatainak gyűjtésére és továbbítás általi közlésére, úgy tűnt, hogy a Fashion ID annak ellenére helyezte el honlapján a Facebook Ireland által a honlap-üzemeltetők rendelkezésére bocsátott Facebook „Like" gombot, hogy tisztában volt azzal, hogy olyan eszközről van szó, amely a honlap látogatóira vonatkozó személyes adatok gyűjtésére és továbbítás általi közlésére szolgál, függetlenül attól, hogy a látogatók tagjai-e a Facebook közösségi hálózatnak. A Fashion ID másfelől ennek a közösségi modulnak a honlapján történő elhelyezésével döntően az említett modul szolgáltatója, vagyis a Facebook Ireland javára befolyásolja az említett honlap látogatóira vonatkozó személyes adatok gyűjtését és továbbítás általi közlését, amelyekre az említett modul elhelyezése nélkül nem kerülne sor. E

[78] vö. 29. cikk szerinti adatvédelmi munkacsoport 1/2010. számú véleménye az „adatkezelő" és az „adatfeldolgozó" fogalmáról (WP 169); 24. o. és ezzel összhangban EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.1, Adopted on 07 July 2021; 163. pont 44. o.
[79] Európai Unió Bírósága, C-40/17. sz., Fashion ID kontra Facebook Ireland ügyben 2019. július 29-én hozott ítélet (ECLI:EU:C:2019:629).

körülményekre, figyelemmel az EU Bíróság megállapította, hogy a Facebook Ireland és a Fashion ID közösen határozták meg a Fashion ID honlapjának látogatóira vonatkozó személyes adatok gyűjtésének és továbbítás általi közlésének alapjául szolgáló műveletek módját és közös adatkezelőnek minősültek. Az adatkezelői minőség azonban csak arra a személyesadat-kezelési műveletre vagy műveletcsoportra vonatkozott, amelynek céljait és módját ténylegesen ő határozza meg, azaz a szóban forgó adatok gyűjtésére és továbbítás általi közlésére.

A fent bemutatott 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, melyet az Európai Unió Bírósága a *C-604/22. számú IAB Europe ügyben* hozott 2024. március 7.-i döntésében[80] is megerősített. Ebben az ügyben a Bíróság szerint az IAB Europe közös adatkezelőnek minősült, mivel az általa létrehozott és általa egyesületi szabályok által kikényszerített „Transparency & Consent Framework" [TCF] keretében a tagjai adatkezelésének céljait és eszközeit befolyásolta. Ezen ügy háttere az IAB Europe által létrehozott TCF alkalmazásának megítélése az adatkezelői pozíció meghatározása szempontjából, amely IAB keretrendszer az adatok kezelésének átláthatóságát és a felhasználói hozzájárulások kezelését hivatott elősegíteni. A Bíróság ezzel kapcsolatosan megállapította, hogy a személyes adatok kezeléséhez való hozzájárulást érintően az IAB Europe, mint szakmai szervezet az általa létrehozott, a kötelező technikai szabályokon túlmenő olyan előírásokat tartalmazó szabálykeretet hozott létre és kényszerített ki, amely részletesen meghatározza, hogy milyen módon kell tárolni és terjeszteni a hozzájárulásra vonatkozó személyes adatokat. A Bíróság ezzel kapcsolatosan rögzítette, hogy az IAB-ot „közös adatkezelőnek" kell tekinteni, ha ezzel saját céljaiból befolyást gyakorol az érintett személyes adatok kezelésére, és ennélfogva tagjaival együtt meghatározza az ilyen adatkezelés célját és eszközeit. Ez a megállapítás azt jelenti, hogy a TCF kereteit alkalmazó szolgáltatóknak figyelembe kell venniük a közös adatkezelésre vonatkozó kötelezettségeiket, és nincs jelentősége annak, hogy az IAB Europe nem fér hozzá közvetlenül a tagok által kezelt adatokhoz, illetve az adatokhoz hozzáférés sem zárja ki a közös adatkezelői minőséget. A Bíróság tehát egyértelművé tette,

[80] Európai Unió Bírósága, 2024 március 07. sz. ítélet, C-604/22. sz. ügy, az IAB Europe és a Gegevensbeschermingsautoriteit (belga adatvédelmi hatóság) között (ECLI:EU:C:2024:214)

hogy az IAB Europe a tagjainak címzett adatkezelési szabályok kialakítása és az érintettek hozzájárulásának kezelése kapcsán közös adatkezelő és ezáltal a tagjaival osztozott a GDPR 26. cikkében meghatározott kötelezettségekben, függetlenül attól, hogy közvetlen hozzáféréssel nem rendelkezik az adatokhoz

A közös adatkezelés azt jelenti, hogy *mindegyik 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[81] 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, melynek azonban nem szükséges alakszerű formát öltenie[82]. Ennek a megállapodásnak tartalmaznia kell az érintettek jogainak biztosítását szolgáló intézkedéseket is. Nem követelhető meg az, hogy az adatkezelők között alakszerű megállapodás jöjjön létre az adatkezelés céljait és eszközeit illetően. 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 egyértelmű a felek közötti felelősség megosztása a személyes adatok kezelése tekintetében.

A platformszolgáltatók meghatározzák és ellenőrzik a személyes adatok kezelésének általános eszközeit a platformjukon azáltal, ha maguk alakítják ki az ún. határ-erőforrásokat, mint például az API[83]-kat, SDK[84]-kat, amelyek felépítik az adott típusú felhasználói adatokhoz való hozzáférés eszközeit és korlátait a szolgáltatásaik számára, mivel ezáltal befolyásolják azokat az eszközöket és célokat, amelyekre a személyes adatokat a platformon kezelni lehet. A határ-

[81] vö. GDPR 26. cikk (2) bekezdése
[82] vö. Európai Unió Bírósága, 2023. december 5-i Nacionalinis visuomenės sveikatos centras ítélet, C-683/21, EU:C:2023:949, 43. és 44. pontja
[83] Az API jelentése "Application Programming Interface" (alkalmazásprogramozási felület). Az API egy olyan meghatározott szabályok és protokollok gyűjteménye, amely lehetővé teszi, hogy különböző szoftveralkalmazások vagy komponensek kommunikáljanak egymással. Az API biztosítja az interfészt, amelyen keresztül egy program elérheti egy másik program funkcióit, adatbázisokat vagy webszolgáltatásokat anélkül, hogy azok belső működésébe közvetlenül beavatkozna. Például egy webes API lehetővé teszi egy mobilalkalmazás számára, hogy adatokat kérjen egy távoli szervertől vagy szolgáltatástól (pl. időjárás-jelentés, fizetési rendszer).
[84] SDK / „Software Development Kit" (szoftverfejlesztő készlet). Az SDK olyan eszközök, könyvtárak és dokumentációk gyűjteménye, amelyek segítik a fejlesztőket alkalmazások létrehozásában egy adott platformra, rendszerre vagy programozási nyelvre. Az SDK-k tartalmazhatnak API-kat, fejlesztői eszközöket, példakódokat, és akár tesztelési keretrendszereket is, hogy megkönnyítsék az adott platformra történő szoftverfejlesztést.

erőforrások tehát szabályozzák és strukturálják a platform és a külső szolgáltatók közötti interakciókat, beleértve azt is, hogy hogyan és milyen célból kezelhetők a személyes adatok. A platformok adatkezelésében tehát azért minősülnek közös adatkezelőként a szolgáltatók, mivel e tevékenységükkel befolyásolják a szolgáltatásaikat felhasználó más szereplők adatkezelési tevékenységeit. A határ-erőforrások jelentős hatással lehetnek az adatvédelmi szabályozásra, mivel a platformszolgáltatók ezen erőforrások kialakításán keresztül nagy befolyást gyakorolhatnak az adatkezelési gyakorlatokra, az adatvédelmi megfelelésre és az elszámoltathatósági kötelezettségekre.[85] Az adatkezelési módok és a célok meghatározása pedig GDPR szerint felelősséggel és kötelezettségekkel jár.

2.3 Adatvédelmi alapelvek érvényesülése online platformok esetén

A GDPR által követett, a rendelet 1. cikkéből, valamint 1. és 10. preambulumbekezdéséből következő célkitűzés arra irányul, hogy biztosítsa a természetes személyek alapvető jogainak és szabadságainak, különösen a magánélet tiszteletben tartásához való jognak a magas szintű védelmét a személyes adatok kezelése tekintetében, amelyet az Alapjogi Charta 8. cikkének (1) bekezdése és az EUMSZ 16. cikk (1) bekezdése rögzít.[86] E célkitűzésnek megfelelően a személyes adatok kezelésének meg kell felelnie többek között a GDPR 5. cikkében foglalt, az ilyen adatok kezelésére vonatkozó elveknek, és meg kell felelnie a jogszerűségre vonatkozóan a GDPR 6. cikkében felsorolt jogszerűségi feltételeknek[87], amely online platformok adatkezelése esetén is irányadó.

A fentiekben bemutattuk, hogy az online platformok alapvetően *adatkezelőnek*, más üzleti platform felhasználóval jellemzően *közös adatkezelőnek* minősülnek és ekként *felelősek az adatvédelmi alapelvek betartásáért*. Az adatvédelmi alapelvek online platformok esetében alapvető fontosságúak, mivel ezek biztosítják, hogy a személyes adatok kezelése jogszerűen, tisztességesen és átlátható módon, a GDPR rendelkezéseivel összhangban történjen. Az Európai

[85] vö. 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 Technology, 9.; 7. o. https://www.sciencedirect.com/science/article/pii/S2666659621000111?via%3Dihub; lehívás: 2024.09.10
[86] vö. EU Bíróság 2024. március 7-i IAB Europe ítélet, C-604/22, EU:C:2024:214, 53. pont
[87] vö EU Bíróság 2024. július 11-i Meta Platforms Ireland [Képviseleti kereset] ítélet, C-757/22, EU:C:2024:598, 49. pont és a Koninklijke Nederlandse Lawn Tennisbond és az Autoriteit Persoonsgegevens C-621/22. sz. ügyben meghozott ítélet; ECLI:EU:C:2024:857; 27. pont

Bíróság a Meta Platforms Inc. és társai kontra Bundeskartellamt ügyben[88] kifejtette, hogy a GDPR 5. cikkében foglalt elszámoltathatósági követelményeknek megfelelően az adatkezelőre hárul annak bizonyítása, hogy ezeket az adatokat többek között meghatározott, egyértelmű és jogszerű célból gyűjtik, és hogy azok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végezzék.

2.3.1 Jogszerűség és jogalap kérdések

Az EU Alapjogi Chartájának 8. cikk (2) bekezdése értelmében személyes adatok kezelésére „*az érintett személy hozzájárulása alapján vagy valamilyen más, törvényben rögzített jogos okból*" kerülhet sor, ami általánosan az adatkezelés jogszerűségének követelményét fogalmazza meg, tehát azt, hogy a személyes adatok kezelése minden esetben valamely jogalapot, jogos okot feltételez. Ezen jogalapok *numerus clausus*-át a GDPR 6. cikk (1) bekezdés (a)-(f) pontjai rögzíti, amely rendelkezés felsorolja a személyes adatok kezelésének jogszerűségéhez szükséges lehetséges jogalapokat, ideértve az érintett hozzájárulását, szerződés teljesítését, jogi kötelezettség teljesítését, az érintett létfontosságú érdekeinek védelmét, közérdekű feladat végrehajtását vagy a közhatalmi jogosítvány gyakorlását, valamint az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítését.

Az adatkezelés „jogszerűsége" legszűkebb értelemben a megfelelő adatkezelési jogalap meglétére utal, míg az legtágabban azt jelenti, hogy a személyes adatok kezelésére csak a jogszabályokkal összhangban kerülhet sor[89]. Utóbbi követelmény alapján egy hozzájáruláson vagy szerződésen alapuló adatkezelés is lehet jogellenes, amennyiben az adatkezelés jogszabályt sért[90]. Az adatkezelés jogszerűségéhez tehát nem elég csupán a megfelelő jogalap megléte; az adatkezelés teljes folyamatának összhangban kell lennie a vonatkozó jogszabályi

[88] Európai Unió Bírósága, C-252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság (ECLI:EU:C:2023:537); 95. pont; https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1; lehívás: 2024.08.25

[89] vö. Liber Ádám: A jogos érdeken alapuló adatkezelésről – 2012/2. (49.), 79. o.; Infokommunikáció és jog; https://infojog.hu/liber-adam-a-jogos-erdeken-alapulo-adatkezelesrol-20122-49-79-88-o/; lehívás: 2024.09.13

[90] Vö. Stewart, Room – Data Protection and Compliance in Context – BCS, 2007, p. 103; az adatkezelés tartalmi jogellenességének példája lehet az adatvédelmi biztos 26/A/2006-12. számú ügye, melyben a fogyasztói hozzájárulás mellett postai úton kiküldött dohányreklámokkal kapcsolatos adatkezelést minősített jogellenesnek az adatvédelmi biztos, mivel az – bár formálisan hozzájáruláson alapult, ám a biztos álláspontja szerint az az általános dohányreklám-tilalomba ütközött.

rendelkezésekkel. Ha az adatkezelés bármely része sérti a jogszabályokat, akkor az egész adatkezelés jogellenesnek tekinthető.

Az online platformok alapvetően adatkezelőként, adott esetben más platform felhasználóval közös adatkezelőként járnak el és kötelesek a személyes adatokat a GDPR által meghatározott egy vagy több jogalap alapján kezelni. A GDPR 6. cikkének (1) bekezdése meghatározza azokat a jogalapokat, amelyek alapján az online platformok (és más adatkezelők) jogosultak személyes adatokat kezelni. Minden adatkezelési tevékenységnek legalább egy ilyen jogalapon kell alapulnia ahhoz, hogy az jogszerű legyen. Személyes adatok kezelésével járó tevékenységek kezdeményezésekor egy online platformnak, mint adatkezelőnek mindig mérlegelnie kell, hogy mi lenne a megfelelő jogalapja egy tervezett adatkezeléshez.

Az Európai Bíróság a *Meta Platforms Inc. és társai kontra Bundeskartellamt ügyben*[91] részletesen foglalkozott azon jogalap kérdésekkel, melyet online platformok a személyes adatok kezelése során igénybe vehetnek és utalt az igénybe vehető adatvédelmi jogalapok zárt körére, tehát arra, hogy a GDPR *kimerítő és korlátozó jelleggel* meghatározza azokat az eseteket, amelyekben a személyes adatok kezelése jogszerűnek tekinthető.[92] A GDPR 6. cikke (1) bekezdése első albekezdésének a) pontja értelmében a személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben az érintett *hozzájárulását adta* személyes adatainak egy vagy több konkrét célból történő kezeléséhez. Ilyen hozzájárulás hiányában, vagy ha e hozzájárulást nem önkéntesen, konkrétan, megfelelő tájékoztatás alapján és egyértelműen adták meg GDPR értelmében, az ilyen adatkezelés mindazonáltal akkor is indokolt lehet, ha megfelel az a GDPR 6. cikke (1) bekezdése első albekezdésének b)–f) pontjában említett *szükségességi követelmények* valamelyikének. Az ezen rendelkezésekben előírt indokokat, amennyiben azok lehetővé teszik, hogy az érintett hozzájárulásának hiányában végzett személyesadat-kezelést jogszerűnek lehessen tekinteni, viszont *megszorítóan kell értelmezni*.[93] Amennyiben megállapítható, hogy valamely személyesadat-kezelés a GDPR 6. cikke (1) bekezdése első

[91] Európai Unió Bírósága, C-252/21. sz. Meta Platforms Inc. & Others v német versenyhatóság ügy (ECLI:EU:C:2023:537); 91-94 pontok; https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1; lehívás: 2024.08.25

[92] Európai Unió Bírósága, C-252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság, 90. pont

[93] vö. Európai Unió Bírósága, 2022. február 24-i Valsts ieņēmumu dienests [Személyes adatok adóügyi célból történő kezelése] EUB ítélet, C-175/20, EU:C:2022:124, 73. pont, valamint az ott hivatkozott ítélkezési gyakorlat.

albekezdésének b)–f) pontjában előírt indokok valamelyikére tekintettel szükséges, nem kell meghatározni, hogy ezt az adatkezelést ezen indokok közül egy másik is indokolja-e[94].

Az ePrivacy irányelv rendelkezései a GDPR általános szabályai mellett szintén relevánsak a platformokra irányadó megfelelő adatkezelési jogalap megválasztása tekintetében. Az ePrivacy irányelv ugyanis az információs társadalommal kapcsolatos szolgáltatások területén „*pontosítja és kiegészíti*" a GDPR rendelkezéseit. Az ePrivacy irányelvnek az ún. „forgalmi adatok" kezelésére vonatkozó 6. cikke például egy olyan eset, amikor ePrivacy irányelv „pontosítja" a GDPR rendelkezéseit. Általánosságban véve a személyes adatok kezelése a GDPR 6. cikkében említett jogszerű indokok bármelyike alapján indokolható. Ugyanakkor egy szolgáltató a forgalmi adatok kezelésének indokaként nem alkalmazhatja a GDPR 6. cikkében felsorolt lehetséges jogszerű indokok mindegyikét, mert az ePrivacy irányelv 6. cikke kifejezetten korlátozza a forgalmi adatok – köztük a személyes adatok – kezelésének feltételeit. Ebben az ePrivacy irányelv konkrétabb rendelkezései *lex specialis-ként* elsőbbséget élveznek a GDPR általánosabb rendelkezéseivel szemben[95].

2.3.1.1 Az érintett hozzájárulása [GDPR 6. cikk (1) a) pont]

Az online platformok jogszerűen kezelhetik a személyes adatokat, ha az érintett személy *egyértelműen hozzájárult* adatainak kezeléséhez egy vagy több konkrét célra. A GDPR 4. cikk 11. pontjában foglalt meghatározás szerint „*az érintett hozzájárulása*" az érintett akaratának *önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása*, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez. Az Európai Adatvédelmi Testület a 5/2020 sz. iránymutatásában[96] , melyet többször pontosítottak, értelmezte részletesen a GDPR szerinti hozzájárulás követelményeit és kifejti az érvényes hozzájárulás megszerzésére és bizonyítására vonatkozó követelményeket, melyek a hozzájárulás megadásának

[94] vö. Európai Unió Bírósága, 2022. augusztus 1-jei Vyriausioji tarnybinės etikos komisija EUB ítélet, C-184/20, EU:C:2022:601, 71. pont
[95] vö. EDPB - 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, 39. sarokpont
[96] EDPB Guidelines 05/2020 on consent under Regulation 2016/679; https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en; lehívás: 2024.09.07

érvényességi feltételei és ha bármelyik hiányzik, akkor nem lehet a hozzájárulásra, mint érvényes jogalapra támaszkodni.

2.3.1.1.1 Önkéntesség

A hozzájárulás általában csak akkor lehet megfelelő jogalap, ha az érintett számára felajánlják, hogy maga rendelkezzen az adatok felett és *valódi választási lehetőséget* biztosítanak számára a felajánlott feltételek elfogadásához vagy elutasításához, illetve azok károkozás nélküli elutasításához, illetőleg visszavonásához (vö. GDPR 7. cikk (3) bekezdése). Ebből a szempontból kritikusan fontos a hozzájárulás önkéntessége, melynek kritériumait a hivatkozott iránymutatás 3.1 pontja taglalja. A hozzájárulás kizárólag akkor lehet érvényes, ha az érintett élni tud a valódi választás lehetőségével, és a hozzájárulás megtagadása esetén nem áll fenn a *megtévesztés*, a *megfélemlítés*, a *kényszerítés* vagy más jelentős *negatív következmény* (például jelentős többletköltségek) kockázata. A hozzájárulás nem önkéntes olyan esetekben, ha kényszer, nyomás vagy a szabad akarat gyakorlására való képtelenség bármely eleme felmerül.[97] Ha a felek (adatkezelő és érintett között) egyenlőtlen hatalmi feltételek állnak fenn, az nem jelenti azt, hogy hozzájárulás érvénytelen, azonban ez gyakorlatilag vélelmet keletkeztet, hogy a hozzájárulás nem önkéntes és az adatkezelő ekkor bizonyíthatja, hogy a hozzájárulás ténylegesen önkéntes és a feltételei fennállnak.[98]

Az Európai Bíróság a *Meta Platforms Inc. és társai kontra Bundeskartellamt* ügyben megerősítette[99] az Európai Adatvédelmi Testület fent bemutatatott gyakorlatát és kimondta, hogy a hozzájárulás olyan egyedi esetekben nem szolgálhat érvényes jogalapként a személyes adatok kezeléséhez, amelyekben az érintett és az adatkezelő között egyértelműen *egyenlőtlen viszony* áll fenn. Az Európai Bíróság döntése ebben ügyben fontos precedenst teremtett a személyes adatok kezelésének hozzájárulás-alapú jogalapja kapcsán, különösen olyan esetekben, amikor az adatkezelő és az érintett között egyértelműen egyenlőtlen viszony áll fenn. A bíróság megerősítette az Európai Adatvédelmi Testület korábbi gyakorlatát, amely szerint az egyenlőtlen viszonyban lévő felek esetében a hozzájárulás nem tekinthető érvényesnek a személyes adatok kezeléséhez. A Bíróság a GDPR 43. preambulumbekezdésére hivatkozott,

[97] vö. EDPB Guidelines 05/2020 on consent under Regulation 2016/679, 24. sarokpont
[98] vö. EDPB Guidelines 05/2020 on consent under Regulation 2016/679; 22. sarokpont
[99] Európai Unió Bírósága – C-252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság (ECLI:EU:C:2023:537); 91-94 pontok; 143-144 pontok.

amely kimondja, hogy ha egy adott adatkezelési művelethez nincs lehetőség külön hozzájárulás adására, akkor vélelmezni kell, hogy a hozzájárulás nem önkéntes. Ez különösen akkor fontos, ha a felhasználók választási szabadságát korlátozza az a tény, hogy nem tudják megtagadni vagy visszavonni a hozzájárulást anélkül, hogy az hátrányos következményekkel járna számukra. A döntés értelmében a Meta, mint a Facebook üzemeltetője, jelentős erőfölényben van, ami önmagában nem zárja ki, hogy a felhasználók érvényes hozzájárulást adjanak személyes adataik kezeléséhez. Azonban *az ilyen erőfölény befolyásolhatja a hozzájárulás érvényességét*, különösen annak önkéntességét. Ha a felhasználóknak nincs valódi lehetőségük visszavonni a hozzájárulást anélkül, hogy ez számukra hátrányos lenne, az a hozzájárulás önkéntességét kérdőjelezheti meg. A Bíróság hangsúlyozta, hogy az adatkezelési műveleteknek szükségesnek kell lenniük a szolgáltatás nyújtásához. A Meta által végzett adatkezelési műveletek – különösen a Facebook felhasználók közötti szerződés teljesítése érdekében – nem minden esetben tűnnek szükségesnek. Ennek megfelelően a felhasználóknak lehetőséget kell biztosítani arra, hogy a szerződés teljesítéséhez nem szükséges adatkezelési műveleteket külön megtagadják, anélkül, hogy ez a szolgáltatás igénybevételének teljes lemondását eredményezné. A bíróság emellett kimondta, hogy az ilyen helyzetekben alternatív lehetőséget kell biztosítani a felhasználók számára, amely lehetőséget ad a szolgáltatás használatára anélkül, hogy ehhez nem szükséges adatkezelési műveletek történnének. Ez különösen fontos olyan esetekben, amikor a felhasználók nem számítanak arra, hogy az online közösségi hálózat üzemeltetője olyan adatokat kezel, amelyek nem közvetlenül kapcsolódnak a szolgáltatás nyújtásához. A bíróság ezzel arra utal, hogy külön hozzájárulást kell biztosítani például az "off Facebook" adatok kezeléséhez, így a felhasználóknak valós választási lehetőséget biztosítva. Ez a döntés megerősíti azt az elvet, hogy a hozzájárulás akkor tekinthető érvényesnek, ha azt önkéntesen és valódi választási lehetőségek mellett adják meg, különösen egyenlőtlen viszonyok esetén, ahol az adatkezelő erőfölénye befolyásolhatja a felhasználó döntési szabadságát.[100]

2.3.1.1.2 Konkrét

A GDPR 6. cikk (1) bekezdésének a) pontja megerősíti, hogy az érintett hozzájárulását „*egy vagy több konkrét*” céllal összefüggésben kell megadni, és hogy az érintettnek mindegyik céllal

[100] Európai Unió Bírósága – C-252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság (ECLI:EU:C:2023:537); 91-94 pontok; 147-151 pontok

összefüggésben választási lehetősége van. A „célok” meghatározásával kapcsolatban további útmutatás a célhoz kötöttségről szóló 3/2013. számú véleményben (WP 203) található. Az a követelmény, hogy a hozzájárulásnak „konkrétnak” kell lennie, annak biztosítását célozza, hogy a felhasználó bizonyos mértékben rendelkezzen az adatok felett, az érintett számára pedig biztosítható legyen bizonyos mértékű átláthatóság. Az Európai Adatvédelmi Testület ezen véleménye szerint a konkrét hozzájárulás szükségessége, valamint a célhoz kötöttség fogalma az adatkezelési célok fokozatos bővülése vagy elmosódása elleni garanciaként működik, miután az érintett hozzájárult az eredeti adatgyűjtéshez. A hozzájárulásnak kifejezetten a célhoz kell kapcsolódnia. Az érintettek úgy adják meg a hozzájárulásukat, ha megértik, hogy rendelkeznek az adataik felett, és az adataik kizárólag a meghatározott célokból kerülnek kezelésre. A hozzájárulási mechanizmusoknak nemcsak részletesnek kell lenniük az „önkéntes” követelmény teljesítéséhez, hanem eleget kell tenniük a „konkrét” elemnek is. Ez azt jelenti, hogy annak az adatkezelőnek, aki/amely különféle eltérő célokra kér hozzájárulást, külön hozzájárulási lehetőséget kell biztosítania mindegyik célhoz, annak érdekében, hogy a felhasználók konkrét célokra konkrét hozzájárulást adhassanak.

2.3.1.1.3 Tájékozottság

A GDPR előírja, hogy a hozzájárulásnak megfelelő tájékoztatáson alapulónak kell lennie, az átláthatóság alapelvére támaszkodva. A „tájékoztatáson alapuló” hozzájáruláshoz szükséges tartalmi minimumkövetelmények[101] között szerepel, hogy az érintettet tájékoztatni kell az adatkezelő kilétéről, azaz arról, hogy ki fogja kezelni a személyes adatait. Ezen kívül világosan meg kell határozni, hogy milyen célra kérik a hozzájárulást. Továbbá az érintettet tájékoztatni kell arról, hogy milyen típusú személyes adatok kerülnek gyűjtésre és felhasználásra. Szintén fontos elem, hogy az érintettet tájékoztassák a hozzájárulás visszavonásának jogáról (vö. GDPR 7. cikk (3) bekezdése), valamint, hogy adott esetben az adatokat érintő automatizált döntéshozatalról, illetve az adattovábbítás kockázatairól, ha például harmadik országokba továbbítják az adatokat. Ezek az elemek együttesen szükségesek ahhoz, hogy a hozzájárulás megfelelő tájékoztatáson alapulónak minősüljön, ami a hozzájárulás megadásának érvényességi feltétele. A tájékoztatást egyértelmű, közérthető módon kell nyújtani, és nem

[101] vö. EDPB Guidelines 05/2020 on consent under Regulation 2016/679; 64-65. sarokpontok

rejthető el általános szerződési feltételekben[102]. A hozzájárulásnak megkülönböztethetőnek és különállónak kell lennie a többi információtól.[103]

2.3.1.1.4 Kívánság egyértelmű kinyilvánítása

A hozzájárulásnak minden esetben aktív, egyértelmű, és tájékozott cselekedetnek kell lennie, amely megelőzi az adatkezelést. A 29. cikk szerinti munkacsoport által kiadott korábbi hozzájárulással kapcsolatos útmutatással összhangban az Európai Adatvédelmi Testület egyértelművé tette, hogy az érvényes hozzájárulás nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján történő egyértelmű kinyilvánítást tesz szükségessé[104]. Az adatkezelők felelőssége, hogy biztosítsák a hozzájárulás megszerzésének folyamatát, és kerüljék az olyan mechanizmusokat, amelyek félreérthetők vagy megkérdőjelezhetők. Ez azt jelenti, hogy az érintettnek egyértelműen ki kell fejeznie szándékát, hogy beleegyezik a személyes adatai kezelésébe. A hozzájárulás megszerzése nem történhet meg hallgatás, nem cselekvés, vagy egyszerűen egy szolgáltatás használatának folytatása révén. Az ilyen típusú passzív magatartások nem felelnek meg a GDPR követelményeinek[105]. Például az előre bejelölt jelölőnégyzetek használata nem tekinthető érvényes hozzájárulásnak, mint ahogyan azt az Európai Unió Bírósága a Planet49 ügyben[106] is megerősítette. A hozzájárulásnak mindig aktív nyilatkozattal vagy egyértelmű cselekedettel kell történnie, ami lehet például egy négyzet bejelölése, vagy egy írásbeli nyilatkozat. Másrészről a hozzájárulás megszerezhető írásban, elektronikusan, vagy rögzített szóbeli nyilatkozat formájában is. Az írásbeli hozzájárulás különböző formákat ölthet, de minden esetben biztosítani kell, hogy az érintett rendelkezésére állnak a megfelelő információk a hozzájárulás megadása előtt. Fontos kiemelni, hogy a hozzájárulás megszerzésének folyamata nem akadályozhatja szükségtelenül a szolgáltatás igénybevételét, amelyre a hozzájárulást kérik. Továbbá, az adatkezelőknek világosan elkülönített hozzájárulási mechanizmust kell kialakítaniuk. A hozzájárulás nem vonható össze más nyilatkozatokkal, mint például egy szolgáltatás általános szerződési feltételeinek elfogadása. Ennek megfelelően az adatkezelők nem használhatnak olyan

[102] vö. EDPB Guidelines 05/2020 on consent under Regulation 2016/679; 67. sarokpont
[103] Lásd még a GDPR (58) preambulumbekezdését a gyermekek számára érthető tájékoztatással kapcsolatban.
[104] vö. EDPB Guidelines 05/2020 on consent under Regulation 2016/679; 77. sarokpont
[105] vö. EDPB Guidelines 05/2020 on consent under Regulation 2016/679; 79. sarokpont
[106] vö. Európai Unió Bírósága C-673/17. számú, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH ügyben hozott, 2019. október 1-i ítélete (ECLI:EU:C:2019:801)

rendszereket, amelyek előre megjelölt opciókat tartalmaznak, és az érintettnek kellene cselekednie a beleegyezés megakadályozása érdekében („opt-out" rendszer) [107]. A GDPR szellemében a hozzájárulásnak mindig megelőznie kell az adatkezelési tevékenységet. Bár a GDPR nem írja elő kifejezetten, hogy a hozzájárulást az adatkezelés megkezdése előtt kell megszerezni, ez a hozzájárulás általános értelmezésből ez egyértelműen következik.

2.3.1.1.5 Gyermekek hozzájárulása

Gyermekek hozzájárulására szintén különleges követelmények vonatkoznak a GDPR alapján. A GDPR 8. cikke szerint a közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelése akkor jogszerű Magyarországon, ha a gyermek a 16. életévét betöltötte. A 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte. Egy online platformnak adatkezelőként ésszerű erőfeszítéseket kell tennie annak érdekében, hogy ellenőrizze az érintett életkorát. A 16 éves vagy annál idősebb gyermekeket képesnek kell tekinteni arra, hogy saját maguk adjanak hozzájárulást. GDPR lehetőséget ad az EU tagállamoknak arra, hogy nemzeti jogszabályaikban az interneten keresztül nyújtott szolgáltatások esetén a hozzájárulás korhatárát kiskorúak esetében 13 és 16 év között határozzák meg. Amennyiben a célközönségben vannak kiskorú érintettek, az Európai Adatvédelmi Testület hozzájárulásról szóló útmutatása szerint az adatkezelővel szemben elvárás, hogy meggyőződjön arról, hogy a tájékoztatás érthető a kiskorúak számára. Az adatkezelőknek a közönségük meghatározása után el kell dönteniük, hogy milyen tájékoztatást adjanak, ezután pedig azt, hogy a tájékoztatást hogyan fogják ismertetni az érintettekkel.[108]

2.3.1.1.6 Hozzájárulás igazolása

A GDPR elszámoltathatóságból eredő követelménye, hogy a hozzájárulás megadását az adatkezelőnek képesnek kell lennie igazolni, melyet a GDPR 7. cikk (1) bekezdése és a GDPR 42. preambulumbekezdése rögzít. A GDPR nem írja elő az igazolás konkrét módját, ezért ezzel kapcsolatosan az adatminimalizálási követelményeket szükséges figyelembe venni. Ebből a

[107] vö. EDPB Guidelines 05/2020 on consent under Regulation 2016/679; 81. sarokpont
[108] vö. EDPB Guidelines 05/2020 on consent under Regulation 2016/679; 70. sarokpont

szempontból lényeges a hozzájárulás megadásának igazolhatósága, tehát olyan „*audit trail*” kialakítása, ami képes arra, hogy az hozzájárulás megadását az adatkezelés időtartama alatt igazolni tudja. Az angol UK ICO vonatkozó útmutatója szerint[109] a hozzájárulás dokumentálásának tartalmaznia kell, hogy (i) *ki adta a hozzájárulást*, például az érintett nevét vagy más azonosítót, mint az online felhasználónév vagy a munkamenet azonosítója. Rögzíteni kell, hogy (ii) *mikor történt* a hozzájárulás megadása, például egy dátummal ellátott dokumentum vagy online nyilvántartás esetén időbélyeggel, illetve szóbeli hozzájárulás esetén egy jegyzetet kell készíteni a beszélgetés időpontjáról. Szintén dokumentálni kell, hogy (iii) *az érintett milyen tájékoztatást* kapott a hozzájárulás idején: ehhez szükséges egy példány az akkor használt hozzájárulási nyilatkozatról, valamint a kapcsolódó adatvédelmi tájékoztatók és egyéb információk verziószámmal és dátummal. Fontos rögzíteni azt is, hogy (iv) *hogyan adták meg a hozzájárulást*: írásos hozzájárulás esetén a megfelelő dokumentum másolatát, online hozzájárulás esetén az elküldött adatok időbélyeggel együtt. Szóbeli hozzájárulás esetén jegyzetet kell készíteni a beszélgetés idején, de nem szükséges a teljes beszélgetés részleteit rögzíteni. Végül pedig nyilvántartani kell azt is, ha az érintett *visszavonta a hozzájárulását*, és azt is, hogy mikor történt ez meg, ami az adatkezelő elszámoltathatósággal kapcsolatos dokumentációs kötelezettségeivel kapcsolatos elvárásokat mutatja, különösen az online térben. Az Európai Adatvédelmi Testület szerint az adatkezelés befejezését követően a hozzájárulás bizonyítékát csak a feltétlenül szükséges ideig kell megőrizni jogi kötelezettség teljesítése vagy jogi igények előterjesztése, érvényesítése vagy védelme érdekében, összhangban a GDPR 17. cikk (3) bekezdésének b) és e) pontjaival.[110]

2.3.1.1.7 Hozzájárulás az ePrivacy szabályok alapján

A hozzájárulásnak, mint jogalapnak kiemelt szerepe van információs társadalommal kapcsolatos szolgáltatások kontextusában, mivel az ePrivacy irányelv 5. cikk (3) bekezdése szerint felhasználó végberendezésében történő adattároláshoz, illetve az ott tárolt adatokhoz való hozzáféréshez főszabály szerint a felhasználók hozzájárulása szükséges, ha az adattárolás vagy hozzáférés célja az elektronikus hírközlő hálózaton keresztül történő közléstovábbítás, vagy a felhasználó által kifejezetten kért, az információs társadalommal összefüggő szolgáltatás

[109] UK ICO - How should we obtain, record and manage consent? - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/how-should-we-obtain-record-and-manage-consent/; 2024.09.15
[110] vö. EDPB Guidelines 05/2020 on consent under Regulation 2016/679; 107. sarokpont

nyújtásához szükséges. ePrivacy irányelv 5. cikk (3) bekezdése szerinti hozzájárulásra a GDPR szerinti hozzájárulás fogalmat és annak kritériumait kell alkalmazni, mivel a GDPR és az ePrivacy irányelv ekkor egymást kiegészítve alkalmazandó.[111]

Az Európai Adatvédelmi Testület az ePrivacy irányelv 5. cikke (3) bekezdésének technikai hatályáról szóló iránymutatásában[112] részletes elemzést nyújt a hivatkozott irányelv 5. cikke (3) bekezdésének hatálya alá tartozó technikai műveletek tisztázásával kapcsolatosan. Az iránymutatás foglalkozik a hagyományos eszközök, például a cookie-k alternatívájaként megjelenő új nyomon követési módszerekkel kapcsolatos növekvő aggályokkal, valamint az ePrivacy-irányelv ilyen technológiákra való alkalmazhatóságának tisztázásának szükségességével. Ez a szükségszerűség abból adódott, hogy az irányelv alkalmazása az új nyomkövető eszközökre nem volt egyértelmű, ami a jogi kötelezettségek megkerülésére irányuló módszerek, többek között sötét tervezési minták kifejlesztéséhez vezetett.

Az iránymutatás az ePrivacy irányelv 5. cikk (3) bekezdésének alkalmazhatósága szempontjából négy kulcsfontosságú elemet határoz meg: (i) információ, (ii) az előfizető vagy felhasználó végberendezése, (iii) hozzáférés megszerzése, valamint (iv) tárolt információ és tárolás. Az iránymutatás továbbá ezeket az elemzéseket különböző felhasználási esetekre alkalmazták, beleértve az URL- és pixelkövetést, a helyi feldolgozást, az IP-alapú követést, az időszakos és közvetített IoT-jelentést, valamint az egyedi azonosítók használatát. Ezek az esetek a jelenlegi technológiai környezetben elterjedt technikákat képviselik, és ezáltal gyakorlati betekintést nyújtanak az ePrivacy irányelv 5. cikk (3) bekezdésének alkalmazásába.

Az iránymutatás az ePrivacy irányelvben az „információ” fogalmának tágabb hatályának hangsúlyozásával kezdi, amely magában foglalja mind a nem személyes, mind a személyes adatokat, függetlenül az adatok eredetétől vagy a tárolás okától. Ez a tág értelmezés a felhasználók magánszférájának védelmét célozza, ahogyan azt az ePrivacy irányelv is hangsúlyozza és az Európai Unió Bírósága is megerősítette[113]. A „végberendezés” meghatározása kiterjed a nyilvános hírközlési hálózathoz közvetlenül vagy közvetve

[111] vö. Planet49 GmbH ügyben hozott ítélet, 93. pont
[112] EDPB Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive; https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf, lehívás: 2024.10.25
[113] vö. Planet49 ítélet, 70. sarokpontja

csatlakoztatott eszközökre, kiemelve a felhasználók magánéletének és eszközeik integritásának védelmének fontosságát. Az iránymutatás egyértelművé teszi, hogy az ePrivacy irányelv által biztosított védelem természetes és jogi személyekre egyaránt kiterjed, és a végberendezések típusainak és használati forgatókönyveinek széles körére vonatkozik. Az „elektronikus hírközlő hálózat" fogalmát úgy határozza meg, hogy az magában foglal minden olyan rendszert, amely lehetővé teszi az elektronikus jelek továbbítását, függetlenül attól, hogy a hálózat nyilvános vagy magánjellegű. Ez a tág meghatározás biztosítja az ePrivacy irányelv alkalmazhatóságát a kommunikációs technológiák széles körére. A „hozzáférés megszerzése" olyan műveletként értelmezendő, amely a felhasználó magánéletébe való beavatkozás, és az ePrivacy irányelv attól függetlenül alkalmazandó, hogy a megszerzett információt ugyanaz a fél vagy egy másik fél tárolta. Az iránymutatás hangsúlyozza a hozzájárulás fontosságát és a jogosulatlan hozzáférés elleni védelem szükségességét. A „tárolt információ" és a „tárolás" fogalmát vizsgálják, kiemelve, hogy az ePrivacy irányelv a felhasználó végberendezésén belül bármilyen fizikai vagy elektronikus adathordozón tárolt információra vonatkozik, a tárolt információ időtartamára vagy típusára vonatkozó korlátozások nélkül.

2.3.1.1.8 Hozzájárulás és annak visszavonásával kapcsolatos sötét minták online platformok gyakorlatában

A hozzájárulás alkalmazása számos esetben jelent komoly kihívást és gyakran jelenik meg ún. "sötét tervezési minta" részeként online platformok gyakorlatában, melyet az Európai *Adatvédelmi Testület a 3/2022. sz. iránymutatásában*[114] fedett le részletesen. Ha a hozzájárulás nyelvezete vagy megjelenítése félrevezető, ez azt jelentheti, hogy a GDPR 4. cikk 11. pontja és a GDPR 7. cikke értelmében a hozzájárulás nem önkéntes, és nem jelenti az érintettnek az adatai kezelésére vonatkozó akaratának konkrét, tájékozott és egyértelmű kinyilvánítását. A hozzájárulás kialakításának sötét mintái (félrevezető gombszínek és -méretek; az információk elhomályosítása, a visszautasítási lehetőség eltemetése, hozzájárulás visszavonhatatlansága) szintén azt jelenthetik, hogy az ilyen hozzájárulás érvénytelen, mivel az adatkezelő nem nyújtja a személyes adatok kezelésére vonatkozó információkat (GDPR 39. preambulumbekezdése) tömör, átlátható, érthető és könnyen hozzáférhető formában, világos és közérthető nyelven,

[114] EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them; Version 2.0; Adopted on 14 February 2023; https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_hu

illetve nem biztosítja a hozzájárulás önkéntességének feltételeit. Ezek a minták gyakran megakadályozzák, hogy a felhasználók tudatos, szabad döntéseket hozzanak az adatvédelmi beállításaik kapcsán. Az Európai Adatvédelmi Testület a 3/2022. sz. iránymutatásában bemutatott hozzájárulás alapú sötét minta[115] többek között a *túlterhelés (overloading)*[116], amely során a felhasználókat túl sok választási lehetőség elé állítják. Ez arra ösztönözheti a felhasználókat, hogy a szükségesnél több adatot osszanak meg, vagy akaratlanul is olyan módon kezeljék személyes adataikat, amely ellentétes az elvárásaikkal. Ilyen esetekben előfordulhat, hogy folyamatos nyomásgyakorlás alatt állnak, amikor ismételten szükségtelen adatokat kérnek tőlük, vagy hozzájárulást az adatkezeléshez. Gyakran az is problémát jelent, hogy a felhasználóknak túl sok oldalon kell végignavigálniuk, hogy adatvédelmi beállításokat módosítsanak, ami megnehezíti számukra a döntéshozatalt. Egy másik gyakori tervezési minta a felhasználók figyelmének elterelésére épít, amikor az UX (felhasználói élmény) kialakítása oly módon történik, hogy elfeledteti velük az adatvédelmi szempontokat. Például a reklám célú adatkezelés alapértelmezés szerint előre bekapcsolt funkcióként jelenik meg, vagy olyan vizuális elemeket használnak, amelyek elvonják a figyelmet a fontos adatvédelmi beállításokról. Az *érzelmi felkavarás*[117] olyan módszer, amelyben a felhasználók érzelmi állapotát befolyásolják. Az ilyen technikák gyakran olyan vizuális és nyelvi megoldásokat alkalmaznak, amelyek erősen hatnak az érzelmekre (pl. confirmshaming), így a felhasználók hajlamosak lehetnek olyan döntéseket hozni, amelyek ellentétesek saját adatvédelmi érdekeikkel. Ilyen helyzetekben például félelmet, bűntudatot vagy biztonságérzetet keltenek, ami befolyásolja a döntéshozatalt. Az *akadályozás*[118] is gyakran alkalmazott módszer, amely során megnehezítik a felhasználók számára, hogy hozzáférjenek adatvédelmi beállításaikhoz, vagy hogy tájékozódjanak a lehetőségeikről. Előfordulhat, hogy egy oldal *zsákutcába*[119] torkollik, ahol a felhasználó nem találja meg a keresett információt, vagy indokolatlanul sok lépés szükséges ahhoz, hogy egy adatvédelmi beállítást aktiváljon. A *bizonytalanságban tartás*[120] során a felületet következetlenül és nehezen érthetően alakítják ki, ami miatt a felhasználók nem tudják pontosan, hogyan kezeljék adataikat. Gyakran a *hierarchia hiánya*[121]

[115] EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them; Version 2.0, Content-based patterns; p.17.
[116] EDPB Guidelines 03/2022; Version 2.0; Annex I checklist 4.1.1
[117] EDPB Guidelines 03/2022; Annex I checklist 4.3.1
[118] EDPB Guidelines 03/2022; Annex I checklist 4.4.3
[119] EDPB Guidelines 03/2022; Annex I checklist 4.4.1
[120] EDPB Guidelines 03/2022; Annex I checklist 4.4.2
[121] EDPB Guidelines 03/2022; Annex I checklist 4.5.1

vagy a dekontextualizált információk[122] vezetnek ahhoz, hogy a felhasználók nem tudják megfelelően értelmezni az adatvédelmi lehetőségeket. A *sötétben tartás*[123] arra irányul, hogy az adatvédelmi ellenőrzési eszközöket elrejtsék vagy olyan módon jelenítsék meg, hogy a felhasználók bizonytalanságban maradjanak az adatkezeléssel kapcsolatban. Ilyen esetekben gyakran ellentmondásos vagy kétértelmű információkat[124] közölnek, ami tovább nehezíti a tudatos döntéshozatalt.

A hozzájárulással kapcsolatos sötét minták közül a „süti fal" („consent wall")[125] olyan gyakorlatot jelent, amikor a felhasználóknak egy webhely vagy szolgáltatás eléréséhez el kell fogadniuk a sütiket vagy bizonyos honlap beállításokat. Ez azért tekinthető sötét mintának, mert nem ad valódi választási lehetőséget a felhasználóknak; a hozzájárulás nem „önkéntes", ha ez a hozzáférés előfeltétele. Az Európai Adatvédelmi Testület (EDPB) és több nemzeti adatvédelmi hatóság bírálta ezt a gyakorlatot, azzal érvelve, hogy az sérti a GDPR követelményeit. A Planet49-ügyben az EU Bíróság 2019-ben kimondta, hogy az előre kipipált négyzet nem minősül érvényes hozzájárulásnak a GDPR 4. cikkének 11. pontja és 6. cikke (1) bekezdésének a) pontja alapján. A „consent bundling" vagy „consent tying"[126] pedig olyan gyakorlatokra utal, amikor a személyes adatok kezeléséhez való hozzájárulást más feltételek - például szolgáltatási feltételek - elfogadásához kötik, vagy a szolgáltatás igénybevételének előfeltétele. A Google[127] és az Amazon[128] CNIL ügyei rávilágítottak a sütikre vonatkozó egyértelmű és konkrét, a hozzájárulás egyéb formáitól vagy a szolgáltatási feltételek elfogadásától elkülönített hozzájárulás fontosságára. Amikor a sötét minták révén a felhasználók nyomás alatt vagy manipulált módon adják meg hozzájárulásukat, az nem felel meg az adatvédelmi követelményeknek, így az ilyen hozzájárulás jogellenesnek és érvénytelennek minősül és azok alapján nem lehet jogszerűen személyes adatok kezelését folytatni.

[122] EDPB Guidelines 03/2022; Annex I checklist 4.5.2
[123] EDPB Guidelines 03/2022; Annex I checklist 4.6.2
[124] EDPB Guidelines 03/2022 - Annex I checklist 4.6.3
[125] EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020; 39-41. pontok; p. 12.
[126] EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020; 26. pont; p. 10.
[127] CNIL - Délibération de la formation restreinte n°SAN-2021-023 du 31 décembre 2021 concernant les sociétés X et Y; https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840062; lehívás: 2024.09.12
[128] CNIL - Délibération de la formation restreinte no SAN-2020-013 du 7 décembre 2020 concernant la société X; https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635729; lehívás: 2024.09.12

2.3.1.2 Szerződés teljesítése [GDPR 6. cikk (1) b) pont]

Ha az adatkezelés szükséges egy szerződés teljesítéséhez, amelyben az érintett fél, vagy az adatkezelés az érintett kérésére történő lépések megtételéhez szükséges, akkor ez jogalapot biztosít az adatkezeléshez. Például, egy online platform a felhasználó nevét és címét kezeli, hogy a megrendelt szolgáltatást a részére nyújthassa.

Az Európai Adatvédelmi Testület gyakorlatában[129] a szerződés teljesítését, mint jogalapot *szűken értelmezik* és a Testület értékelése szerint egy szervezet csak akkor hivatkozhat a szerződéses szükségességre, ha bizonyítani tudja, hogy: (i) a szerződés létezik és érvényes a nemzeti jog alapján; és (ii) az adatkezelés objektíve szükséges a szerződés teljesítéséhez. Az Európai Adatvédelmi Testület úgy ítélte meg, hogy a felügyeleti hatóságoknak korlátozott hatáskörük van a szerződés érvényességének értékelésére a GDPR céljainak teljesítése érdekében. Az objektív szükségességet a szolgáltatás konkrét célja alapján kell megítélni, és az adatkezelőnek igazolnia kell, hogy az adatkezelés valóban szükséges a szerződéses cél teljesítéséhez. Az Európai Adatvédelmi Testület szigorú értelmezést javasolt a „szükségesség" fogalmára vonatkozóan, hogy megakadályozza az adatkezelőket a hozzájárulás követelményének megkerülésében. Ennek megfelelően ez a jogalap nem alkalmazható, ha egy érintett személyes adatait marketing célokra, csalás megelőzésére, célzott hirdetésekre vagy az online platform üzleti modelljéhez kapcsolódó egyéb célokra kívánja kezelni.

Az Európai Bíróság a *Meta Platforms Inc. és társai kontra Bundeskartellamt ügyben* szintén egyértelművé tette, hogy az adatkezelési tevékenységek szerződésbe foglalása önmagában nem jelenti automatikusan azt, hogy az ilyen adatkezelés szükséges lenne a szerződés teljesítéséhez a GDPR 6. cikk (1) bekezdés b) pontja alapján. Ahhoz, hogy a személyesadat-kezelést a szerződés teljesítéséhez szükségesnek lehessen tekinteni, annak *objektíve elengedhetetlennek* kell lennie az érintettnek nyújtott szerződéses szolgáltatás szerves részét képező cél megvalósításához. Az adatkezelőnek tehát képesnek kell lennie annak bizonyítására, hogy a szerződés fő célja tárgya miért nem lenne elérhető a szóban forgó adatkezelés nélkül. Az a tény, hogy az ilyen adatkezelést a szerződés említi, vagy az csupán hasznos a szerződés

[129] EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf ; lehívás: 2024.08.20

teljesítéséhez, e tekintetben önmagában nem releváns. Az igazolás alkalmazása szempontjából ugyanis az a meghatározó tényező, hogy az adatkezelő általi személyesadat-kezelés *alapvető fontosságú* legyen az adatkezelő és az érintett között létrejött szerződés megfelelő teljesítéséhez, és hogy ennélfogva ne álljanak rendelkezésre más, a gyakorlatban megvalósítható és kevésbé beavatkozó jellegű megoldások.[130] A Bíróság tehát azt hangsúlyozta, hogy az adatkezelésnek *közvetlenül* és *objektíven* kapcsolódnia kell a szerződés lényegi kötelezettségeihez, és elengedhetetlennek kell lennie ahhoz, hogy a felhasználó által igénybe vett szolgáltatást teljesíteni lehessen. A Bíróság kiemelte, hogy a tartalmak személyre szabása a Facebook platformon nem tűnik szükségesnek ahhoz, hogy e felhasználó számára online közösségi hálózati szolgáltatásokat kínáljanak. E szolgáltatásokat adott esetben olyan egyenértékű alternatíva formájában is lehet nyújtani a számára, amely nem jár ilyen személyre szabással, ezért ez utóbbi *nem objektíve elengedhetetlen* az ugyanezen szolgáltatások szerves részét képező cél eléréséhez.[131] Ha az adatkezelés más célokat szolgál, például személyre szabott reklámozást vagy a felhasználói viselkedés nyomon követését különböző platformokon és szolgáltatásokon, az nem igazolható szerződéses jogalapon, és más jogalapra, például a felhasználó kifejezett hozzájárulására lehet szükség ehhez. Ez az értelmezés korlátozza az online platformok, mint például a Meta és más online platformok lehetőségét arra, hogy a szerződés teljesítésére hivatkozva általánosan igazolják az adatkezelési gyakorlatokat, anélkül, hogy alaposan vizsgálnák és igazolnák azok szükségességét.

2.3.1.3 Kötelező adatkezelések [GDPR 6. cikk (1) c) és e) pont]

Az adatkezelés jogszerű akkor is, ha szükséges az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez. A jogi kötelezettség azt jelenti a GDPR hatálya alatt, hogy az adatkezelés kötelező és nincs eltérési lehetőség a személyes adatok kezelése tekintetében. Ha az adatkezelés közérdekű feladat végrehajtásához vagy közhatalmi jogosítvány gyakorlásához szükséges, amelyet az adatkezelőre ruháztak, akkor ez is jogalapot biztosít. Lényeges, hogy ezek a jogalap nem használható kereskedelmi vagy tisztán üzleti célokra.

[130] vö. Európai Unió Bírósága – C-252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság (ECLI:EU:C:2023:537); 98-99. sarokpontok
[131] vö. Európai Unió Bírósága – C-252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság (ECLI:EU:C:2023:537); 102-104. sarokpontok

Az online platformoknak az Európai Unióban számos jogi kötelezettséget kell teljesíteniük a személyes adatok kezelése terén. Ide tartoznak az adójogi és számviteli előírások, amelyek alapján a platformoknak biztosítaniuk kell a pénzügyi tranzakciók nyilvántartását és a szükséges adózási kötelezettségek teljesítését vagy hatósági megkeresések, kötelező határozatok megválaszolását. Magyarországon az Elkertv. rögzíti az online terrorista tartalom terjesztésével szembeni eljárás szabályait (vö. 12/B. §); a jogsértő információs társadalommal összefüggő szolgáltatással kapcsolatos értesítések kezelését és a kiskorúak védelmére vonatkozó szabályokat (vö. 13. §). A platformoknak továbbá meg kell felelniük a hálózat- és információbiztonságra vonatkozó előírásoknak, biztosítva az adatbiztonságot és a kibervédelmet, illetve az incidensek bejelentését[132]. Ezek a kötelezettségek mind a nemzeti, mind az uniós jogszabályok szigorú betartását igénylik, hogy az online platformok megfeleljenek az irányadó jogi előírásoknak.

Az online platformok számára 6. cikk (1) bekezdés e) pont szerinti jogalap pedig általában csak akkor releváns, ha a platform közszolgáltatásokkal kapcsolatos tevékenységet végez, vagy közérdekből végzett feladat végrehajtásával vagy közhatalmi jogosítvány gyakorlásával bízták-e meg, különösen közérdekű kutatás, valamint a biztonság, integritás és védelem elősegítése érdekében. Az online platformok tevékenységének típusára és alapvetően gazdasági és kereskedelmi jellegére tekintettel atipikus, hogy e magán gazdasági szereplőt ilyen feladattal bíznak meg.[133]

Az Európai Bíróság a Meta Platforms Inc. és társai kontra Bundeskartellamt ügyben fontos iránymutatást adott arra vonatkozóan, hogy egy online platform milyen körülmények között hivatkozhat a GDPR 6. cikk (1) bekezdésének c) pontjára, amely a jogi kötelezettség alapján történő adatkezelésről szól. A konkrét kérdés az volt, hogy a Meta Platforms Irelandet terheli-e jogi kötelezettség a felhasználói személyes adatok megelőző jellegű gyűjtésére és megőrzésére annak érdekében, hogy a nemzeti hatóságok későbbi megkeresései esetén ezekhez az adatokhoz hozzáférést biztosíthasson. Az ügyben hozott ítéletében a Bíróság hangsúlyozta[134], hogy a GDPR 6. cikk (1) bekezdésének c) pontja szerint a személyes adatok kezelése akkor jogszerű,

[132] vö. 270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről
[133] vö. Európai Unió Bírósága, C 252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság (ECLI:EU:C:2023:537); 133. sarokpont
[134] vö. Európai Unió Bírósága, C 252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság (ECLI:EU:C:2023:537); 138. sarokpont

ha az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges. Az adatkezelésnek egyértelmű jogi kötelezettségen kell alapulnia, amely lehet uniós jogból vagy az érintett tagállam nemzeti jogából eredő kötelezettség. Ez a jogalap csak akkor alkalmazható, ha az adatkezelés közérdekű célt szolgál, arányos az elérni kívánt jogszerű céllal, és az adatkezelés a feltétlenül szükséges mértékre korlátozódik. A konkrét ügy kapcsán a Bíróság megvizsgálta, hogy a Meta Ireland jogosult-e a felhasználói személyes adatok megelőző jellegű gyűjtésére, beleértve azokat az adatokat is, amelyek más szolgáltatásokból vagy harmadik fél weboldalainak és alkalmazásainak használatából származnak. A Bíróság kimondta, hogy az ilyen adatkezelés csak akkor igazolható a jogi kötelezettség jogalapjával, ha az adatkezelőre vonatkozó konkrét jogszabályi előírás alapján történik, és ha az adatkezelés arányos és a szükséges határokon belül marad. Ez az ítélet kiemelkedő jelentőségű, mivel segít tisztázni, hogy az online platformok, mint például a Meta, milyen feltételek mellett hivatkozhatnak a jogi kötelezettségre, mint adatkezelési jogalapra. Emellett az adatkezelés arányosságának és szükségességének követelménye is kulcsfontosságú, ami azt jelenti, hogy a platformoknak csak akkor van joguk ilyen adatgyűjtést végezni, ha az kifejezetten szükséges egy konkrét jogi kötelezettség teljesítéséhez, és nem léphetik túl a szükséges mértéket.

2.3.1.4 Érintett létfontosságú érdekeinek védelme [GDPR 6. cikk (1) d) pont]

Az adatkezelés jogszerű lehet, ha az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme érdekében szükséges. Online platformok esetében ez a jogalap csak *kivételes* körülmények között alkalmazható, amikor az adatkezelés célja az érintett életének vagy testi épségének védelme. Ilyen eset lehet például, ha egy online platform olyan szolgáltatást nyújt, amely közvetlenül kapcsolódik a felhasználók egészségéhez vagy biztonságához, és ahol az érintett hozzájárulásának megszerzése nem lehetséges időben, például sürgősségi helyzetekben. Ez a jogalap nem használható általános adatkezelési célokra, mint például marketing, felhasználói élmény javítása vagy üzleti tevékenységek optimalizálása, hanem kizárólag az érintett életének vagy testi épségének megóvására irányuló, feltétlenül szükséges adatkezelés esetén alkalmazható.

Az Európai Bíróság megállapítása a Meta Platforms Inc. és társai kontra Bundeskartellamt ügyben nagy jelentőséggel bír, mivel pontosítja, hogy milyen körülmények között lehet a GDPR 6. cikk (1) bekezdésének d) pontjára hivatkozni, amely jogalap a személyes adatok

kezelését akkor teszi lehetővé, ha az érintett személy vagy egy másik természetes személy életének védelme érdekében szükséges. A Bíróság itt egyértelműen kimondta[135], hogy az ilyen jogalap csak különleges helyzetekben alkalmazható, ahol az adatkezelés ténylegesen az érintett vagy más személy életét fenyegető veszély elhárításához kapcsolódik. Az ügy egyik fő kérdése az volt, hogy a Meta Platforms Ireland hivatkozhat-e erre a jogalapra a felhasználói személyes adatok kezelése során. A Bíróság megállapította, hogy a GDPR 6. cikk (1) bekezdésének d) pontja megszorítóan értelmezendő, és olyan különleges helyzetekre vonatkozik, mint a járványok vagy humanitárius vészhelyzetek, például természeti katasztrófák. Az ilyen adatkezelés csak akkor indokolt, ha az élet védelme érdekében feltétlenül szükséges. A Bíróság ezzel összefüggésben kifejtette, hogy az online platformok – különösen azok, amelyek gazdasági és kereskedelmi tevékenységet folytatnak, mint például a Meta – nem hivatkozhatnak erre a jogalapra általánosan és megelőző jelleggel a felhasználói adatok kezelésének igazolására. Ez a megállapítás azért jelentős, mert megerősíti, hogy az adatkezelők nem hivatkozhatnak önkényesen az életvédelemhez kapcsolódó jogalapra, ha az adatkezelés célja valójában gazdasági vagy kereskedelmi természetű. Az ilyen jogalap csak valós, közvetlen életveszély elhárításához szükséges adatkezelés esetében alkalmazható, és nem használható fel például általános adatgyűjtésre vagy üzleti célok igazolására. Ez a döntés jelentősen szűkíti a jogalap alkalmazási körét, és fontos védelmet biztosít az érintettek személyes adatai felett.

2.3.1.5 Az adatkezelő vagy egy harmadik fél jogos érdeke [6. cikk (1) f) pont]

A jogos érdek, mint a személyes adatok kezelésének jogalapja a GDPR 6. cikk (1) bekezdésének f) pontjában található és kiemelt szerepet játszik az uniós adatvédelmi jog rendszerében és a közvetítő szolgáltatók adatkezelésében is. Ez az adatkezelési jogalap akkor alkalmazható, ha az adatkezelés szükséges az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez, kivéve, ha az érintett személy alapvető jogai és szabadságai elsőbbséget élveznek az ilyen érdekkel szemben, különösen, ha az érintett gyermek.

2.3.1.5.1 A jogos érdekkel szemben támasztott követelmények

[135] Európai Unió Bírósága, C 252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság (ECLI:EU:C:2023:537); 136-137. pontok

A jogos érdek fogalmát a GDPR nem határozza meg kifejezetten, és nincs egy meghatározott, zárt lista sem, amely felsorolná, hogy milyen esetekben alkalmazható ez a jogalap. AZ EU Bíróság gyakorlata szerint az érdekek széles köre jogszerűnek tekinthető[136], az uniós jogalkotó nem követelte meg, hogy az adatkezelő által érvényesíteni kívánt érdeket jogszabály írja elő, azaz a „jogos érdek" fogalma nem korlátozódik a jogszabály által elismert és meghatározott érdekekre, azonban a GDPR megköveteli, hogy az állítólagos jogos érdek jogszerű legyen.[137]

A 29. cikk szerinti Adatvédelmi Munkacsoport a 6/2014. sz. véleményében[138] hangsúlyozza, hogy a jogos érdek egy előny, amely közvetlen kapcsolatban áll az adatkezeléssel, és akár az adatkezelő, akár egy harmadik fél, csoport vagy egyén javára szolgálhat. Fontos, hogy ez az érdek valós legyen, és ne pusztán spekuláción alapuljon. A jogos érdek továbbá jogszerű kell, hogy legyen, és összhangban kell állnia a vonatkozó jogszabályokkal.

A jogos érdekek spektrumként kezelendők, mivel ezek a jelentéktelen érdekektől egészen a kényszerítő erejű jogos érdekekig terjedhetnek. Például a GDPR 47. preambulumbekezdése szerint a csalások megelőzése, illetve a direkt marketing jogos érdeknek minősülhet[139]. A 48. preambulumbekezdés értelmében vállalkozáscsoporton belül az ügyfél- és munkavállalói adatok adminisztratív célú továbbítása is jogos érdeket képezhet, míg a 49. preambulumbekezdésben az informatikai biztonság fenntartása és az incidenskezelés szerepel jogos érdek példájaként.

A jogos érdek, mint jogalap alkalmazása három együttes feltételt ír elő a személyes adatok kezelésének jogszerűségéhez: így az adatkezelő vagy harmadik személy jogos érdekének érvényesítése szükséges, másodszor a személyes adatok kezelése valamely jogos érdek érvényesítéséhez szükséges, és harmadszor, hogy az adatvédelemmel érintett személy érdekei

---

[136] vö. EU Bíróság; 2023. december 7-i SCHUFA Holding [Tartozáselengedés] ítélet, C-26/22 és C-64/22, EU:C:2023:958, 76. pont

[137] vö. Koninklijke Nederlandse Lawn Tennisbond és az Autoriteit Persoonsgegevens C-621/22. sz. ügyben 2024. október 4. napján meghozott ítélet; ECLI:EU:C:2024:857; 38-40. pontok

[138] 29. cikk szerinti adatvédelmi munkacsoport 06/2014. számú véleménye az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról; WP 217; elfogadás időpontja: 2014. április 9.; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf; lehívás: 2024.09.13.

[139] Az EU Bíróság nem zárta ki, hogy az adatkezelőnek a hirdetések értékesítésének marketing célú előmozdításában és értékesítésében megnyilvánuló kereskedelmi érdekét a GDPR 6. cikke (1) bekezdése első albekezdésének f) pontja értelmében vett jogos érdeknek lehessen tekinteni, lásd analógia útján: 2014. május 13-i Google Spain és Google ítélet, C-131/12, EU:C:2014:317, 73. pont.

vagy alapvető jogai és szabadságai nem magasabb rendűek az adatkezelő vagy a harmadik fél jogos érdekénél.[140] Az adatkezelés jogos érdek jogalapján történő végrehajtása során tehát elengedhetetlen a gondos érdekmérlegelés[141], melyet több lépésben kell elvégezni. Először is, az adatkezelőnek azonosítania kell, hogy milyen konkrét jogos érdek alapján kíván adatokat kezelni. Ezt követően fel kell mérni, hogy az érintett személy érdekei, jogai és szabadságai milyen mértékben érintettek az adatkezelés által. Végül a két szempontot össze kell vetni, és meg kell határozni, hogy az adatkezelés arányos-e az érintett jogainak korlátozásával. Ezen elemzés része lehet az adatvédelmi hatásvizsgálat elvégzése is, amennyiben magas kockázatot azonosítanak az érintett jogaira és szabadságaira nézve. A 29. cikk szerinti Adatvédelmi Munkacsoport a 6/2014. sz. véleményének 1. számú melléklete részletes útmutatást adott az érdemérlegelési teszt elvégzésének módszertanához. A GDPR 5. cikk (2) bekezdése és a 24. cikk (1) bekezdése alapján az adatkezelő felelőssége, hogy megfelelően dokumentálja az érdekmérlegelési teszt elvégzését, valamint, hogy igazolja az adatkezelés jogszerűségét.

A GDPR különös hangsúlyt fektet az adatkezelő által igénybe vett jogos érdekekkel kapcsolatos tájékoztatásra és a GDPR 21. cikke szerinti tiltakozáshoz való jog érvényesítésére. Az érintettet a GDPR 13 és 14. cikke szerint tájékoztatni kell arról, hogy milyen jogos érdekek alapján történik az adatkezelés, és az adatkezelőnek fel kell hívnia a figyelmet arra, hogy az érintett jogosult tiltakozni az adatkezelés ellen. A tiltakozáshoz való jogról szóló tájékoztatást egyértelműen és más információktól elkülönítve kell megjeleníteni (vö. GDPR 21. cikk (4) bekezdés). Ha az érintett tiltakozik, az adatkezelést az adatkezelő csak akkor folytathatja, ha olyan kényszerítő erejű jogos indokokat tud felmutatni, amelyek felülírják az érintett érdekeit, jogait és szabadságait, vagy ha az adatkezelés jogi igények érvényesítéséhez szükséges (vö, GDPR 21. cikk (1) bekezdés). A GDPR 47. preambulumbekezdése alapján a tájékoztatásnak oly módon kell történnie, hogy az érintett elvárásait figyelembe vegye, és elkerülje az információ-túlterhelést. A 29. cikk szerinti munkacsoport transzparencia iránymutatása[142] („*Transzparencia Iránymutatás*") szerint az érintetteknek lehetőséget kell biztosítani arra, hogy további információt kérjenek az érdekmérlegelési tesztről, ha erre szükségük van.

[140] 2023. július 4-i Meta Platforms és társai [Közösségi hálózat általános felhasználási feltételei] ítélet, C-252/21, EU:C:2023:537, 106. pont; EU Bíróság a Koninklijke Nederlandse Lawn Tennisbond és az Autoriteit Persoonsgegevens C-621/22. sz. ügyben 2024. október 4.-i ítélet; ECLI:EU:C:2024:857; 37. pontja
[141] vö. 29. cikk szerinti adatvédelmi munkacsoport 06/2014. számú vélemény; 58-59. oldalak;
[142] A 29. cikk szerinti adatvédelmi munkacsoport Iránymutatás az (EU) 2016/679 rendelet szerinti átláthatóságról (wp260rev.01); elfogadás időpontja: 2017. november 29. A legutóbbi felülvizsgálat és elfogadás időpontja: 2018. április 11.; https://ec.europa.eu/newsroom/article29/items/622227/en; lehívás: 2024.09.15

Megjegyzendő továbbá, hogy a gyermekek személyes adatai különleges védelmet igényelnek, mivel kevésbé vannak tisztában a személyes adatok kezelésével járó kockázatokkal és következményekkel. Ez a védelem különösen fontos közvetlen üzletszerzési célú felhasználás, profilalkotás, illetve a gyermekeknek nyújtott szolgáltatások igénybevétele során. Ez azt jelenti, hogy az alkalmazandó adatvédelmi jogszabályok és joggyakorlat szerint e célból korlátozottan lehet jogos érdekre, mint adatkezelési jogalapra hivatkozni, ha gyermekek az érintettek.

Az EU Bíróság a Koninklijke Nederlandse Lawn Tennisbond és az Autoriteit Persoonsgegevens C-621/22. sz. ügyben 2024. október 4. napján meghozott ítéletében[143] részletesen foglalkozott a jogos érdek mint jogalap alkalmazhatóságával olyan esetben, mikor egy teniszegyesület szponzorációs szerződés alapján, tehát ellenérték fejében szerencsejáték- és kaszinójáték-szolgáltatónak továbbította az egyesületi tagok nevét, címét és lakcímét egy promóciókat tartalmazó szórólap postai küldeményként történő megküldése céljából. Ez az ügy az online platformok adatmonetizációs, vagy mesterséges intelligencia alkalmazások ügyféladatokkal kapcsolatos tréningelésével kapcsolatos stratégiájának[144] jogi megítélésével kapcsolatosan is alkalmazható, releváns megállapításokat rögzít. A Bíróság az üggyel kapcsolatosan megerősítette, hogy akár egy *kereskedelmi érdek is jogos érdeknek minősülhet*[145], azonban a Bíróság szigorú érdekmérlegelés hatálya alá rendelte e jogalap alkalmazhatóságát. A Bíróság szerint e jogalap alkalmazása megköveteli azt, hogy az adatkezelő tiszteletben tartsa a GDPR szabályozásából eredő valamennyi egyéb kötelezettségét[146], tehát azt, hogy az személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. Vizsgálni kell az adatkezelésnek az említett érdek érvényesítéséhez való *szükségességét*, különösen az érintettek alapvető jogait és szabadságait kevésbé veszélyeztető, ugyanolyan megfelelő eszközök fennállását, hogy van-e olyan adatkezelési alternatíva, ami kevésbé korlátozza az érintettek jogait, így az érintettek adatok ellenőrzése feletti jogát és az adatminimalizálás elvének megfelelően az adatok közlését ténylegesen arra korlátozza, ami ténylegesen szükséges és releváns azon célok szempontjából, amelyek érdekében az említett

[143] EU Bíróság a Koninklijke Nederlandse Lawn Tennisbond és az Autoriteit Persoonsgegevens C-621/22. sz. ügyben 2024. október 4.-i ítélet; ECLI:EU:C:2024:857
[144] Ádám Liber – Tamás Bereczki - The state of web scraping in the EU – IAPP; https://iapp.org/news/a/the-state-of-web-scraping-in-the-eu; lehívás: 2024.10.26.
[145] EU Bíróság a Koninklijke Nederlandse Lawn Tennisbond és az Autoriteit Persoonsgegevens C-621/22. sz. ügyben 2024. október 4.-i ítélet; ECLI:EU:C:2024:857; 48. pontja
[146]

adatokat továbbítják és kezelik. A Koninklijke Nederlandse Lawn Tennisbond ügyben a Bíróság kiemelte, hogy a személyes adatok visszterhes, reklámcélú értékesítésével kapcsolatosan, amennyiben ez jogos érdeken alapul, az érdekmérlegelés szempontjából relevánsnak minősül és figyelembe kell venni, hogy az érintettek racionálisan számolhattak-e az adattovábbítással a teniszegyesületbe való belépésükkor, mely szempontból az érintettek és az adatkezelő közötti releváns és megfelelő kapcsolatot is figyelembe kell venni, továbbá mérlegelni kell azokat a kockázatokat, hogy az ilyen adatok kezelése káros hatással lehet a teniszegyesületek érintett tagjaira, mivel az említett tevékenységek e tagokat a játékfüggőség kialakulásához kapcsolódó kockázatoknak tehetik ki[147]. A Bíróság az előzetes döntéshozatali kérdést előterjesztő holland nemzeti bíróság mérlegelésére bízta ezen feltételek elbírálását.

2.3.1.5.2 Jogos érdek az ePrivacy irányelv hatálya alatt

Az ePrivacy irányelv rendelkezései szintén jelentősen befolyásolják azt, hogy egy online platform mikor és hogyan támaszkodhat a jogos érdek, mint jogalapra, különösen az információs társadalommal kapcsolatos szolgáltatásokat érintő adatkezelések (például sütik használata, nyomkövető technológiák alkalmazása) esetében. Az ePrivacy irányelv és a GDPR ugyanis együttesen szabályozzák a személyes adatok kezelését az online környezetben, de az ePrivacy irányelv specifikusabb szabályokat állapít meg az elektronikus kommunikációhoz kapcsolódó adatvédelem területén. Az ePrivacy irányelvre figyelemmel információs társadalommal kapcsolatos szolgáltatások nyújtásával kapcsolatosan a jogos érdek csak akkor alkalmazható adatkezelési jogalapként, ha az adattárolás vagy hozzáférés célja az elektronikus hírközlő hálózaton keresztül történő közléstovábbítás, vagy a felhasználó által kifejezetten kért, az információs társadalommal összefüggő szolgáltatás nyújtásához szükséges (vö. ePrivacy irányelv 5. cikk (3) bekezdése). Az ePrivacy irányelv ugyanis különös hangsúlyt fektet a felhasználói hozzájárulásra, különösen az elektronikus kommunikációs hálózatokon keresztüli adatkezelések tekintetében. Ez azt jelenti, hogy ha egy információs társadalommal kapcsolatos szolgáltatás adatkezelési tevékenysége nem tartozik a közléstovábbítás végrehajtásához szükséges kategóriába, vagy nem része a felhasználó által kifejezetten kért szolgáltatásnak, melyet az Európai Adatvédelmi Testület gyakorlata szerint szűken kell értelmezni, akkor az

[147] EU Bíróság a Koninklijke Nederlandse Lawn Tennisbond és az Autoriteit Persoonsgegevens C-621/22. sz. ügyben 2024. október 4.-i ítélet; ECLI:EU:C:2024:857; 56-57. pontok

adatkezelő nem támaszkodhat a jogos érdek jogalapjára az adatkezeléshez, hanem köteles megszerezni a felhasználó hozzájárulását.[148]

Az ePrivacy irányelv rendelkezései akkor is relevánsak, mikor a szolgáltató az érintettek személyes adatait felhasználhatja direkt marketing célokra jogos érdek alapján. Ennek jogszerűségi feltétele, hogy az érintettek számára biztosítsák a tiltakozás jogát, és hogy a marketing tevékenység ne invazív módon történjen. A jogos érdek teszt keretében mérlegelni szükséges ilyenkor: a kommunikáció tárgyát (gazdasági reklám vagy társadalmi céllal kapcsolatos üzenet, amelyet a véleménynyilvánítás szabadsága is erősebben véd); a kommunikáció címzettjeit (üzletfél címzett, mint üzleti kapcsolattartó, B2B üzenetek vagy fogyasztó, magánfél címzett, akiknek a magánszféráját erősebben szükséges védeni); a küldő és a címzett fél közötti jogviszonyt, fennálló üzleti vagy ügyleti kapcsolatot és az ügyleti kapcsolat létesítésének időpontját; a kommunikáció magánélettel kapcsolatos hatását, esetleges zavarását (elektronikus vagy postai üzenet, ezek gyakorisága, az üzenetküldés automatizáltsága pl. hívórendszer útján); a leiratkozás, illetve a tiltakozás lehetőségét, illetve annak hatékonyságát.

Az ePrivacy irányelv 13. cikk (1) bekezdése értelmében ez a jogos érdek nem vonatkozik az emberi beavatkozás nélküli automatizált hívó- és távközlési rendszerek (automatikus hívóberendezések), telefax- (fax-) berendezések, illetve elektronikus levelek alkalmazására, mivel ilyen eszközök közvetlen üzletszerzési célból történő használata kizárólag hozzájárulással lehetséges. Az ePrivacy irányelv 13. cikk (2) bekezdése értelmében ez alól egyetlen kivétel van, még pedig az ún. „soft opt-in” szabályozás, melynek alapján jogos érdek alapján küldhetők elektronikus direkt marketing üzenetek. A "soft opt-in" arra vonatkozik, mikor egy vállalkozás elektronikus levelezés során megszerzi ügyfelei elektronikus elérhetőségi adatait egy termék vagy szolgáltatás értékesítése során, mely esetben ezeket az elektronikus elérhetőségi adatokat a vállalkozás saját hasonló termékeivel vagy szolgáltatásaival kapcsolatos közvetlen üzletszerzési célra felhasználhatja, azaz nem szükséges külön hozzájárulást kérni az ilyen kommunikációkhoz, hanem az adatok felvételekor tiltakozási jogot (opt-out) szükséges biztosítani az ügyfél részére. Problémás azonban, hogy a magyar jogalkotó nem ültette át a magyar jogba az ePrivacy irányelv 13. cikk (2) bekezdését, azaz az

[148] EDPB - Report of the work undertaken by the Cookie Banner Taskforce; Adopted on 17 January 2023; 24. sarokpont

elektronikus direkt marketing esetében a magyar jog egyáltalán nem biztosít lehetőséget az ún. "soft opt-in" kommunikációkra[149] és ezzel kapcsolatosan a magyar adatvédelmi hatóság gyakorlata is sem egyértelmű, különösen elégedettség felméréssel kapcsolatos kommunikációk esetében[150].

Itt rögzítendő, hogy az Európai Adatvédelmi Testület 2024. október 9. napjával 1/2024. szám alatt kiadta a GDPR 6. cikk (1) bekezdés (f) pontjával kapcsolatos iránymutatását, amely 2024. november 20. napjáig társadalmi konzultáció alatt áll[151] és felülvizsgálja a 29. cikk szerinti adatvédelmi munkacsoport 06/2014. számú véleményét. Ez az iránymutatás számos fontos megállapítást rögzít a jogos érdek mint jogalap alkalmazásával kapcsolatosan a digitális szolgáltatások területén és megállapítja, hogy jogos érdek alkalmazása ezen a területen adott esetben kizárt lehet, mert az adatkezelőknek minden esetben figyelembe kell venniük az európai és nemzeti jogszabályokat, amelyek előírhatják a hozzájárulás szükségességét bizonyos műveletekhez a közvetlen üzletszerzés kontextusában, vagy megtilthatják bizonyos típusú közvetlen üzletszerzési tevékenységeket, melynél fogva ezekere a jogos érdek, mint jogalap nem alkalmazható a digitális szolgáltatások kontextusában.[152] Az ePrivacy irányelv értelmében a kéretlen üzenetek küldése közvetlen üzletszerzési célból – ideértve az e-mailt, SMS-t, MMS-t és hasonló alkalmazásokat – ugyanis az ePrivacy szabályok értelmében csak az érintett

[149] A „soft opt-in" lehetőségét eredetileg 2007. évi XCIV. törvény 10. §.-val magyar jogba bevezetett, majd a 2008. évi XLVII. törvény 41. §-val hatályon kívül helyezte. A gyakorlatban bizonytalanság tapasztalható, hogy a magyar reklámozási szabályok mennyiben alkalmazhatóak a GDPR rendelkezései fényében. A GDPR (47) preambulumbekezdése szerint ugyanis a személyes adatok közvetlen üzletszerzési célú kezelése is jogos érdeken alapulónak tekinthető. Ezzel szemben azonban a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló 2008. évi XLVIII. törvény („reklámtörvény") 6. § (1)-(9) bekezdései, továbbá a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény („direkt marketing törvény") szabályai jelenleg nem teszik lehetővé, illetve nem biztosítanak lehetőséget személyes adatok jogos érdek alapján történő kezelésére közvetlen üzletszerzési célból.

[150] vö. NAIH-6737-1/2024 (NAIH-2900/2023, NAIH-636/2022, NAIH-9230/2021 - A NAIH ebben az ügyben egy csomagküldő cég adatkezelési gyakorlatát vizsgálta, ahol a cég ügyfélelégedettségi felhívást helyezett el a kézbesítési státuszüzenetben, és jogszerűnek találta azt. Az adatkezelést a szerződés teljesítéséhez kapcsolódó céllal végezték, ezért nem volt szükség külön jogalapra. A hatóság megállapította, hogy az érintett neve és e-mail címe jogszerűen került felhasználásra, és az adatkezelés nem sértette az érintettek magánszféráját, mivel az értesítést figyelmen kívül lehetett hagyni. Az érintett tiltakozási jogát sem biztosították. Az ügy vitathatósága abban rejlik, hogy a német szövetségi legfelsőbb bíróság (VI ZR 225/17) egy hasonló esetben az Amazon gyakorlatát reklámnak minősítette, és az ePrivacy Irányelv soft-opt-in szabályait alkalmazta. Ha a NAIH is reklámnak tekintette volna az ügyfélelégedettségi felhívást, a döntés más lehetett volna, és az érintettek számára tiltakozási jogot kellett volna biztosítani.

[151] Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, under public consultation; https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en; lehívás: 2024.10.25.

[152] Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, under public consultation; 113. sarokpont

személy előzetes hozzájárulásával történhet.[153] Ezen hozzájárulásnak meg kell felelnie a GDPR 4. cikk 11. pontjában foglalt követelményeknek, ezért a közvetlen üzletszerzési célú adatkezelés ebben az esetben *nem alapulhat jogos érdeken*, azaz a GDPR 6. cikk (1) bekezdés f) pontján, figyelemmel arra, hogy az ePrivacy irányelv ebben az esetben szűkíti ezen jogalap alkalmazásának lehetőségeit. A hozzájárulás, mint jogalap ePrivacy irányelv 5. cikk (3) bekezdése szerinti alkalmazása ugyanis korlátozza a jogos érdek mint jogalap alkalmazhatóságát, mivel a „soft opt-in" ePrivacy irányelv 13. cikk (2) bekezdése szerinti lehetőségére szűkíti azt[154], ami azt jelenti, hogy csak akkor küldhető jogos érdek alapján direkt marketing kommunikáció, ha az ePrivacy irányelv „soft opt-in" feltételei teljesülnek ezzel kapcsolatosan. Figyelembe kell azonban venni, hogy a GDPR és az ePrivacy irányelv közötti kölcsönhatás csak akkor merül fel, amikor a személyes adatok kezelése egyidejűleg mindkét jogszabály anyagi hatálya alá tartozik. Ezért az elektronikus hírközlési eszközökkel történő, de személyes adatkezelést nem igénylő közvetlen üzletszerzés (pl. jogi személyeknek címzett közvetlen üzletszerzés) csak az ePrivacy irányelv hatálya alá tartozik és arra nem alkalmazandó a GDPR. Amikor azonban személyes adatok kezelése a kérdés, az ePrivacy irányelvet „lex specialis"-nak kell tekinteni, amennyiben az ilyen adatkezelést szabályozza. Ezzel szemben a közvetlen üzletszerzés céljából, nem elektronikus hírközlési eszközökkel folytatott kommunikációk (például postai levél) nem tartoznak az ePrivacy irányelv anyagi hatálya alá, és így az irányelv szerint nem követelik meg a hozzájárulást[155], mely esetben a jogos érdek alkalmazható jogalapnak minősülhet. Ebben a kőrben tehát a ePrivacy irányelvet átültető nemzeti szabályok, Magyarországon az Elkertv. alkalmazási körét kell értékelni, ami a hozzájárulásra vonatkozó követelményeket az irányelvben foglaltakon túl is kiterjeszthetik, mint ahogyan azt Magyarországon az Elkertv. 13/A §. (4) és (6) bekezdése teszi ezt.

2.3.1.5.3 Jogos érdekek online platformok adatkezelésénél

Egy online platform számos esetben támaszkodhat a jogos érdekre, mint jogalapra. Ilyen eset lehet a csalások megelőzése, az informatikai rendszerek biztonságának fenntartása és a

[153] Lásd az ePrivacy irányelv 13. cikk (1) bekezdését, valamint a (40) és (67) preambulumbekezdéseket.
[154] Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, under public consultation; vö. 114-116. sarokpontok
[155] Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, under public consultation; vö. 117. sarokpont

jogellenes tevékenységek felderítése, mivel az ilyen adatkezelés során az adatkezelő jogos érdeke a csalás elleni védelem és a platform biztonságának biztosítása.

A 29. cikk szerinti adatvédelmi munkacsoport keresőprogramokkal kapcsolatos adatvédelmi kérdésekről szóló 1/2008. véleménye szintén utalt a jogos érdek, mint jogalap alkalmazására. E vélemény szerint a keresőprogramok számos cél érdekében kezelnek személyes adatokat, így különösen a szolgáltatás javítása, a rendszer biztonságának fenntartása, csalások megelőzése, számviteli előírások betartása, személyre szabott hirdetések nyújtása, statisztikai adatokat gyűjtése, továbbá akár bűnüldözési cél érdekében is. A hozzájárulás nem megfelelő jogalap a keresőprogramokkal kapcsolatos adatkezeléshez, mikor szolgáltatást névtelenül igénybe vevő felhasználók érintettek, továbbá a szerződéses adatkezelési jogalap sem irányadó, amennyiben nem regisztrált felhasználók a szolgáltatás felhasználói. A munkacsoport álláspontja szerint a szolgáltatás javítása, személyre szabott hirdetések nyújtása céljából nem tekinthető indokoltnak nem anonimizált személyes adatok kezelése, míg a rendszer biztonságának fenntartása és csalások megelőzése érdekében – szigorúan meghatározott megőrzési idő rögzítése az így felvett adatok más célból történő felhasználásának korlátozása mellett – a jogos érdek érvényesítése érdekében kezelhetőek az ehhez szükséges személyes adatok.[156]

A gyakorlat alapján azonosítható, hogy az információbiztonsági célú intézkedéseket alapvetően a jogos érdek jogalap hatálya alatt ítélik meg, azonban a jogos érdek nem fogadható el, ha az adatkezelő egyéb célból is felhasználja az azokat. Így a francia adatvédelmi hatóság, a CNIL, a Google reCAPTCHA eszközzel kapcsolatosan mondta ki[157], melyet a Cityscoot felhasználói hitelesítés céljából használtak, hogy hozzájárulás szükséges ennek alkalmazásához. A Google reCAPTCHA egy biztonsági intézkedés, amelyet a weboldalak használnak annak érdekében, hogy megkülönböztessék az emberi felhasználókat a robotoktól, és így megelőzzék a weboldalak elleni visszaéléseket. Mivel a Google az ekként gyűjtött adatokat elemzési célokból is felhasználta, ezért a francia hatóság nem fogadta el, hogy ez az adatkezelési kizárólag felhasználói hitelesítés céljából és jogos érdek alapján szükséges és hozzájárulást követelt meg ehhez az adatkezeléshez.

[156] 29. cikk szerinti adatvédelmi munkacsoport keresőprogramokkal kapcsolatos adatvédelmi kérdésekről szóló 1/2008. vélemény 18–19. oldala

[157] CNIL - Délibération de la formation restreinte n° SAN-2023-003 du 16 mars 2023 concernant la société CITYSCOOT; Mardi 28 mars 2023; https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000047346903; https://www.cnil.fr/en/geolocation-rental-scooters-cityscoot-fined-eu125000; letöltés: 2024.08.25

Az online platformok továbbá használhatnak adatokat jogos érdek alapján elemzési célokra, például a felhasználói viselkedés elemzésére és a platform funkcionalitásának javítására, mely esetben az adatkezelő jogos érdeke a szolgáltatások és a felhasználói élmény javítása lehet. Számos adatvédelmi hatóság (beleértve a CNIL-t is[158]) szintén engedélyezi a felhasználóbarát, első féltől származó analitikai sütik használatát hozzájárulás nélkül. Ez azonban kizárólag anonim statisztikai adatokra korlátozódnak, amelyeket nem lehet a felhasználóhoz kapcsolni. Nem szabad más célra, például hirdetési vagy nyomkövetési célokra felhasználni őket; korlátozott, legfeljebb tizenhárom hónapos élettartammal kell rendelkezniük és az adatok kezelése során biztosítani kell, hogy az adatok azonnal anonimizálásra kerüljenek, így a felhasználók nem lesznek azonosíthatóak. Más adatvédelmi hatóságok[159] viszont ebben a körben sem fogadják el az analitikai sütik alkalmazását hozzájárulás nélkül.

A *Meta Platforms Inc. és társai kontra Bundeskartellamt* ügyben az Európai Bíróság részletesen foglalkozott azzal a kérdéssel, hogy egy olyan vállalkozás, mint a Meta Platforms Ireland, amely egy reklámbevételből finanszírozott digitális közösségi hálózatot üzemeltet, hivatkozhat-e jogos érdekek érvényesítésére, mint jogalapra, ha az általa kínált szolgáltatások keretében a felhasználói adatokat összegyűjti és felhasználja. Az érintett adatok a vállalatcsoport más szolgáltatásaiból és harmadik felektől származhatnak, és azokat olyan eszközökkel, mint a "Facebook Business Tools" interfészek, illetve cookie-k vagy hasonló technológiák alkalmazásával gyűjtik össze. A kérdés azt is érintette, hogy ezek az adatok összekapcsolhatók-e a felhasználó Facebook-fiókjával, és felhasználhatók-e a hirdetések személyre szabására, a hálózat biztonságára, a termékek fejlesztésére és a vállalatcsoport egységes használatára. A Bíróság ezzel kapcsolatosan megállapította, hogy a GDPR 6. cikk (1) bekezdésének f) pontja értelmében az adatkezelés jogszerű, ha három feltétel együttesen teljesül. Az első feltétel az adatkezelő vagy harmadik fél jogos érdekének fennállása, a második feltétel az adatkezelés szükségessége ezen érdek érvényesítéséhez, míg a harmadik feltétel,

[158] CNIL - Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019; https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042388179; Guide de configuration de la solution Contentsquare exemptée de recueil du consentement (“ Exemption Mode”); https://www.cnil.fr/sites/cnil/files/atoms/files/contentsquare_-_guide_de_configuration_solution_de_mesure_daudience_exemptee.pdf; lehívás: 2024.08.25

[159] vö. Irish Data Protection Commission - Do I need consent for analytics cookies? https://www.dataprotection.ie/en/faqs/cookies/do-i-need-consent-analytics-cookies; lehívás: 2024.09.11

hogy az érintett alapvető jogai és szabadságai nem élveznek elsőbbséget a jogos érdekkel szemben. A Bíróság szerint ezek vizsgálata a konkrét ügy összes körülményének mérlegelését igényli. Az adatkezelés szükségességére vonatkozóan a Bíróság hangsúlyozta, hogy az adatkezelőnek meg kell vizsgálnia, hogy az érintett jogait és szabadságait kevésbé sértő eszközökkel nem lehetne-e elérni ugyanazt a célt. Emellett az adattakarékosság elvének is érvényesülnie kell, azaz az adatkezelésnek csak a feltétlenül szükséges adatokra kell korlátozódnia. A Bíróság továbbá megjegyezte, hogy az érintettnek észszerűen számítania kell az adatkezelésre; különös figyelmet kell fordítani a gyermekek védelmére, mivel ők fokozott védelemre szorulnak a személyes adatok kezelése során.

A Bíróság részletesen megvizsgálta az egyes adatkezelési célokat a GDPR 6. cikk (1) bekezdésének f) pontja fényében és különböző megállapításokat tett, hogy egy online platform mikor és milyen körülmények között támaszkodhat jogos érdek jogalapra[160]. A *termékek fejlesztése* esetében a Bíróság nem zárta ki a jogos érdek lehetőségét, de hangsúlyozta, hogy az adatkezelés mértékét és hatását alaposan mérlegelni kell, különös tekintettel az érintettek alapvető jogaira. A *hálózat biztonságának biztosítása tekintetében* a Bíróság úgy vélte, hogy ez jogos érdek lehet, azonban az adatkezelés szükségességét és annak mértékét meg kell vizsgálni az adattakarékosság elvének figyelembevételével. A *kiskorúak esetében* a Bíróság különleges védelmet tartott indokoltnak, mivel ők kevésbé vannak tisztában a személyes adataik kezelésével kapcsolatos kockázatokkal, így ez az adatkezelés nem indokolható pusztán jogos érdek alapján. A *hirdetők, fejlesztők és más partnerek számára biztosított mérések és elemzések* esetében a Bíróság nem hozott konkrét megállapítást, de hangsúlyozta, hogy az érintett jogai és érdekei minden esetben elsőbbséget élvezhetnek, ezért ezt az adatkezelést és mérlegelést mindig egyedi vizsgálat tárgyává kell tenni. A marketingcélú kommunikációval és direktmarketinggel kapcsolatban a Bíróság elismerte, hogy ezek jogos érdeknek tekinthetők, de csak akkor, ha az érintett alapvető jogai és érdekei nem élveznek elsőbbséget. Az ilyen adatkezeléshez azonban kifejezett hozzájárulásra van szükség. A kutatás és fejlesztés a közjó érdekében nem került részletesen kifejtésre, mivel az előzetes döntéshozatali kérelem nem tartalmazott erre vonatkozó indoklást, így a Bíróság nem tudott állást foglalni ebben a kérdésben. Végül, a bűnüldöző szervek tájékoztatása és a hivatalos megkeresésekre adott válaszok kapcsán a Bíróság kimondta, hogy ezek nem tekinthetők jogos érdeknek, mivel nem

[160] Európai Unió Bírósága, C 252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság (ECLI:EU:C:2023:537); 106-126. pontok

kapcsolódnak közvetlenül az adatkezelő gazdasági tevékenységéhez. Az ilyen adatkezelés csak jogi kötelezettség teljesítése esetén igazolható. A konkrét ügyben a Bíróság megállapította, hogy a *tartalmak és hirdetések személyre szabása* esetében az érintett felhasználók nem számíthatnak arra, hogy hozzájárulásuk nélkül adatokat gyűjtenek és használnak fel ezen célra. Ebből következően az érintettek alapvető jogai és szabadságai elsőbbséget élveznek a Meta Platforms Ireland jogos érdekeivel szemben, különösen a hirdetések személyre szabása tekintetében, így ezen adatkezelés nem jogszerű jogos érdek alapján, tehát a Meta csoportnak más jogalapot kell azonosítania a személyes adatok jogszerű kezeléséhez, ami jelen esetben az érintett felhasználó hozzájárulása lehet. A Bíróság döntése tehát rávilágít arra, hogy a jogos érdek jogalapja nem alkalmazható automatikusan minden adatkezelési cél esetében, különösen a hirdetések személyre szabása tekintetében. A Meta csoportnak ebben az esetben más jogalapot kell találni, például az érintett hozzájárulását, hogy jogszerűen kezelhesse a személyes adatokat. Ez a döntés tehát fontos precedenst teremt az adatkezelési gyakorlatok értékelésében, különösen közösségi platformok esetében.

2.3.1.5.4 Jogos érdek és tiltakozás, mint sötét tervezési minta online platformok gyakorlatában

A jogos érdek és a tiltakozás kérdésköre gyakran kapcsolódik a sötét tervezési minták problémájához, különösen az online platformok adatkezelési gyakorlataiban, melyek célja a felhasználók manipulálása olyan döntések meghozatalára, amelyek nem feltétlenül az ő érdekeiket szolgálják, hanem az adatkezelő vállalat javát szolgálják.

Az online platformok azonban gyakran sötét tervezési minták alkalmazásával akadályozzák vagy bonyolítják meg a tiltakozás jogának gyakorlását. Ilyen gyakorlatok például[161] a *tiltakozási lehetőség elrejtése*, mikor a felhasználóknak nehéz megtalálni a tiltakozásra vonatkozó opciókat a felhasználói felület bonyolult elrendezése miatt; *zavaros tájékoztatás*, mikor a platformok homályos vagy zavaros nyelvezettel írják le a tiltakozáshoz kapcsolódó jogokat, így a felhasználók nem tudják világosan, mire is vonatkozik a jogos érdek, és hogyan élhetnek tiltakozási jogukkal; és az *eltérítés*, amikor a felhasználók megpróbálnak tiltakozni az

[161] vö. EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them; https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf; lehívás: 2024.09.13

adatkezelés ellen, a felület gyakran hosszadalmas vagy nehezen értelmezhető lépésekkel vezeti őket végig, amelynek eltántorító hatása lehet. Az egyik legismertebb példa az, amikor a platformok a cookie-beállításokban a hozzájárulás meg nem adását követően jogos érdek alapján próbálja meg folytatni az adatkezelést, például „személyre szabott tartalomprofil létrehozása" vagy „személyre szabott hirdetések kiválasztása" céljából. Mint az Európai Adatvédelmi Testület 2021-ben létrehozott Cookie Banner Munkacsoportjának 2023-as jelentése is rámutat, ha az ePrivacy irányelv 5. cikk (3) bekezdésében foglalt hozzájárulási követelmények nem teljesülnek, akkor az ezt követő adatkezelés nem lehet GDPR-kompatibilis és nem alapulhat az adatkezelő jogos érdekén[162]. Az ilyen manipulatív tervezési gyakorlatok rontják a felhasználói élményt, és aláássák a felhasználói jogokat, különösen a jogos érdek alapján történő adatkezelés ellen tiltakozás jogának érvényesítését.

2.3.1.6 Különleges adatok kezelésére vonatkozó további korlátozások

Online platformok csak szigorú feltételek mellett kezelhetnek különleges adatokat (például faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre, szakszervezeti tagságra, genetikai adatokra, biometrikus adatokra, egészségügyi adatokra, szexuális életre vagy szexuális irányultságra vonatkozó adatok). A GDPR 9. cikk (1) bekezdése általánosságban megtiltja a különleges adatok kezelését, de a 9. cikk (2) bekezdése néhány kivételt sorol fel, amelyek alapján mégis lehetséges ilyen adatok kezelése. Az online platformok kezelhetnek különleges adatokat, ha az *érintett kifejezetten hozzájárult* az adatkezeléshez egy vagy több meghatározott célból, illetve az EUB joggyakorlatára figyelemmel fogyatékossággal élő személyek vonatkozásában merülhet fel áttételesen egészségügyi személyes adatok [azaz a fogyatékosság tényére és jellegére vonatkozó] adatok kezelésének lehetősége. Ezen hozzájárulásnak önkéntesnek, konkrétnak, tájékozottnak és egyértelműnek kell lennie. Az online platformoknak biztosítaniuk kell, hogy a hozzájárulás visszavonása bármikor lehetséges legyen. Egészségügyi adatok esetében a magyar jog sajátossága, hogy a GDPR 9. cikk (4) bekezdése szerint nyitóklauzula alapján szigorúbb feltételeket rögzít az ilyen adatok kezelésére, ami a gyakorlatban azt jelenti, hogy az az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény 4. § (1) bekezdésében

[162] EDPB - Report of the work undertaken by the Cookie Banner Taskforce, Adopted on 17 January 2023; 24. pont; https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf; lehívás: 2024.09.13

meghatározott további szigorúbb jogalap feltételeknek is eleget kell tenni ilyen adatok kezelésekor.

Az Európai Bíróság *a Meta Platforms Inc. és társai kontra Bundeskartellamt ügyben*[163] foglalkozott a platformok által kezelt különleges kategóriájú személyes adatok kezelésének kérdésével és ennek korlátaival, ami jelentős iránymutatást adott a különleges kategóriájú személyes adatok kezelésének korlátairól és az ezzel kapcsolatos jogi feltételekről. Az ügy központi kérdése az volt, hogy a GDPR 9. cikke (1) bekezdése értelmében az olyan adatok kezelése, amelyek a felhasználó által megnyitott weboldalakról vagy alkalmazásokról származnak, és amelyeket a közösségi hálózat üzemeltetője rögzít (például cookie-k vagy integrált interfészek segítségével), a „különleges kategóriájú" adatok kezelésének minősül-e, különösen, ha ezeket az adatokat összekapcsolják a felhasználó közösségi hálózati fiókjával. Ezzel kapcsolatosan az Európai Bíróság rámutatott arra, hogy a GDPR 9. cikkének (1) bekezdése rögzíti a személyes adatok ott említett különleges kategóriáira vonatkozó adatkezelés tilalmának elvét, melynél fogva a tilalom alóli kivételeket megszorítóan kell értelmezni[164], összhangban a Bíróság eddigi állandó gyakorlatával.[165]A Bíróság kiemelte, hogy a GDPR 9. cikke (2) bekezdésének e) pontja alapján kivétel csak akkor alkalmazható, ha az érintett személy kifejezetten és félreérthetetlenül nyilvánosságra hozta az adatokat. A döntés értelmében az önmagában nem tekinthető kifejezett nyilvánosságra hozatalnak, ha a felhasználó olyan weboldalakat vagy alkalmazásokat nyit meg, amelyek különleges kategóriájú adatokat kezelnek, és ezekhez kapcsolódóan adatokat ad meg, vagy például „Like" gombra kattint. A Bíróság szerint az ilyen cselekmények nem elegendőek annak bizonyítására, hogy a felhasználó kifejezetten nyilvánosságra kívánta hozni ezeket a különleges adatokat. Ez a döntés kiemelkedő jelentőségű, mert megerősíti a GDPR 9. cikke szerinti védelem szigorúságát, különösen a különleges kategóriájú adatok kezelésének tekintetében. A Bíróság rámutatott, hogy az ilyen adatkezelés csak akkor jogszerű, ha az érintett félreérthetetlen és tudatos cselekvéssel nyilvánosságra hozza adatait. Ez védi a felhasználók alapvető jogait, mivel nem elegendő

[163] Európai Unió Bírósága, C 252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság (ECLI:EU:C:2023:537); https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1; lehívás: 2024.08.25

[164] vö. Európai Unió Bírósága, C 252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság; 76. sarokpontja

[165] vö. Európai Unió Bírósága, 2014. szeptember 17-i Baltic Agro ítélet, C-3/13, EU:C:2014:2227, 24. sarokpont, valamint az ott hivatkozott ítélkezési gyakorlat; 2019. június 6-i Weil ítélet, C-361/18, EU:C:2019:473, 43. sarokpontja, valamint az ott hivatkozott ítélkezési gyakorlat

pusztán az ilyen weboldalak használata vagy a közösségi hálózat fiókjával való kapcsolódás ahhoz, hogy ezen adatok kezelése automatikusan jogszerű legyen. A döntés emellett a megszorító értelmezés fontosságára hívja fel a figyelmet, különösen akkor, ha az adatkezelő arra hivatkozik, hogy az érintett maga hozta nyilvánosságra a különleges adatait.

Ezt meghaladóan az Európai Unió Bírósága az C-446/21. sz. ügyben meghozott ítéletében foglalkozott azzal a kérdéssel, hogy ha valamely személy kifejezetten nyilvánosságra hozott a Meta által üzemeltetett Facebook platformon egy, a szexuális irányultságára vonatkozó adatot a GDPR 9. cikk e) pontja értelmében, úgy ez milyen körben ad lehetőséget a személyes adatok kezelésére. A Bíróság megállapította, hogy ezt a különleges kategóriájú adatok kezelésére vonatkozó felhatalmazást megszorítóan kell értelmezni, az ilyen adatok a GDPR rendelkezéseinek tiszteletben tartása mellett kezelhetők. Ennél fogva nem állapítható meg, hogy az érintett személy a GDPR 9. cikke (2) bekezdésének a) pontja értelmében hozzájárulását adta ahhoz, hogy az online közösségi hálózati platform üzemeltetője a szexuális irányultságára vonatkozó más adatokat kezeljen, illetőleg nem hatalmazza fel az online közösségi hálózati platform üzemeltetőjét arra, hogy az illető szexuális irányultságára vonatkozó egyéb olyan adatokat kezeljen, amelyeket adott esetben e platformon kívül, harmadik személy partnerek alkalmazásaiból és weboldalairól szerez be az adatok összesítése és elemzése céljából annak érdekében, hogy ilyen adatok felhasználásával személyre szabott hirdetéseket kínáljon az ilyen érintett számára.[166]

2.3.2 Átláthatóság, transzparencia követelmények

A platformok átláthatósága a digitális környezetben fontos kérdés, különösen az EU adatvédelmi szabályai szempontjából. Az online platformok működésének szabályozásával kapcsolatosan az egyik legnagyobb probléma az átláthatóság hiánya és a felhasználókkal szembeni információs aszimmetria, melyet az FTC fent hivatkozott jelentése is kiemelt. A szabályozók jellemzően az átláthatósági intézkedésekkel próbáltak meg választ adni erre,

[166] lásd Európai Unió Bírósága, 2024. október 4-i Maximilian Schrems és a Meta Platforms Ireland Ltd ítélet, C-446/21, ECLI:EU:C:2024:834, 76-83. pontok.

azonban sokszor nehéz meghatározni, hogy ez mit jelent a digitális platformok gyakorlatában és hogyan lehet ezt megvalósítani[167].

Adatvédelmi kontextusban az átláthatóság azt jelenti, hogy az online platformnak, mint adatkezelőnek egyértelműen és nyíltan közölnie kell az érintettel a személyes adatok gyűjtésének, felhasználásának és megosztásának módját. Az átláthatóság követelménye keretében lehetővé kell tenni az érintettek számára, hogy megértsék az érintetti jogaikat, és szükség esetén éljenek azokkal. Az átláthatóság elvét a GDPR 5. cikk (1) bekezdés a) pontja határozza meg, amelynek követelményeit a GDPR 39. és az 58.-62. preambulumbekezdései és a GDPR 12 – 14. és 34. cikkei bontják ki. Az átláthatóság elvének támogatására bevezetett intézkedéseknek és garanciáknak e cikkek végrehajtását is támogatniuk kell.[168] Ezek a rendelkezések rögzítik, hogy az érintetteknek nyújtott információknak lehetővé kell tenniük, hogy az érintettek „tudatában legyenek a kockázatoknak", „a profilalkotás létezésének és az ilyen profilalkotás következményeinek", „az adatkezelőknek", „az adatkezelés céljainak", „az érintettek jogainak", „a megfelelő védelmi intézkedéseknek", valamint „minden egyéb olyan információnak, amely a tisztességes és átlátható adatkezelés biztosításához szükséges". Mindezt figyelembe kell venni az adott személyes adatok kezelése során fennálló sajátos körülményeket és kontextust, és az információkat „könnyen érthető" módon, „világos és egyszerű nyelvezetet" használva kell megadni. Amennyiben automatizált döntéshozatal, beleértve a profilalkotást is, történik, legalább az alkalmazott logikáról, valamint annak jelentőségéről és várható következményeiről lényeges információt is nyújtani kell.[169]

A 29. cikk szerinti adatvédelmi munkacsoport iránymutatást[170] tett közzé az adatvédelmi szempontú átláthatóságról. Az iránymutatás szerint az átláthatóság a GDPR értelmében olyan általános előírás, amely az alábbi három központi területre alkalmazandó: (1) a tisztességes adatkezeléssel kapcsolatos tájékoztatás nyújtása az érintettek részére; (2) az érintettek

[167] Arcangelo Leone de Castris - Types of Platform Transparency: An Analysis of Discourse Around Transparency and Global Digital Platforms; Public Integrity; https://doi.org/10.1080/10999922.2024.2304741; lehívás: 2024.08.25

[168] EDPB - 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről 2.0 változat Elfogadás időpontja: 2020. október 20.; https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf; lehívás: 2024.08.25

[169] vö. AEPD - Artificial Intelligence: Transparency; https://www.aepd.es/en/prensa-y-comunicacion/blog/artificial-intelligence-transparency, ahol a spanyol adatvédelmi hatóság kifejti az Mesterséges Intelligencia rendelet és a GDPR transzparencia rendelkezései közötti viszonyt; lehívás: 2024.08.25

[170] A 29. cikk szerinti munkacsoport Iránymutatás az (EU) 2016/679 rendelet szerinti átláthatóságról; WP260 rev.01 („Transzparencia iránymutatás")

adatkezelők általi tájékoztatása az érintettek GDPR szerinti jogaival kapcsolatban; valamint (3) annak módja, hogy az adatkezelők miként könnyítik meg az érintettek számára jogaik gyakorlását[171]. Az átláthatóság az adatkezelési ciklus valamennyi szakasza során alkalmazandó; így az adatkezelési ciklus előtt vagy annak kezdetén, azaz amikor sor kerül a személyes adatoknak az érintettől vagy más módon történő gyűjtésére; a teljes adatkezelési időszak alatt, azaz az érintettek jogaikról való tájékoztatása során; valamint az adatkezelés folyamán bizonyos pontokon, például amikor adatvédelmi incidens történik, vagy az adatkezelés jelentős mértékben megváltozik[172]. Az átláthatóság biztosítása érdekében a munkacsoport különösen digitális környezetben többszintű adatkezelési tájékoztatók alkalmazását javasolja[173]. A vonatkozó tájékoztatásnak tömörnek, átláthatónak, érthetőnek és könnyen hozzáférhetőnek kell lennie, összhangban a GDPR 12. cikkével és azt egyértelműen el kell különíteni az egyéb, nem adatvédelemmel kapcsolatos tájékoztatástól, például a szerződéses rendelkezésektől vagy általános felhasználási feltételektől.[174]

A digitális platformoknak különleges felelőssége van az átláthatóság terén, mivel jelentős mennyiségű felhasználói adatot kezelnek. Ennek megfelelően az online platformoknak világosan kommunikálniuk kell, hogy milyen típusú adatokat gyűjtenek, milyen célból, és hogyan használják fel ezeket a személyes adatokat. Amennyiben a platformok harmadik felekkel is megosztják az adatokat, ezt is átláthatóan kell közölniük, beleértve azt, hogy kik ezek a harmadik felek, és milyen célból történik az adatok megosztása. Ezt meghaladóan a platformoknak tájékoztatniuk kell a felhasználókat a cookie-k és egyéb nyomonkövetési technológiák használatáról, és lehetőséget kell biztosítaniuk a felhasználóknak, hogy ezeket kezelhessék, elutasíthassák, illetve a hozzájárulásukat visszavonhassák.

2.3.3 Tisztességes adatkezelés elve

A tisztességes eljárás olyan átfogó elv, amely megköveteli, hogy a személyes adatokat ne kezeljék az érintettre nézve indokolatlanul hátrányos, jogellenesen hátrányosan megkülönböztető, váratlan vagy félrevezető módon. A tisztességes eljárás elvét megvalósító intézkedések és garanciák az érintettek jogait és szabadságait is támogatják, különösen a

[171] Vö. Transzparencia Iránymutatás 1. sarkpontja
[172] Vö. Transzparencia Iránymutatás 5. sarkpontja
[173] Vö. Transzparencia Iránymutatás 35. sarokpontja
[174] Vö. Transzparencia Iránymutatás 8. sarokpontja

tájékoztatáshoz való jogot (átláthatóság), a beavatkozáshoz való jogot (hozzáférés, törlés, adathordozhatóság, helyesbítés) és az adatkezelés korlátozásához való jogot (ahhoz való jog, hogy az érintettre ne terjedjen ki az egyedi ügyekben történő automatizált döntéshozatal és az érintettek hátrányos megkülönböztetésének tilalma ezekben az eljárásokban).[175]

A tisztességes eljárás elvét az online környezetben gyakran sértik a különféle platformok által alkalmazott manipulációs gyakorlatok, különösen a sötét mintázatok. Ezek a gyakorlatok jelentősen befolyásolják a felhasználók hozzájárulását és döntéshozatalát a digitális térben. Az ilyen problémák kezelésére irányuló adatvédelmi és fogyasztóvédelmi hatósági iránymutatások, végrehajtási intézkedések és jogi értelmezések kiemelik a tisztességes eljárás, átláthatóság és a valódi felhasználói hozzájárulás fontosságát, különösen személyes adatok kezelése során.

Az Európai Adatvédelmi Testület (EDPB) 2022-ben iránymutatást[176] adott ki a közösségi média platformok felhasználói felületein alkalmazott sötét mintázatokról. Az útmutató hangsúlyozza, hogy a tisztesség, mint alapelv (GDPR 5. cikk (1) a) pont), megköveteli, hogy a személyes adatokat ne dolgozzák fel hátrányos, diszkriminatív, váratlan vagy félrevezető módon. Az útmutató általános elveket tartalmaz a sötét mintázatokkal kapcsolatban, és példákat hoz fel a sütik használatára, amelyeket különböző kategóriákba sorol (felhasználói figyelem túlterhelése, akadályozás, homályosság), valamint a legjobb gyakorlatokat mutat be a sötét mintázatok elkerülésére.

Az Európai Bizottság által koordinált vizsgálat során a Fogyasztóvédelmi Együttműködési Hálózat 2022-ben 399 weboldalt és alkalmazást vizsgált meg a sötét mintázatok szempontjából. A vizsgálat számos manipulációs gyakorlatot azonosított, mint például az információk elrejtése vagy hamis hierarchia, előre bejelölt hozzájárulást jelölő vezérlők, zaklató jellegű felugró ablakok, nehezen elutasítható cookie-k és kötelező regisztrációk. Ezek a gyakorlatok aláássák a felhasználók döntéshozatali autonómiáját és gyakran a fogyasztói jogokat sértik. A sötét

[175] EDPB - 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről 2.0 változat; 69. sarokpont

[176] EDPB - Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them Version 2.0 https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf; lehívás: 2024.08.25

mintázatok kereskedelmi gyakorlatként való használata kapcsán az irodalomban[177] a legkomolyabb fenntartás az egyéni fogyasztói jóléttel kapcsolatban fogalmazódik meg, amely három fő kategóriára osztható: (i) gazdasági kár [amikor a sötét mintázatok olyan pénzügyi veszteséget okoznak, amely egy olyan vásárlás következménye, amelyet a fogyasztó egyébként nem tett volna meg]; (ii) a magánélet megsértése [amikor a sötét mintázatok aláássák a fogyasztók magánéletét, például alapértelmezett beállítások és sütik elfogadása révén], és (iii) kognitív teher [amikor a sötét mintázatok szükségtelen idő-, energia- és figyelemráfordítást okoznak]. A sötét mintázatokat olyan gyakorlatként tartják számon, amely aláássa az egyéni döntéshozatalt és autonómiát. Ennek alapján a fogyasztóvédelmi hatóságok hivatkozhatnak a tisztességtelen kereskedelmi gyakorlatokról szóló irányelv rendelkezéseire és annak nemzeti végrehajtására, és fogyasztóvédelmi bírságot szabhatnak ki a sötét mintázatokat alkalmazó weboldal vagy alkalmazás üzemeltetőjére.

A belső piacon a vállalkozások és fogyasztók közötti tisztességtelen kereskedelmi gyakorlatokról szóló, az Európai Parlament és a Tanács 2005/29/EK irányelvének értelmezéséről és alkalmazásáról szóló bizottsági iránymutatás[178] a 1.2.10. pontjában szintén hivatkozik a tisztességtelen kereskedelmi gyakorlatokról szóló irányelv, a GDPR és az e-Privacy irányelv közötti kapcsolatra, és megerősíti az adatkezelési és adatgyűjtési gyakorlatok jelentőségét a fogyasztóvédelem és a tisztességtelen kereskedelmi gyakorlatok szempontjából. Ezt kiegészíti a Meta (Facebook) kontra Bundeskartellamt ügy [C-252/21 számú ügy (Meta Platforms Bundeskartellamt)] az Európai Unió Bíróságán, amely ítélet megállapítása szerint a versenyhatóságok az értékelésük során figyelembe vehetik a kereskedelmi gyakorlatok GDPR rendelkezésekkel való összeegyeztethetőségét.

[177] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. 2021. What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 360, pp. 1–18. https://doi.org/10.1145/3411764.3445610; vö. European Commission - Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation - Final Report; April 2022; p. 90;

[178] A Bizottság közleménye – Iránymutatás a belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól szóló 2005/29/EK európai parlamenti és tanácsi irányelv értelmezéséhez és alkalmazásához (EGT-vonatkozású szöveg); C/2021/9320; HL C 526., 2021.12.29, pp. 1–129; https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv%3AOJ.C_.2021.526.01.0001.01.HUN&toc=OJ%3AC%3A2021%3A526%3AFULL, lehívás: 2024.09.09

A hazai gyakorlatban Gazdasági Versenyhivatal (GVH) úgy véli, hogy a személyes adatok védelme a fogyasztói jólét része, és az online termékek adatvédelmi vonatkozásai jelentős termékjellemzőnek minősülnek. A Google Allo ügyben (VJ/88/2016. ügy) például a GVH megállapította, hogy az adatkezelés átláthatósága kulcsfontosságú a fogyasztók tájékozott döntéshozatalában. A TikTokkal kapcsolatos legutóbbi döntésében[179] a GVH hangsúlyozta, hogy az adatkezelési gyakorlatok a tisztességtelen kereskedelmi gyakorlatok keretében jelentősek, és a „szakmai gondosság" kötelezettsége magában foglalja azt a modellt, amely szerint a személyes adatok kezelése és a sütikhez való hozzájárulás a fogyasztó hozzájárulása nélkül csak az online szolgáltatás nyújtásához szükséges mértékig korlátozódhat. Hasonló megállapításokat tett a GVH a Viber ügyben[180], amely szintén kötelezettségvállalással zárult és figyelembe vette az Európai Adatvédelmi Testület „hozzájárulás vagy fizetés" modellel kapcsolatos iránymutatását is.

2.3.4 Célhoz kötöttség

A célhoz kötöttség elve kiemelten fontos az adatvédelmi jogszabályokban és nemzetközi egyezményekben, mert biztosítja, hogy a személyes adatokat csak az előre meghatározott, konkrét és jogszerű célok érdekében kezeljék. Ez az elv védi az egyének magánszféráját, korlátozza az adatokkal való visszaélés lehetőségét, és elősegíti az átláthatóságot, az egyének adatainak biztonságát és jogi védelmét. A célhoz kötöttség követelménye azt jelenti, hogy az adatkezelő meghatározott, egyértelmű és jogszerű célból gyűjthet adatokat, és azokat nem kezelheti a gyűjtésük céljával össze nem egyeztethető módon, melyet a GDPR 5. cikk (1) bekezdés b) pontja rögzít követelményként. Az adatkezelés formáját ezért annak megfelelően kell kialakítani, hogy mi szükséges a célok elérése szempontjából. Amennyiben további adatkezelésre kerül sor, az adatkezelőnek először meg kell győződnie arról, hogy ezen adatkezelés céljai összeegyeztethetők az eredeti célokkal, és ennek megfelelően kell

[179] GVH - VJ/24-185/2020; 2024. november 27.
[180] GVH - VJ/6/2020.; https://www.gvh.hu/sajtoszoba/sajtokozlemenyek/2024-es-sajtokozlemenyek/szamos-ponton-modosit-a-viber-a-gvh-eljarasanak-koszonhetoen; lehívás: 2024.08.25

megterveznie az ilyen adatkezelést.[181] A 29. cikk szerinti munkacsoport részletes útmutatást nyújtott a célhoz kötöttség 95/46/EK irányelv szerinti elvének értelmezéséhez.[182]

A célhoz kötöttség elve azért lényeges, mert biztosítja, hogy a személyes adatokat csak olyan célokra használják fel, amelyekre eredetileg gyűjtötték őket, és hogy a felhasználók tisztában legyenek azzal, hogyan kezelik adataikat. Ez az elv két fő részből áll: egyrészt a személyes adatok gyűjtése előtt világosan meg kell határozni, hogy azokat milyen célra fogják felhasználni, másrészt tilos az adatokat más célokra felhasználni. Ez különösen az online platformok olyan gyakorlatai esetén releváns, mint az adatelemzés és a viselkedés alapú hirdetések, mesterséges intelligencia alapú tartalom- vagy termékajánlások, egyedi árazások, ahol gyakran olyan célból használják fel az adatokat, amelyekkel adott esetben az érintett felhasználók egyáltalán nem számolnak.

Az Európai Adatvédelmi Biztos online manipulációról szóló véleménye kiemeli a célhoz kötöttség követelményének online platformok adatkezelési gyakorlatában való fontosságát[183]. Az online platformok által alkalmazott adat-elemzés olyan módszereket és felhasználási mintákat foglal magában, amelyeket sem az adatokat gyűjtő szervezet, sem az érintettek nem vettek figyelembe, vagy nem is tudtak volna elképzelni az adatgyűjtés időpontjában. A személyes adatok algoritmikus kezelése lehetőséget teremt új adatok generálására. Amikor egy érintett néhány különálló adatot oszt meg, gyakran előfordulhat, hogy ezek az adatok egyesíthetők, másod- és harmadgenerációs adatokat hozva létre az adott személyről. A közösségi média platformok által biztosított eszközök használatával ezek az adatok kombinálhatók demográfiai információkkal (pl. családi állapotra vonatkozó adatokkal) és az egyének viselkedésére és érdeklődési köreire vonatkozó információkkal, vagy a felhasználók által használt eszköz adatokkal, amelyekből további más, például vagyoni vagy szociális helyzetre utaló következtetések vonhatók le. Az algoritmusok segítségével történő profilokból származó adatok más célokra való felhasználásával kapcsolatos fenntartás, hogy az eredeti céltól való eltérő célú adatkezelés során olyan többletadatok és következtetések vonhatók le az

[181] Lásd EDPB 4/2019. számú iránymutatása a 25. cikk szerinti beépített és alapértelmezett adatvédelemről; 71. sarokpont
[182] Lásd 29. cikk szerinti munkacsoport. „03/2013. számú vélemény a célhoz kötöttségről”. WP 203, 2013. április 2. ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2013/wp203_en.pdf; lehívás: 2024.09.13
[183] EDPS Opinion 3/2018 - Opinion on online manipulation and personal data; pp. 15.-16.

érintettekre vonatkozóan [pl. szexuális orientációra vonatkozóan[184]], amelyek akár különleges kategóriájú személyes adatoknak is minősülhetnek, és amely adatok kezelésére az online platformnak nincs jogalapja. Az adatok újra felhasználása hátrányosan érinti az egyén információs önrendelkezési jogát, tovább csökkenti az érintettek adatainak feletti kontrollját, és így csökkenti a digitális környezetbe és szolgáltatásokba vetett bizalmat [szintén eklatáns példája ennek a Reddit nevű fórum tőzsdei bevezetése előtti azon magatartása, hogy lényegében a felhasználói által generált tartalmakat – amelyeket nyilvánvalóan nem azzal a céllal írtak a felhasználók – mesterséges intelligencia algoritmusok tanításához értékesítette harmadik felek számára[185]]. Ezért kulcsfontosságú a célhoz kötöttség, mint az adatvédelmi jog egyik alapelve. Az Európai Adatvédelmi Biztos ezért lényegesnek tekintette, hogy az érintetteket tájékoztatni kell a jövőbeni adatkezelési formákról, amelyekben részt fognak venni, és szorosan figyelemmel kell kísérniük gyakorlataikat, hogy biztosítsák, hogy az adatkezelés ne lépje túl az ezen célokra megengedett határokat.[186]

A célhoz kötöttséggel kapcsolatosan lényeges utalni a GDPR 6. cikk (4) bekezdésébe foglalt ún. *kompatibilitási követelményekre*, amely rendelkezés az adatkezelési cél megváltozása esetén lehetővé teszi az új és a korábbi cél kompatibilitása alapján a személyes adatok további kezelését, feltéve, hogy az adatkezelés nem hozzájáruláson vagy jogszabályon alapul és amely rendelkezés kiegészíti a célhoz kötöttség alapelvének alkalmazását. A GDPR 5. cikk (1) bekezdés b) pontja szerint ugyanis a személyes adatok további kezelése az eredeti jogalap alapján nem megengedett, ha az olyan módon történik, amely nem egyeztethető össze az adatok gyűjtésekor meghatározott, egyértelmű és jogszerű célokkal. Ez egyben azt is jelenti, hogy az adatkezelő online platform a célváltozás esetén az adatkezelést az eredeti adatkezelési jogalapra alapozhatja, ha az új cél összeegyeztethetőnek, kompatibilisnek minősül az eredeti adatkezelési céllal. Ez gyakorlatilag azt jelenti, hogy ez a rendelkezés célváltozás esetén – ha ez a cél nem tér el lényeges mértékben az eredeti céltól – lehetőséget ad a személyes adatok további kezelésére az eredeti jogalapon anélkül, hogy ahhoz az érintettől külön hozzájárulásra vagy jogszabályi engedélyre lenne szükség. Az új célt megfelelően *konkretizálni* és

[184] Európai Unió Bírósága, C-184/20. sz. ügy, OT és a közszolgálati összeférhetetlenség megelőzésével foglalkozó litván főbizottság között (ECLI:EU:C:2022:601); https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:62020CJ0184; lehívás: 2024.09.09

[185] CNBC: FTC conducting inquiry into Reddit's AI data-licensing practices ahead of IPO; https://www.cnbc.com/2024/03/15/ftc-investigating-reddit-over-ai-data-licensing-practices-ahead-of-ipo.html , 2024.09.15.

[186] EDPS Opinion 3/2018 EDPS Opinion on online manipulation and personal data; pp 15-16

elszámoltathatósági követelményeknek megfelelően *dokumentálni szükséges* és azt az eredeti adatgyűjtési céllal is össze kell hasonlítani. A GDPR 6. cikk (4) bekezdés a)-e) pontjai meghatározzák, hogy milyen szempontokat kell figyelembe venni annak megállapítására, hogy egy új adatkezelési cél összeegyeztethető-e az eredeti célokkal. Ez az értékelési folyamat, amelyet „*kompatibilitási tesztnek*" neveznek, a következő fő szempontokat veszi figyelembe, figyelemmel a 29. cikk szerinti adatvédelmi munkacsoport célhoz kötöttségről szóló 03/2013. számú korábbi véleményére:

(i) *Az eredeti és az új cél közötti kapcsolat*, hogy az új cél milyen mértékben és hogyan kapcsolódik az eredeti célhoz. Célok összeegyeztethetősége például fennállhat, ha a már meglévő adatok egy aktív ügyféllel történő kereskedelmi kommunikáció céljából kerülnek kezelésre, figyelembe véve az általa megvásárolt termékeket vagy szolgáltatásokat. Ez azonban csak akkor igaz, ha a kommunikáció módja és formája is összeegyeztethető ezzel. Ez fennállhat közösségi hálózatok tagjainál is, azonban nem terjed ki olyan személyekre, akik nem tagjai a közösségi platformnak, vagy a platform továbbfejlesztésére vagy új szolgáltatások felkínálsására.[187] Ugyanígy az adatok monetizálásánál sem alkalmazható ez, még ha a profilozás és ezen profilok monetizálása (reklámozás) ingyenes platformszolgálatások esetén gazdaságilag összefügghetnek, mivel ezek a célok eltérnek egymástól.[188] Akkor sem áll fenn a kompatibilitás, ha harmadik személy végzi az adatkezelést, különösen reklámozás céljából[189], amely különösen releváns online platformok és a hozzájuk kapcsolódó reklámozási ökoszisztémák (így retal-time-bidding[190]) adatkezelése esetében. A GDPR 5. cikk (1) bekezdés b) pontja vélelmet rögzít, hogy a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés kompatibilis az adatkezelési céllal, azonban a platformok Big-Data analitikai célú adatkezelése már nem tartozik ebbe a körbe, ha ezt nem közérdekű, hanem kereskedelmi célból végzik ezeket.[191]

[187] Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), Datenschutzrecht. DSGVO mit BDSG (Nomos 2019), 1. Auflage; Artikel 6. Abs. 4.; Rn 37., p. 459
[188] Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), Datenschutzrecht. DSGVO mit BDSG (Nomos 2019), 1. Auflage; Artikel 6. Abs. 4.; Rn 38., p. 459
[189] Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), Datenschutzrecht. DSGVO mit BDSG (Nomos 2019), 1. Auflage; Artikel 6. Abs. 4.; Rn 40., p. 459
[190] Irish Council for Civil Liberties - The Biggest Data Breach, ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe - 16 May 2022; https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/; lehívás: 2024.09.15
[191] Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), Datenschutzrecht. DSGVO mit BDSG (Nomos 2019), 1. Auflage; Artikel 6. Abs. 4.; Rn 42., p. 460

(ii) *Az adatgyűjtés körülményei*, melynek keretében az adatkezelőnek értékelnie kell az érintettek és az adatkezelő közötti kapcsolatot (pl. esetleges ügyfélkapcsolat fennállását), az eredeti adatgyűjtés körülményeit, különös tekintettel arra, hogy az érintett mennyire volt tudatában annak, hogy adatait később más célokra is felhasználhatják. Ezzel kapcsolatosan különösen az érintett elvárásainak és a részére adott tájékoztatásnak van szerepe és jelentősége van annak, hogy az érintett számolhat-e az adatai továbbításával, ami az kompatibilitás ellen szóló érv lehet. Profilozás esetén, az erre vonatkozó intézkedésekről szintén tájékoztatást kell adni. Ezek csak akkor tekinthetők kompatibilisnek, ha az adatgyűjtés időpontjában az érintett személy számára előre láthatóak voltak, vagy ha azokat ő maga kezdeményezte. Az érintett személy nem számíthat azokra a profilalkotásokra, amelyek számára előzetesen nem voltak ismertek; ezek nem felelnek meg az érintett ésszerű elvárásainak.[192]

(iii) *Az adatok jellege*: az adat típusától is függ a kompatibilitás, mivel különleges kategóriájú adatok és bűnügyi személyes adatok kezelése esetén szigorúbb feltételek érvényesek, az érintett jogainak és szabadságainak nagyobb kockázata miatt. Ugyanez vonatkozik gyermekek és sérülékenynek minősülő érintettek adataira, mivel esetükben szintén magasabb adatvédelmi kockázatokat lehet feltételezni a célváltozás esetében.

(iv) *Az adatkezelés következményei az érintettre nézve*: Az adatkezelőnek értékelnie kell, hogy az új cél milyen hatással van az érintettekre, jelentős beavatkozást jelent-e az érintettek magánszférájába, vagy magasabb kockázatot jelent számukra, amely esteben valószínűsíthető, hogy új jogalapra lesz szükség az adatkezelés jogszerűségéhez. Itt mind a pozitív, mind a negatív következményeket figyelembe kell venni.[193] Ha a további adatkezelés az érintett személy számára összességében hátrányos következményekkel járhat, az rendszerint a célok összeegyeztethetősége ellen szól. Ha a következmények az érintett személy számára nem, vagy csak nehezen becsülhetőek, mert nem tudja pontosan, ki kezeli az adatokat, kik ismerik meg ezeket az adatokat, vagy milyen következmények kapcsolódnak az adatokhoz, az mind a célok összeegyeztethetőségével ellentétes lehet[194] és jelentősége van, hogy mennyiben érinti, illetve

[192] Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), Datenschutzrecht. DSGVO mit BDSG (Nomos 2019), 1. Auflage; Artikel 6. Abs. 4.; Rn 51., p. 461
[193] Lásd 29. cikk szerinti munkacsoport. „03/2013. számú vélemény a célhoz kötöttségről". WP 203, 2013. április 2.; 25. oldal ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2013/wp203_en.pdf; lehívás: 2024.09.15
[194] Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), Datenschutzrecht. DSGVO mit BDSG (Nomos 2019), 1. Auflage; Artikel 6. Abs. 4.; Rn 56., p. 462

korlátozza ez az érintett információs önrendelkezési jogát.[195] A modern adatkezelések olyan körülményei között, melyek az online platformok üzleti modelljéhez kapcsolódnak, mint a Big Data alkalmazások, mesterséges intelligencia, gépi tanulás alkalmazása, kontextusfelismerés, az Internet of Things [IoT] és a mindenütt jelenvaló számítástechnika [ubiquitous computing, ubicomp] alkalmazásaival kapcsolatban a célváltoztatások lehetséges érintettre vonatkozó következményeinek figyelembevétele csak korlátozottan működhet, figyelemmel arra, hogy az érintett csak korlátozott lehetőségekkel rendelkezik ezek működésére és befolyásolására.[196]

(v) *A megfelelő biztosítékok megléte*: ezzel kapcsolatosan az adatkezelő által alkalmazott védelmi intézkedések, például a pszeudonimizálás (a nyers adatok törlésével) vagy titkosítás relevánsak, amelyek minimalizálhatják az érintettre vonatkozó adatvédelmi kockázatokat. Ezek az intézkedések hozzájárulhatnak ahhoz, hogy az új cél és az eredeti cél összeegyeztethető legyen. A biztosítékok megléte azt jelzi, hogy az adatkezelő megfelelő módon védi az érintettek személyes adatait, így enyhítheti az új cél okozta esetleges kockázatokat.

A célhoz kötöttség és a kompatibilitási teszt fent bemutatott követelményeit online platformok esetében közvetlenül befolyásolják az ePrivacy rendelet és az Elkertv. adatvédelmi követelményei. Az ePrivacy irányelv 5. cikk (3) bekezdése ugyanis ezzel kapcsolatosan további szabályokat hoz be az elektronikus kommunikáció területén. Ha például a cookie-k használatára kerül sor a felhasználó nyomon követésére vagy profilalkotására, az ePrivacy irányelv szerinti előzetes hozzájárulás szükséges, ami adott esetben kizárhatja a kompatibilitási teszt alkalmazását. Ennek eredményeként az adatok olyan célokra való felhasználása, amelyek nem állnak összhangban az eredeti célokkal (pl. marketing vagy felhasználói elemzések), új jogalapot, így hozzájárulás megszerzését igényli. Az ePrivacy irányelv célja ugyanis, hogy biztosítsa a végberendezések adatainak fokozott védelmét, például a cookie-k vagy egyéb nyomkövető eszközök esetében. Míg a GDPR szerint egy célváltozás megengedett lehet, ha az új cél összeegyeztethető az eredeti céllal (GDPR 6. cikk (4) bekezdés), addig az ePrivacy irányelv szigorúan előírja, hogy a felhasználói hozzájárulást újra meg kell szerezni, ha az új cél nem illeszkedik szorosan az eredeti célhoz, vagy ha az a felhasználói végberendezés további manipulációját, ahhoz történő hozzáférést igényel. Például, ha egy szolgáltató cookie-t használ

[195] Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), Datenschutzrecht. DSGVO mit BDSG (Nomos 2019), 1. Auflage; Artikel 6. Abs. 4.; Rn 59., p. 462
[196] Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), Datenschutzrecht. DSGVO mit BDSG (Nomos 2019), 1. Auflage; Artikel 6. Abs. 4.; Rn 58., p. 462

a weboldal technikai működéséhez, majd a műszaki közléstovábbítás és szolgáltatás nyújtási célokat meghaladó körben kívánja használni az adatokat, az ePrivacy irányelv szerint ehhez újabb hozzájárulást kell kérnie, amely ezáltal nem biztosít lehetőséget a kompatibilitási teszt alkalmazására. Ezzel kapcsolatosan Magyarországon az Elkertv. 13/A § (4) bekezdése releváns, amelynek értelmében a szolgáltató a szolgáltatás igénybevételével kapcsolatos adatokat bármely, a szolgáltatási szerződés létrehozásától, módosításától, teljesítésének figyelemmel kísérésétől, az abból származó díjak számlázásától, vagy az azzal kapcsolatos követelések érvényesítése vagy a szolgáltatás nyújtásától eltérő célból – így különösen szolgáltatása hatékonyságának növelése, az igénybe vevőnek címzett elektronikus hirdetés vagy egyéb címzett tartalom eljuttatása, piackutatás céljából – csak az adatkezelési cél előzetes meghatározása mellett és az igénybe vevő hozzájárulása alapján kezelhet. Mivel minden ilyen további adatkezelési cél kötelezően hozzájárulást igényel az Elkertv. alapján, ebből következően a magyar jog alapján az információs társadalommal kapcsolatos szolgáltatások körében szűk körre korlátozott a GDPR 6. cikk (4) bekezdésének alkalmazása.[197]

2.3.5 Adattakarékosság

Az adatminimalizálás elve a GDPR egyik alapvető követelménye, amely különösen releváns a digitális platformok működésében és előírja, hogy a személyes adatoknak „*az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lenniük, és a szükségesre kell korlátozódniuk*”. Az adatminimalizálás az *arányosság elvét* fejezi ki[198] és azt jelenti, hogy a digitális platformok

[197] Itt említendő a NAIH NAIH-6737-1/2024. számú határozata, melyben jogszerűnek ismerte el az e-mailes ügyfélelégedettségi felmérést egy csomagküldő cégnél, ahol a felmérésre vonatkozó felhívást a kézbesítéssel kapcsolatos státuszüzenetben helyezték el. A NAIH egy csomagküldő cég adatkezelését vizsgálta, és jogszerűnek találta azt a gyakorlatot, amelyben az adatkezelő a kézbesítési státuszüzenetben helyezett el ügyfélelégedettségi felhívást. A hatóság szerint ez az adatkezelés kompatibilis volt a szerződés teljesítésével, így nem volt szükséges külön jogalap ehhez. A NAIH megállapította, hogy a státuszüzenetek küldése és az ügyfélelégedettség mérése a szolgáltatással, annak teljesítésével és értékelésével, mint egységes vásárlási folyamattal függ össze. Az érintett magánszféráját a hatóság nem sértette, mivel a felkérés a kézbesítés sikerességéről szóló értesítés mellett elhelyezett elektronikus levélben szerepelt, amelyet a címzett figyelmen kívül hagyhatott. Németországban hasonló esetben, amikor az Amazon a számlalevélben helyezett el ügyfélelégedettségi felhívást, a német szövetségi legfelsőbb bíróság (VI ZR 225/17) eltérő döntésre jutott. Az európai jogra (a reklám fogalmára) hivatkozva közvetlen üzletszerzésnek minősítette az ilyen gyakorlatot annak lojalitási funkciója miatt, és a soft-opt in (E-Privacy Irányelv 13. cikk (2) bekezdése) hatálya alá rendelte azt. Ha a NAIH a német bírósághoz hasonlóan reklámnak minősítette volna az elégedettség felmérést, akkor a kompatibilitási teszt alkalmazása is kizárt lett volna, mert akkor a hozzájárulási követelmények alá kellett volna rendelni ezt az adatkezelést.

[198] lásd Európai Unió Bírósága, 2024. október 4-i Maximilian Schrems és a Meta Platforms Ireland Ltd ítélet, C-446/21, ECLI:EU:C:2024:834, 50. pont; 2021. június 22-i Latvijas Republikas Saeima [Büntetőpontok] ítélet, C-439/19, EU:C:2021:504, 98. pont, valamint az ott hivatkozott ítélkezési gyakorlat; 2024. január 30-i Direktor na Glavna direktsia »Natsionalna politsia« pri MVR – Sofia ítélet, C-118/22, EU:C:2024:97, 41. pont

csak azokat a személyes adatokat gyűjthetik, tárolhatják és dolgozhatják fel, amelyek feltétlenül szükségesek az adatkezelés konkrét céljainak eléréséhez. Másrészről az adatminimalizálás követelménye a személyes adatok olyan *kezelésének időbeli korlátozását* is megköveteli, hogy az adatkezelő köteles a szóban forgó személyes adatok gyűjtésének időszakát a tervezett adatkezelés céljára tekintettel a feltétlenül szükséges mértékre korlátozni[199]. Az adatgyűjtést ennek alapján korlátozni kell azokra az adatokra, amelyek elengedhetetlenek a platform szolgáltatásainak nyújtásához. Online platformok esetében pedig az adatminimalizálás alkalmazása több kihívást és lehetőséget hordoz magában. Sok esetében nehéz pontosan meghatározni, hogy mely adatok szükségesek a platform szolgáltatásainak biztosításához, különösen, ha a platform többféle szolgáltatást kínál. A különböző rendszerekből és forrásokból származó adatok integrációja kihívást jelenthet az adatminimalizálás gyakorlati megvalósítása során. Sok platform üzleti modellje az adatok gyűjtésére és elemzésére épül, ami szemben állhat az adatminimalizálás elvével. A versenytársak gyakran versenyelőnyt szerezhetnek a felhasználói adatok szélesebb körű elemzésével, ami nyomást gyakorolhat a platformokra az adatminimalizálás elvének betartása ellen.

A német adatvédelmi hatóságok grémiuma, a DSK[200] az adatminimalizálás elvével indokolta azt, hogy az online kereskedelemben biztosítani kell a vendég hozzáférés, illetőleg a vendég vásárlás lehetőségét, állandó ügyfélfiók létrehozása nélkül és az ügyfelek hozzájárulását kell kérni minden olyan további adatkezeléshez, amely túlmutat az adott online tranzakció lebonyolításán.

Az Európai Unió Bírósága az C-446/21. sz. ügyben meghozott ítéletében behatóan foglalkozott az adatminimalizálás követelményével és kimondta, hogy egy közösségi hálózati platform felhasználóihoz tartozó személyes adatok célzott hirdetések céljából korlátlan ideig történő tárolását a felhasználók számára a GDPR által biztosított jogokba való aránytalan beavatkozásnak kell tekinteni.[201] A Bíróság rögzítette, hogy az ilyen adatkezelést az adatkezelő

[199] lásd Európai Unió Bírósága, 2024. október 4-i Maximilian Schrems és a Meta Platforms Ireland Ltd ítélet, C-446/21, ECLI:EU:C:2024:834, 52. pont; 2022. február 24-i Valsts ieņēmumu dienests [Személyes adatok adóügyi célból történő kezelése] ítélet, C-175/20, EU:C:2022:124, 79. pont

[200] Hinweise der DSK – Datenschutzkonformer Online-Handel mittels Gastzugang (Stand 24. März 2022); https://www.datenschutzkonferenz-online.de/media/dskb/20222604_beschluss_datenminimierung_onlinehandel.pdf; lehívás: 2024.08.25

[201] lásd Európai Unió Bírósága, 2024. október 4-i Maximilian Schrems és a Meta Platforms Ireland Ltd ítélet, C-446/21, ECLI:EU:C:2024:834, 58. pont

platform nem végezheti általános jelleggel és különbségtétel nélkül a személyes adatok gyűjtését, és tartózkodnia kell az adatkezelés céljai szempontjából nem feltétlenül szükséges adatok gyűjtésétől. (ítélet 59. pontja). A Bíróság hivatkozott továbbá az alapértelmezett adatvédelem GDPR 25. cikk (2) bekezdése szerinti követelményére, amely az adattakarékosság szempontjából a gyűjtött személyes adatok mennyiségére és az adatkezelés mértékére, valamint az adattárolás időtartamára vonatkozik. Az ilyen adatkezelés különösen széles körű a Facebook platformon, mivel az potenciálisan korlátlan adatokra vonatkozik, és jelentős hatással van a felhasználóra, akinek az online tevékenységeinek szinte egészét a Meta nyomon követi, ami a magánélet tiszteletben tartásához és a személyes adatok védelméhez való jogba való súlyos beavatkozás. Ez azonban észszerűen nem volt igazolható a célzott hirdetések lehetővé tételére irányuló célkitűzésre tekintettel. A Bíróság ezért a közösségi hálózati platform birtokában lévő személyes adatok összességének különbségtétel, időbeli és az adatok jellege szerinti korlátozás nélküli, hirdetési célokra történő felhasználását a platform felhasználói számára biztosított jogokba való aránytalan beavatkozásnak tekintette, amely ellentétes az „adattakarékosság" követelményével. (vö. ítélet 65. pontja)

2.3.6 Pontosság

A személyes adatoknak pontosnak és naprakésznek kell lenniük, és minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék. A követelményeket az adatok konkrét felhasználásának kockázataival és következményeivel összefüggésben kell vizsgálni. A pontatlan személyes adatok kockázatot jelenthetnek az érintettek jogaira és szabadságaira nézve, például, ha egy személyről téves képet alkotnak, az akár manuálisan – automatizált döntéshozatal használatával –, akár mesterséges intelligencia révén hibás alapon meghozott döntésekhez vezethet[202], amely korlátozhatja az érintett jogait és alapszabadságait, annak szólásszabadsághoz való jogát, ha például egy algoritmus jogellenesnek nyilvánítja az adott felhasználó által feltöltött tartalmat és emiatt tiltást vagy korlátozást alkalmaz. Az adatkezelés céljától függően a pontatlan adatok torzíthatják a felhasználói élményt, diszkriminációt eredményezhetnek, vagy jogellenes korlátozásokat hozhatnak létre. Az ilyen döntések nemcsak egyéni szinten, hanem társadalmi szinten is negatív hatásokat eredményezhetnek.

[202] Lásd EDPB 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről; 78. sarokpont

A 29. cikk szerinti adatvédelmi munkacsoport az automatizált döntéshozatallal és a profilalkotással kapcsolatban kibocsátott iránymutatásában kiemelte[203], hogy különös kockázatot jelent, ha az automatizált döntéshozatali vagy profilalkotási folyamat során használt adatok pontatlanok, mert minden ebből eredő döntés vagy profil hibás lesz. Döntések elavult adatok vagy a külső adatok hibás értelmezése alapján is születhetnek. A pontatlanságok alkalmatlan előrejelzésekhez vagy kijelentésekhez vezethetnek például valakinek az egészségi állapotáról, hitelképességéről vagy biztosítási kockázatáról. Az adatkezelőknek szigorú intézkedéseket kell bevezetniük annak érdekében, hogy folyamatosan ellenőrizzék és biztosítsák, hogy az újra felhasznált vagy közvetett módon szerzett adatok pontosak és naprakészek legyenek. Ez megerősíti annak fontosságát, hogy világos információt nyújtsanak a kezelt személyes adatokról, hogy az érintett kijavíthassa az esetleges pontatlanságukat, és ezáltal javíthassa az adatok minőségét.

2.3.7 Korlátozott tárolhatóság

Az adatokat csak addig szabad tárolni, amíg az eredeti célok eléréséhez szükségesek, utána törölni vagy anonimizálni kell őket. Az adatkezelőnek biztosítania kell, hogy a személyes adatok tárolása olyan formában történjen, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. Minél tovább tárolnak személyes adatokat, annál nagyobb az adatvédelmi incidensek, például adatlopás vagy adatvesztés kockázata. A korlátozott tárolhatóság elvének betartása csökkenti ezeket a kockázatokat, mivel kevesebb adat áll rendelkezésre, amelyeket potenciálisan kompromittálódhat. Rövidebb tárolási időszakokkal az online platformok minimalizálhatják a hosszú távú adatvédelmi fenyegetéseket. Az adatok hosszú távú tárolása az adatok elavulásához és pontatlanságához vezethet. A korlátozott tárolhatóság elve segít az adatok naprakészen tartásában, mivel biztosítja, hogy csak a releváns és aktuális adatok kerüljenek tárolásra.

A 29. cikk szerinti adatvédelmi munkacsoport az automatizált döntéshozatallal és a profilalkotással kapcsolatban kibocsátott iránymutatásában utalt arra[204], hogy a gépi tanulási

[203] vö. 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához; WP251rev.01, 11-12. oldal
[204] vö. 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához; WP251rev.01, 12. oldal

algoritmusokat nagy mennyiségű információ feldolgozására tervezték, és ezek segítségével adatkezelők olyan összefüggéseket tudnak felállítani, amelyek lehetővé teszik, hogy rendkívül átfogó, részletes profilokat alakítsanak ki az egyénekről. Bár a profilalkotás esetében előnyt jelenthet az adatok megtartása, mivel több adat áll az algoritmus rendelkezésére a tanuláshoz, az adatkezelőknek meg kell felelniük az adatminimalizálás elvének a személyes adatok gyűjtése során, és biztosítaniuk kell, hogy a személyes adatokat csak addig tartsák meg, amíg az szükséges és arányos a személyes adatok kezelésének céljaihoz.

A korlátozott tárolhatóság elvét érvényesítő intézkedések és garanciák kiegészítik az érintettek jogait és szabadságait, különösen a törléshez és a tiltakozáshoz való jogot. Az adatkezelő adatmegőrzésére vonatkozó intézkedéseinek ezáltal figyelembe kell vennie az érintettek jogait és szabadságait a GDPR 5. cikk (1) bekezdésének e) pontjával összhangban.

Számos adatvédelmi hatóság foglalkozott a korlátozott tárolhatóság érvényesítésével. A finn adatvédelmi hatóság, az ODPO megállapította[205], hogy egy online vásárlás fiók létrehozásához kötése ellentétes a korlátozott tárolhatóság elvével, mivel a fiók létrehozásával gyűjtött személyes adatok hosszabb ideig kerülnek tárolásra, mint ami egy egyszeri online vásárlás lebonyolításához szükséges.

2.3.8 Adatbiztonság

A GDPR egyik központi követelménye, különösen fontos a digitális platformok számára, amelyek gyakran kezelnek nagy mennyiségű és érzékeny személyes adatot. Az adatbiztonság célja, hogy megvédje az adatokat a jogosulatlan hozzáféréstől, az adatvesztéstől, az adatlopástól, és az adatok sérülésétől. Az adatbiztonság megvalósítása a platformok számára létfontosságú a felhasználói bizalom megőrzése, a jogszabályi megfelelés biztosítása és a platformok üzleti érdekeinek védelme érdekében.

Az adatbiztonság garantálása jellemzően a klasszikus triász a bizalmasság, integritás és rendelkezésre állás biztosításának mentén történik [angolul gyakran CIA-nak rövidítik a

[205] ODPO - Asiakkaaksi rekisteröitymisen edellyttäminen ja henkilötietojen säilyttäminen ostoksen tekemisen yhteydessä verkkokaupassa - TSV/26/2020 - https://www.finlex.fi/fi/viranomaiset/tsv/2024/20242163 ; lehívás: 2024.08.25

Confidentiality, Integrity és Availability szavak miatt]. A bizalmasság azt jelenti, hogy az adatok csak az arra jogosult személyek számára hozzáférhetőek, a sértetlenség biztosítja az adatok pontosságát és változatlanságát, míg a rendelkezésre állás garantálja, hogy az adatok szükség esetén elérhetők legyenek. A bizalmasságot jellemzően titkosítás és erős felhasználó azonosítás és hozzáférés menedzsment, az integritást ellenőrzőösszegek [hash-elés vagy cyclic redundancy check – CRC alkalmazása] és elektronikus aláírások, a rendelkezésre állást pedig redundancia, így különösen CDN-ek [content delivery network], rendszeres biztonsági mentések és hatékony digitális reziliencia, DDoS elleni védelem biztosítják online platformok esetében.

Az EU kiberbiztonsági stratégiájával összhangban a NIS2 Irányelvre[206] figyelemmel ez a triász online platformok esetében kiegészül az adatok hitelességével [authenticity] is. A hitelesség biztosítható digitális aláírásokkal, kétfaktoros hitelesítéssel, tanúsítvány alapú hitelesítéssel, és titkosított kommunikációs csatornák (pl. VPN, SSH) használatával, amelyek garantálják az adatok és felhasználók valódiságát.

A GDPR igen tágan és elnagyoltan szabályozza az adatbiztonsági követelményeket, amelyek több szakaszban jelennek meg: egyrészről az adatvédelmi jogszabályok által nem szabályozott „security-by-design” szoftvertervezési elv mellé kerül a beépített- és alapértelmezett adatvédelem követelménye [GDPR 25. cikke]. Az online platformok, mint adatkezelők a technológiai fejlődés, a kapcsolódó költségek és adatkezeléssel járó kockázatok figyelembevételével olyan technikai és szervezési intézkedéseket alkalmaznak, hogy biztosítsák az adatvédelmi elvek érvényesülését és az érintettek jogainak védelmét már az adatkezelési tevékenység megtervezése során is. Az EDPB 4/2019 számú iránymutatása[207] szerint a technikai és szervezési intézkedések, valamint a szükséges garanciák széles körben értelmezendők, és minden olyan módszert magukban foglalnak, amelyet az adatkezelő alkalmazhat az adatkezelés során. Ezeknek az intézkedéseknek alkalmasnak kell lenniük az adatvédelmi cél elérésére, és hatékonyan kell biztosítaniuk az adatvédelmi alapelveknek való

[206] Európai Bizottság - Irányelv az egész Unióban egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS2 irányelv); https://digital-strategy.ec.europa.eu/hu/policies/nis2-directive , lehívás: 2024.09.21

[207] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020; https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf; lehívás 2024. 09. 02

megfelelést. Az EDPB szerint az intézkedések egyaránt lehetnek fejlett technikai megoldások vagy akár alapvető személyzeti képzések is. Példák lehetnek ezen intézkedésekre az adatok álnevesítése, hozzáférés szabályozás és jogosultságkezelés, vírusírtók alkalmazása, valamint a dolgozók kibervédelmi képzése stb. Az EDPB kiemeli, hogy az alapértelmezett adatvédelem tervezése során a hatékonyság központi szerepet játszik. Az adatkezelőknek olyan intézkedéseket kell tehát megvalósítaniuk, amelyek hatékonyan védik az adatvédelmi alapelvek teljesülését és biztosítják az érintettek jogait. Az alkalmazott intézkedéseknek el kell érniük a kívánt eredményeket, és az adatkezelőknek igazolniuk kell tudniuk, hogy az adatvédelmi alapelveket betartották. A GDPR 25. cikke tehát nem ír elő konkrét technikai és szervezési intézkedéseket, hanem azokat az adott adatkezelési folyamatra kell szabni, figyelembe véve a kapcsolódó – érintettekre vonatkozó – adatvédelmi jogi és adatbiztonsági kockázatokat. Az adatkezelők KPI-kkel (kulcsfontosságú teljesítménymutatókkal) mérhetik az adott intézkedések hatékonyságát, például az incidensek téves észlelésére vonatkozó arányszámmal vagy az érintetti panaszok csökkenése alapján. Ilyen, a beépített és alapértelmezett adatvédelemre vonatkozó tervezési és működtetési elveknek szükséges teljesülniük például a DSA 25. cikkével [Online interfész tervezése és kialakítása] összefüggésben is.

A GDPR 32. cikke szerint az online platformok, mint adatkezelő, vagy bizonyos esetekben adatfeldolgozó a tudomány és technológia fejlődését, költségeket, az adatkezelés jellemzőit és a természetes személyek jogaira jelentett kockázatokat figyelembe véve megfelelő technikai és szervezési intézkedésekkel biztosítják az adatok biztonságát. Ez magában foglalja a titkosítást, az adatok bizalmasságának, integritásának, rendelkezésre állásának fenntartását, incidensek esetén az adatok helyreállítását, valamint a biztonsági intézkedések rendszeres tesztelését. Az adatkezelési kockázatokat különösen a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan hozzáférése esetén kell figyelembe venni.

Itt érdemes röviden megjegyezni, hogy ezen alapértelmezett és beépített adatvédelmi, valamint adatbiztonsági követelményeknek való megfelelést segíti elő az ún. Privacy Enhancing Technologies [PET] alkalmazása. A PET-ek összefoglalóan azon technológiák, eljárások, megoldások megnevezése, amelyek célja, hogy megvédje az adatokat a jogosulatlan hozzáféréstől, kezeléstől, illetve megosztástól, és a [szenzitív] adatokat így biztonságosan lehessen szervezetek, személyek között kezelni, megosztani.

Az ENSZ kapcsolódó útmutatója[208] alapján a Privacy-Enhancing Technologies (PET-ek) két fő kategóriáját különbözteti meg: bemeneti védelmet (input privacy) és kimeneti védelmet (output privacy) biztosító megoldások. Az első kategória, a bemeneti védelem célja, hogy lehetővé tegye az adatokon közös műveletek végzését anélkül, hogy a beküldőn kívül más szereplők hozzáférhessenek ezekhez az adatokhoz. Az útmutató három fő input privacy megközelítést említ. Az első a megbízható fél közbeiktatása, amely jogszabályi vagy szerződéses úton történik. Ebben az esetben a műveleteket végrehajtani kívánó felek kiválasztanak egy közös megbízható harmadik felet, ahol az adatkezelés megvalósul, vagy aki az adatok hitelességét igazolja. A második megközelítés az elosztott tanulás, amely lehetővé teszi több szereplő számára, hogy mesterséges intelligenciához kapcsolódó tanulási algoritmusokat képezzenek anélkül, hogy egymás adatait megismernék. Az elosztott tanulásnak két típusa fordul elő gyakran a gyakorlatban: az összevont tanulás és a szétosztott tanulás. Az összevont tanulás esetében az algoritmus egy lokális másolata megtalálható minden tanulási rendszerben részt vevő eszközön, és helyben történik az algoritmus tanítása. A központi szereplő csak koordinálja és összehangolja a folyamatot, majd a legnagyobb tudással rendelkező tanuló algoritmust terjeszti a rendszer többi szereplője között. Gyakorlati megvalósítások például a Google és az Apple mobiltelefonjain elérhető szövegpredikciós rendszerek, illetve csalásfelderítési megoldások, vagy a képfelismerésen alapuló diagnosztikai eszközök az egészségügyben.

Az elosztott tanulás másik típusa, a szétosztott tanulás, az algoritmust több részre osztja, és ezeket a részeket a tanulási rendszerben részt vevő eszközökre helyezi. Az eszközök ezután helyben végzik a tanítást, és a végén mindegyik rendelkezni fog a teljes algoritmus egy lokális másolatával. Az ilyen típusú megközelítéseknél figyelembe kell venni az informatikai hálózati és számítási kapacitások elérhetőségét, mind a kliensoldalon, mind a szerveroldalon.

A harmadik input privacy megközelítés a Zero Knowledge Proofs (ZK), amely lehetővé teszi, hogy egy meghatározott kérdést igazoljanak anélkül, hogy a szükséges adatokat ténylegesen

[208] UN Guide on Privacy-Enhancing Technologies for Official Statistics; https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf; Bereczki Tamás - Az ENSZ Privacy Enhancing Technologies [PET] útmutatója, https://www.linkedin.com/pulse/az-ensz-privacy-enhancing-technologies-pet-%C3%BAtmutat%C3%B3ja-tamas-bereczki/?trackingId=yXWzcHSsSgaPjqiODlxllA%3D%3D; lehívás 2024. 09. 02

meg kellene osztani a hitelesítő féllel. A ZK megoldások leginkább autentikációs rendszerekben, illetve kriptovalutákat kezelő rendszerekben használatosak.

Egy további megközelítés, amely az input privacy biztosítására szolgál, tisztán titkosítási alapú, például a biztonságos többszereplős számítás (sMPC) és a homomorfikus titkosítás (HE). Az sMPC egy kriptográfiai módszer, amely lehetővé teszi, hogy a felek különféle műveleteket végezzenek egymás adatai felett úgy, hogy csak a műveletek eredményét ismerik meg, magukat az adatokat nem. A sMPC egyik fajtája a széles körben alkalmazott összevont tanulás. Az útmutató két alkalmazott sMPC eljárást mutat be: a circuit garbling-et, amelyet általában két fél között alkalmaznak, és a lineáris titokmegosztást (LSS), amelyben az adatokat véletlenszerű szeletekre osztják, és ezek összessége adja vissza az eredeti adathalmazt. Az sMPC módszerek jelentős számítási kapacitást igényelnek, és alkalmazásuk során figyelembe kell venni a hálózati látencia mértékét. A homomorfikus titkosítás lehetővé teszi, hogy titkosított adatokon közvetlenül lehessen műveleteket végezni, anélkül, hogy azok titkosítását vissza kellene fejteni. Ez különösen felhőszolgáltatásokban hasznos, ahol titkosítottan tárolják az adatokat. Azonban ezek a megoldások is jelentős számítási erőforrást igényelnek, és alkalmazásuk során előzetes technikai kontrollok szükségesek. A homomorfikus titkosítás egyik gyakorlati megvalósítása a Microsoft SEAL függvénykönyvtára.

Egy másik megközelítés, amely input privacy-t biztosít, a megbízható végrehajtási környezeteken alapul. Itt az adatok kezelésének biztonságát a hardveres vagy felhőszolgáltatói megoldások garantálják. A biztonságos végrehajtási környezetek (Trusted Execution Environment, TEE) célja, hogy az adatkezelés során biztosítsák az adatok bizalmasságát és a szoftverek futtatásának biztonságát.

A kimeneti védelem (output privacy) megoldások célja az, hogy az adatkezelés eredményeként keletkező kimeneti adatok ne legyenek visszafejthetők, azaz ne lehessen azokból következtetni az eredeti, bemeneti adatokra, és ne lehessen azokat visszaazonosítani. Az output privacy egyik megközelítése a differential privacy, amely egy sor technikai megoldást jelent, amelyek korlátozzák az eredményadatokból visszanyerhető információkat az eredeti adatokra vonatkozóan. Ezen megközelítés során az adatokhoz zajt adnak hozzá, így azok pontossága csökken, de védettebbé válnak a visszafejtési próbálkozásokkal szemben. A differential privacy egyik gyakorlati alkalmazása a Google Chrome és az Apple iOS rendszereiben található

felhasználói statisztikagyűjtés, ahol a felhasználók adatai anonimizálva kerülnek feldolgozásra. Ezen módszer alkalmazása esetén azonban figyelembe kell venni, hogy a kimeneti adatok pontossága csökken, ezért mindig mérlegelni kell a bizalmassági szintet és a szükséges pontosságot az adott alkalmazás során.

A kimeneti védelem egy másik megközelítése a szintetikus adatok használata, amelyek az eredeti adatok alapján véletlenszerűen generált adathalmazokat jelentenek. Ezek az adatok ugyanazokat a mintázatokat követik, mint az eredeti adatok, de maguk az adatok fiktívek, így megvédik az eredeti adathalmaz bizalmasságát. A szintetikus adatok különösen hasznosak lehetnek olyan területeken, mint például a gépi tanulási algoritmusok képzése vagy a tesztelési környezetekben történő alkalmazás. Azonban a szintetikus adatok alkalmazása során figyelembe kell venni azok pontosságát és használhatóságát a valós adatokkal való összehasonlításban.

A fentebb körülírt technikai intézkedések alkalmazása [pl. multifaktoros hitelesítés vagy hálózati monitoring eszközök üzemeltetése] önmagukban is adatkezelésnek minősülnek, amelyekkel összefüggésben az online platformnak szintén biztosítania kell az adatvédelmi jogszabályi kötelezettségeknek való megfelelést[209].

Szintén a beépített- és alapértelmezett adatvédelem gyakorlati megvalósulását támogatja az adatvédelmi hatásvizsgálatok végzése és dokumentálása. Az adatvédelmi hatásvizsgálat gyakorlatilag a [tervezett] adatkezelési tevékenységgel érintett egyének jogaira és szabadságaira fókuszáló adatvédelmi jogi és adatbiztonsági kockázatelemzés. Mint minden kockázatelemzésnek az adatvédelmi hatásvizsgálatok sajátja, hogy megfelelő kockázatelemzési módszertan mentén készüljön, amely biztosítja az egyes kockázatelemzések megismételhetőségét [ellenőrizhetőségét], mérhetőségét [pl. a fentebb már hivatkozott kockázati mutatószámokkal, Key Risk Indicators – KRI] és összehasonlíthatóságát az azonos módszertan szerint készült elemzésekkel. A GDPR 34. cikk (4) bekezdése minden tagállami adatvédelmi hatóság számára előírja, hogy az egyes, kötelezően adatvédelmi hatásvizsgálat alá eső adatkezelési tevékenységekről tegyenek közzé egy ún. „fekete listát”. A magyar

[209] CNIL - #Authentification multifacteur. 28 mars 2024. [Clôturée] Authentification multifacteur : consultation publique de la CNIL sur un projet de recommandation; https://www.cnil.fr/fr/cloturee-authentification-multifacteur-consultation-publique-de-la-cnil-sur-un-projet-de, lehívás: 2024.09.11

hatóságnak, a Nemzeti Adatvédelmi és Információszabadság Hatóságnak (NAIH) feketelistája[210] szerint az online platformokat érintően jellemzően pontozás (5. pont), harmadik személytől gyűjtött adatok további felhasználása (8. pont), profilozás (10. pont), csalás elleni fellépés (11. pont), joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal (13. pont), kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos, nagy számban kezelt adatok eredeti céltól eltérő kezelése: pl. gyermekek, fogyatékkal élő személyek esetében (19. pont), gyermekek személyes adatainak kezelése profilozás, automatikus döntéshozatal, vagy marketing céljából, vagy közvetlenül részükre kínált, információs társadalommal összefüggő szolgáltatások ajánlása vonatkozásában (20. pont), illetve ha az adatkezelés célja a különböző forrásokból származó adatok összevonása, egymással való megfeleltetése vagy összehasonlítása (pl. célzott reklámok vagy tartalomszolgáltatás miatt – 24. pont) lehet adatvédelmi hatásvizsgálati kötelezettsége. Ezek tehát azok, a jogalkotó és a felügyeleti hatóság által ab ovo magas kockázatúnak tekintett adatkezelési tevékenységek, amelyek esetében az online platformnak kötelezően csökkentenie szükséges az érintettek jogaira és szabadságaira vonatkozó kockázati hatásokat és megfelelő technikai és szervezési védelmi intézkedéseket kell implementálnia.

A fenti adatbiztonsági kötelezettségeket kiegészíti a NIS2 Irányelv magyarországi átültetése, a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény [Kibertantv.] 19 – 27. §§-i, amelyek az online-piactér szolgáltatókra, a keresőszolgáltatókra, valamint a közösségi média szolgáltatási platform szolgáltatókra ró többek között kiberbiztonsági kötelezettségeket. A Kibertantv. egyik végrehajtási rendelete, a 7/2024 (VI. 24.) MK Rendelet és különösen annak 1-3. sz. mellékletei tartalmazzák azon részletszabályokat és követelményeket, amelyeket a fentiek szerint minősülő online platformnak teljesítenie kell. Ezzel kapcsolatban megjegyzendő, hogy bár az adatvédelmi jogszabályok nem írnak elő konkrét technikai, technológiai intézkedések alkalmazását, csupán általánosságban utalnak a technika mindenkori legfejlettebb állására, addig a vonatkozó nemzeti kiberbiztonsági jogszabályok konkrét védelmi intézkedések alkalmazását és meglétét, és ezen keresztül gyakorlatilag kötelező adatkezelést előírva az érintett platformoknak. Látható tehát, hogy itt alapvetően egymással konkuráló adatvédelmi és kiberbiztonsági jogszabályi kötelezettségek terhelik ezen platformszolgáltatókat.

[210] NAIH Hatásvizsgálati lista GDPR 35. cikk (4) bekezdés - https://naih.hu/hatasvizsgalati-lista; lehívás 2024. 09. 02

2.3.9 Elszámoltathatóság

Az adatkezelők elszámoltathatósága központi szerepet játszik az adatvédelmi jogszabályok alkalmazásában. A GDPR 5. cikk (2) bekezdése alapján elszámoltathatóság elve megköveteli, hogy az adatkezelők felelősek az adatvédelmi alapelvek betartásáért, egyben képesnek is kell lenniük arra, hogy ezt megfelelően igazolják. Az elszámoltathatóságra figyelemmel több követelmény is felmerül, amelyeket az online platformoknak teljesíteniük kell a mindennapi gyakorlatban a személyes adatok kezelése során és ezen követelmény érvényesítése lehetővé teszi azt, hogy az adatvédelmi jogi követelményeket valós adatvédelmi intézkedésekké alakítsák. Annak érdekében, hogy az adatvédelem a gyakorlatban is megvalósuljon, az elszámoltathatóság alapú mechanizmusok bevezetése szükséges ahhoz, hogy az adatkezelők gyakorlati megoldásokat alkalmazzanak a hatékony adatvédelem és megfelelő adatvédelmi irányítás, azaz a „good governance" biztosítása érdekében. A 29. cikk szerinti adatvédelmi munkacsoport az elszámoltathatóságról szóló 3/2010. sz. véleményében[211] az elszámoltathatóság, mint alapelv és ezzel párhuzamosan a kockázat alapú megközelítés adatvédelmi követelményként való megjelenítése mellett tört lándzsát.

Az elszámoltathatóság alapelvének azért van kiemelet jelentősége online platformok esetében, mert ezen szereplők üzleti modelljéhez a személyes adatok tömeges kezelése tartozik hozzá, a technológiai fejlődéssel folyamatosan növekedik a felhasználóik száma, a felhasználók egyre fontosabb értéket tulajdonítanak a személyes adatoknak, illetve az esetleges adatvédelmi incidensek is komolyabb következménnyel járnak az érintettek magánszférájára és a jogaikra, ami növeli a működésük kockázatait.

Az elszámoltathatóságra figyelemmel kiemelt jelentősége van, hogy a platformok adatvédelmi gyakorlata szilárd alapokra épüljön, amely nemcsak a jogi megfelelőséget biztosítja, hanem az adatkezelési folyamatok hatékonyságát és az érintettek jogainak védelmét is előmozdítja. Ennek elengedhetetlen feltétele az *adatvédelmi irányítás* keretében *az adatvédelmi keretrendszer irányításáért felelős személy kijelölése*[212], mivel a jogszabályoknak megfelelő

[211] 3/2010. sz. vélemény az elszámoltathatóságról; lásd https://www.dataprivacy.hu/?p=67, lehívás: 2024.09.09
[212] Lothar Determann's Field Gudie to Data Privacy Law – International Privacy Compliance – Fifth Edition – Elgar – Starting a Privacy Compliance Program; Taking Charge 1.02, p. 1.; Appointing a Privacy Officer; 1.09 pp. 5.-6.

adatkezelés folyamatos ellenőrzést és nyomon követést igényel. Az ilyen személy közreműködése és a hozzá tartozó jelentési csatornák szervezeten belüli kialakítása biztosítja, hogy a szervezet koordináltan működjön és megfeleljen a GDPR előírásainak, emellett átlátható és elszámoltatható működést biztosít.

A megfelelő és karbantartott *szabályzati keretrendszer*[213] megléte szintén kulcsfontosságú az elszámoltathatóság szempontjából, melyet a GDPR 24. cikk (1)-(2) bekezdése is rögzít. Ennek értelmében az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével *megfelelő technikai és szervezési intézkedéseket* hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik. Ha az az adatkezelési tevékenység vonatkozásában arányos, ezen intézkedések részeként az adatkezelő megfelelő *belső adatvédelmi szabályokat is alkalmaz*. A szervezet méretétől és kockázataitól függően belső adatvédelmi szabályzatok, információbiztonsági szabályzatok és az érintettek jogainak gyakorlásával kapcsolatos eljárásrendek kialakítása, kiszervezések és nemzetközi adattovábbítások szabályozásának egységes keretrendszerbe foglalása biztosítja, hogy az adatkezelési tevékenységek világosan szabályozottak és nyomon követhetők legyenek. Az adatmegőrzés szabályozása például az adatok védelmének egyik alapvető eleme, míg a hatásvizsgálatok és a beépített és alapértelmezett adatvédelem követelményének érvényesítése hozzájárulnak a kockázatok minimalizálásához és az adatvédelmi megfelelés biztosításához. Az adatvédelmi incidensek kezelési folyamatának világos szabályozása pedig elengedhetetlen ahhoz, hogy a szervezet gyorsan és hatékonyan reagáljon egy esetleges adatvédelmi incidensre, minimalizálva ezzel a lehetséges adatbiztonság megsértéséből eredő károkat. Az elszámoltathatóság követelménye biztosítja azt a gyakorlatban, hogy ezek a szabályzatok és a szabályzati keretrendszer nem csupán írott dokumentumok (*Law-in-Books*), hanem a gyakorlatban ténylegesen is érvényesülő, hatékony követelmények legyenek (*Law-in-Action*).

Az *adatvédelmi tevékenységek nyilvántartása és megfelelő adatvédelmi dokumentáció vezetése*[214] nélkülözhetetlen az adatkezelési tevékenységek átláthatósága és a hatóságok felé

[213] vö. Executive Editor: Russell R. Densmore - Privacy Program Management - Tools for Managing Privacy Within Your Organization - 2019 by the International Association of Privacy Professionals (IAPP); pp. 76-77.
[214] Lothar Determann's Field Gudie to Data Privacy Law – Drafting Documenation; p. 101.

történő elszámoltathatóság érdekében. Az adatkezelési tevékenységek megfelelő nyilvántartása lehetővé teszi, hogy a szervezet folyamatosan nyomon kövesse az adatkezeléseit, a jogszabályoknak való megfelelést, és időben azonosítani tudja az esetleges kockázatokat és ezeket megfelelő intézkedések útján tudja kezelni.

Az *adatvédelmi tisztviselő* (DPO), akár önkéntesen, akár kötelező a kinevezése, központi szerepet játszik a GDPR szabályozásában, különösen az adatvédelmi hatásvizsgálatok felügyelete és a szervezeti adatvédelmi megfelelés felügyelete terén. A DPO összekötő szerepet játszik a felügyeleti hatóságokkal, amely kulcsfontosságú a szervezet átlátható és jogszerű működése szempontjából. Emellett a DPO koordinálja az adatvédelmi incidensek kezelését és bejelentését, ezáltal csökkentve az esetleges jogi vagy anyagi következmények kockázatát.

A *tréningek és tudatossági programok biztosítása* szintén elengedhetetlenek a szervezet adatvédelmi megfelelőségének biztosításához, mivel megerősítik a szervezet adatvédelmi gyakorlatait.[215] A rendszeres és kötelező adatvédelmi tréningek hozzájárulnak ahhoz, hogy minden alkalmazott tisztában legyen az adatvédelmi szabályokkal és a megfelelő eljárásokkal. A specializált tréningek egyes területekre (pl. információbiztonság, marketing) biztosítják, hogy a különböző szakterületek sajátos adatkezelési kihívásai megfelelő figyelmet kapjanak.

Az elszámoltathatóság és az adatvédelmi megfelelés körébe tartozik a *napra készen tartással* kapcsolatos intézkedések[216], tehát az, hogy a szervezet reagál a változásokra, adatvédelmi politikáját, szabályzati keretrendszerét, dokumentációját, eljárásait rendszeresen felülvizsgálja, azonosítsák az esetleges adatvédelmi hiányosságokat, és szükség esetén megfelelő korrekciós intézkedéseket hozhassanak. A folyamatos megfelelés biztosítása érdekében a szervezetnek nyomon kell követnie a belső és külső változásokat, beleértve a jogi fejleményeket, hatósági iránymutatásokat és új, vagy jelentős módosításokon áteső adatkezelési folyamatokat. Az adatvédelmi politika relevanciája és naprakészsége érdekében a változásokra való azonnali reagálás szükséges, időszakos vagy ad-hoc felülvizsgálatok formájában. Emellett fontos értesíteni az érdekelt feleket az adatvédelmi politikák változásairól, és külső felülvizsgálat vagy tanúsítás bevonása is hozzájárulhat a megfelelés biztosításához.

[215] vö. Russell R. Densmore im pp. 159-160.
[216] Lothar Determann's Field Guide to Data Privacy Law – Maintaining and Auditing Compliance Programs; im p. 105.

Az *adatvédelmi megfelelés mérése* és *megfelelő mérőszámok kiválasztása* elengedhetetlenek az elszámoltathatóság biztosításában, mivel lehetővé teszik az adatvédelmi teljesítmény folyamatos nyomon követését és értékelését[217]. A teljesítménymérés célja az adatvédelmi folyamatok végrehajtásának, hatékonyságának és eredményességének kvantitatív értékelése. A mérőszámok és metrikák olyan eszközök, amelyek az adatok gyűjtése, elemzése és jelentése révén támogatják a döntéshozatalt, és segítenek a megfelelési célok elérésében. Ahhoz, hogy a mérőszámok hasznosak legyenek, mérhetőnek, relevánsnak és világosan definiáltnak kell lenniük, és képeseknek kell lenniük jelezni a haladást, valamint válaszolni a konkrét adatvédelmi kérdésekre[218]. Ez a folyamat biztosítja, hogy a szervezet időben tudjon reagálni az esetleges adatvédelmi hiányosságokra. A mérőszámok tulajdonosa, vagyis az a személy, aki felelős a mérőszámok kezeléséért, gondoskodik arról, hogy a mérőszámok a teljes életciklusuk során megfelelően működjenek, ezáltal elősegítve az adatvédelmi megfelelés fenntartását és javítását.

Az *adatvédelmi compliance, a megfelelési tevékenységek* kritikus szerepet játszanak a digitális platformok elszámoltathatósági követelményeinek teljesítésében. Az adatvédelmi programok célja, hogy biztosítsák a jogszabályok és előírások betartását, ezáltal megelőzzék és felderítsék a megfelelési kötelezettségek megsértését. A vállalati adatvédelmi compliance rendszerek segítik a vállalatokat abban, hogy elkerüljék a szabályszegéseket, ezáltal minimalizálják a kockázatokat és javítsák a szervezeti működés átláthatóságát. A compliance menedzsment lényege, hogy csökkentse a szabálytalan működés kockázatát[219], ami különösen fontos a digitális platformok esetében, ahol a személyes adatok széles körű és folyamatos kezelése történik. A megfelelési kockázatok azok a bizonytalanságok, amelyek a szervezet megfelelési céljait érinthetik, és amelyek bekövetkezésének valószínűsége, valamint a következmények súlyossága határozza meg a megfelelési szintet. A kockázatkezelés célja ezeknek a kockázatoknak az azonosítása, elemzése, értékelése és kezelése, ami a digitális platformok esetében különösen fontos, mivel ezen platformok nagymértékben támaszkodnak a személyes adatok feldolgozására. A megelőzés az üzleti területek támogatásán, valamint a szabályozás és ellenőrzési funkciók fejlesztésén keresztül történik. A felderítés, mint audit és incidenskezelés,

[217] vö. Russell R. Densmore im pp. 76-77.
[218] Russell R. Densmore; p. 78.
[219] Benedek, Petra (2014) A vállalati compliance értékelése. Vezetéstudomány - Budapest Management Review, 45 (7-8). pp. 29-30. DOI 10.14267/VEZTUD.2014.07.03

biztosítja, hogy a szervezetek rendszeresen ellenőrizzék és összevessék gyakorlataikat a jogi szabályozásokkal, ami szintén hozzájárul az elszámoltathatóság elvének betartásához. A helyesbítő tevékenységek, például a szabályozások módosítása, lehetőséget biztosítanak a megfelelés javítására. A jelentéskészítés pedig a szervezeti döntéshozók felé irányul, amely alapján mérhető és nyomon követhető a rendszer hatékonysága.[220]

Az adatvédelmi compliance részeként az *adatvédelmi programmenedzsment* strukturált megközelítést biztosít az adatvédelem irányításában, és segít egy megbízható és hatékony adatvédelmi infrastruktúra kialakításában. Ez magában foglalja a szerepek és felelősségi körök meghatározását, a személyes adatok kezelésére vonatkozó irányelvek kidolgozását, valamint azok operacionalizálását szolgáló folyamatok kialakítását, amelyek biztosítják, hogy a digitális platformok megfeleljenek a jogszabályi előírásoknak, és hatékonyan tudják kezelni az adatvédelmi kockázataikat. Az adatvédelmi elszámoltathatóság és a kockázat alapú megközelítés gyakorlati megvalósítása biztosítja, hogy egy szervezet hatékonyan és jogszerűen kezelje a személyes adatokat. Az átláthatóság, a megfelelő irányítási struktúrák, a belső szabályozási keretrendszer, valamint a folyamatos képzés és felügyelet révén a szervezet képes lesz minimalizálni az adatvédelmi kockázatokat, és biztosítani a hatékony adatvédelmi gyakorlatot.

A DSA új követelményei befolyásolják az online platformok compliance menedzsment tevékenységeit, és új, illetve szélesebb elszámoltathatósági kötelezettségeket vezetnek be platformok számára, melyek közvetlenül kihatnak a platformok személyes adatok kezelésével kapcsolatos tevékenységeikre.

[220] Benedek, Petra - Compliance menedzsment a pénzügyi szolgáltatásokban; Munkaügyi Szemle 62. évf. (2019) 4. szám

3. PLATFORMOK SPECIFIKUS ADATVÉDELMI KÖTELEZETTSÉGEI A DSA HATÁLYA ALATT

A jelen fejezetben részletesen bemutatásra kerülnek a GDPR és a DSA közötti átfedések. Az átfedések elemzése során megvizsgálásra kerül, hogyan kapcsolódnak össze a GDPR adatvédelmi előírásai a DSA szabályaival, különös tekintettel az online közvetítők adatvédelmi kötelezettségeire. Továbbá, feltárásra kerül, hogy a DSA milyen kereteket biztosít az ezen szolgáltatók számára annak érdekében, hogy betartsák a GDPR által előírt adatvédelmi követelményeket. Az előző fejezetben már ismertetett adatvédelmi kötelezettségek alapján részletezésre kerül, hogy a DSA milyen szabályozási eszközökkel és követelményekkel segíti elő ezen kötelezettségek teljesítését, biztosítva az online szolgáltatások jogszerű működését.

3.1 A DSA hatálya és az adatvédelmi jogszabályokkal való kapcsolata

A DSA javaslatról szóló Európai Adatvédelmi Biztosi vélemény szerint az adatvédelemhez való jog nem abszolút jog, és a beavatkozások igazolhatók, feltéve, hogy az ilyen intézkedések szükségesek és arányosak. Továbbá a vélemény is elismeri, hogy 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 online biztonság és az online platformok elszámoltathatóságának biztosítására szolgáló mechanizmusok tovább erősíthetik az alapvető jogok hatékony élvezetét.[221]

A DSA hatályát a 2. cikk (1) bekezdése határozza meg és a „piac helyének elvét” követi, mivel a rendelet az olyan igénybe vevők részére kínált közvetítő szolgáltatásokra vonatkozik, amelyeknek, illetve akiknek a letelepedési helye az Unióban található vagy akik, illetve amelyek az Unióban találhatók, függetlenül az említett közvetítő szolgáltatást biztosító szolgáltatók letelepedési helyétől. Itt rögzítendő, hogy hasonló szabályozási megközelítés szerepel a GDPR 3. cikk (2) bekezdésében, ami az Unióban tartózkodó érintettek személyes

[221] vö. EDPS vélemény 15. sarokpontja

adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére vonatkozik, ha az adatkezelési tevékenységek: a) áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy b) az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve hogy az Unió területén belül tanúsított viselkedésükről van szó. A DSA hatályával kapcsolatos szabályozás alapjául a GDPR 3. cikk (2) bekezdése szolgált.[222]

A DSA hatályát szabályozó 2. cikk (1) bekezdéséhez kapcsolódik a 3. cikk d) és e) pontja, ami a DSA alkalmazását területi alapon határozza meg, hogy mi minősül „*szolgáltatások nyújtásának az Unióban*", illetőleg „*az Unióval fennálló érdemi kapcsolatnak*" e szolgáltatások nyújtása tekintetében. A DSA 7. preambulumbekezdése utal arra, hogy ezek a szabályok a közvetítő szolgáltatókra azok letelepedési helyétől vagy földrajzi helyétől függetlenül alkalmazandók, amennyiben szolgáltatásokat kínálnak az Unióban, ahogy azt az Unióval fennálló érdemi kapcsolat alátámasztja, ami gyakorlatilag kizárja azt, hogy EU-n kívüli, itt nem letelepedett szolgáltatók megkerüljék az európai jogi követelményeket a rendeletben meghatározott szabályok hatékonyságának, illetve a belső piaci egyenlő versenyfeltételek biztosítása érdekében.[223] Ilyen, az Unióval fennálló érdemi kapcsolatnak tekintendő, ha a szolgáltató letelepedési hellyel rendelkezik az Unióban, illetve ilyen letelepedési hely hiányában egy vagy több tagállamban a lakosságszámhoz viszonyítva jelentős számú igénybe vevője van a szolgáltatásainak, vagy ha a tevékenysége egy vagy több tagállam felé irányul[224]. A „szolgáltatások nyújtása az Unióban" fogalommeghatározása szerint elegendő annak lehetővé tétele, hogy természetes vagy jogi személyek legalább egyetlen tagállamban igénybe vegyék az olyan közvetítő szolgáltató szolgáltatásait, amely érdemi kapcsolatban van az Unióval, azaz nem szükséges az, hogy a szolgálatást ténylegesen is igénybe vegyék, mert elegendő ennek az igénybevétel lehetőségének biztosítása. Unióval fennálló érdemi kapcsolatnak tekintendő, ha a szolgáltató letelepedési hellyel rendelkezik az Unióban, illetve ilyen letelepedési hely hiányában egy vagy több tagállamban a lakosságszámhoz viszonyítva jelentős számú igénybe vevője van a szolgáltatásainak, vagy ha a tevékenysége egy vagy több tagállam felé irányul.[225] Az egy vagy több tagállam felé irányuló tevékenység valamennyi

[222] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 3. Rn 2; p. 10.
[223] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 3. Rn 33; p. 27.
[224] vö. DSA (8) preambulumbekezdése
[225] vö DSA 3. cikk (e) pont

releváns körülmény alapján állapítható meg, beleértve az olyan tényezőket is, mint a használt nyelv vagy az általában használt pénznem az adott tagállamban, vagy a termékek vagy szolgáltatások megrendelésének lehetősége vagy egy releváns felső szintű domén használata. A valamely tagállam felé irányuló tevékenység fennállása levezethető abból is, ha rendelkezésre áll egy alkalmazás a szolgáltatónak az adott tagállamra szabott alkalmazás-áruházában, ha helyi hirdetéseket vagy a tagállamban használt valamely nyelven hirdetéseket közölnek, vagy ügyfélkapcsolatok kezeléséből, például az adott tagállamban általánosan használt valamely nyelven történő ügyfélszolgálat biztosításából. A szolgáltatás puszta technikai elérhetősége önmagában azonban nem minősül az Unióval fennálló érdemi kapcsolatnak.[226] A DSA hatálya tehát a GDPR hatályához hasonlóan rendkívül tág, mivel a szabályozás célja az ún. „Brüsszel-hatás"[227] elérése volt, hogy világszinten ne lehessen megkerülni ezeket a szabályokat és ezáltal az Európai Unió gazdasági erejénél fogva egy globális szabályozási standardod képezzenek. Végül a DSA 2. cikk (2) bekezdése rögzíti azt, 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 DSA és a GDPR, valamint az e-Privacy irányelv közötti kapcsolatot elsősorban *kiegészítő jelleg* jellemzi. Ez azt jelenti, hogy a DSA szabályozása nem rontja le az uniós jogi aktusokat, amelyek a személyes adatok védelmét célozzák, hanem azokat kiegészíti és azokkal összhangban működik. A DSA 10. preambulumbekezdésében világosan kimondja[228], hogy a rendelet nem érinti az EU személyes adatok védelméről szóló jogát, a GDPR adatvédelmi szabályozását. Ez azt jelenti, hogy a DSA nem változtatja meg a GDPR által meghatározott adatvédelmi normákat és szabályokat. A GDPR továbbra is az alapvető és központi szabályozás az uniós adatvédelem terén, és minden, a személyes adatok védelmére vonatkozó kérdést a GDPR rendelkezései szerint kell kezelni. Emellett a preambulumbekezdés említi az ePrivacy

[226] vö. DSA (8) preambulumbekezdését; Müller-Terpitz / Köhler- DSA Kommentar – Artikel 3. Rn 37-38; p. 28.
[227] Anu Bradford, The Brussels Effect: How the European Union Rules the World, Columbia Law School; https://doi.org/10.1093/oso/9780190088583.001.0001; lehívás: 2024.09.11
[228] A DSA (10) preambulumbekezdés szerint „*ez a rendelet nem érinti a személyes adatok védelméről szóló uniós jogot, különösen az (EU) 2016/679 európai parlamenti és tanácsi rendeletet*", továbbá „*A magánszemélyeknek a személyes adatok kezelése tekintetében történő védelmét kizárólag az erről a témáról szóló uniós jog szabályai szabályozzák, mindenekelőtt az (EU) 2016/679 rendelet és a 2002/58/EK irányelv*." „*Ugyanakkor, amennyiben az uniós jogi aktusok az e rendeletben meghatározott célokkal azonos célokat követnek, akkor az ebben a rendeletben meghatározott szabályok alkalmazandók azokra a kérdésekre, amelyek nem vagy nem teljes mértékben képezik az említett egyéb jogi aktusok tárgyát, továbbá azokra a kérdésekre, amelyek vonatkozásában ezek az említett egyéb jogi aktusok lehetővé teszik a tagállamok számára egyes intézkedések nemzeti szintű elfogadását."*

irányelvet is. Ez az irányelv, mint fentebb bemutattuk, specifikus adatvédelmi szabályokat határoz meg az elektronikus hírközlési szektor számára. Az e-Privacy irányelv kiegészíti a GDPR-t azáltal, hogy külön szabályokat határoz meg a személyes adatok kezelése tekintetében az elektronikus kommunikáció során, biztosítva ezzel a magánszemélyek adatainak védelmét.

A DSA ugyanakkor rögzíti, hogy ha az uniós jogi aktusok azonos célokat követnek, mint amiket a DSA meghatároz, akkor a DSA szabályai alkalmazandók olyan kérdésekben, amelyeket az egyéb uniós jogi aktusok nem, vagy nem teljes mértékben szabályoznak. Ez azt jelenti, hogy ha van átfedés a célok között, de az adott kérdés nem teljesen rendezett a GDPR vagy az e-Privacy irányelv által, akkor a DSA rendelkezései lépnek érvénybe. Ezen túlmenően, a DSA alkalmazható azokra a területekre is, ahol a GDPR vagy az e-Privacy irányelv lehetőséget biztosít a tagállamoknak arra, hogy nemzeti szinten külön intézkedéseket fogadjanak el. Így a DSA rugalmas keretet biztosít a tagállamok számára, hogy saját nemzeti szabályozásukat a közös uniós célokkal összhangban alakítsák ki.[229]

A fentiek 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.

3.2 Specifikus adatvédelmi kötelezettségek a DSA hatálya alatt

A DSA, figyelemmel annak adatvédelmi szabályozást kiegészítő jellegét, 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[230], mely szerint a DSA rendelet nem érinti a személyes adatok védelméről szóló uniós jogot; profilalkotásra és célzott hirdetésekre vonatkozó korlátozásokra[231]; kiskorúak védelmére vonatkozó rendelkezésekre[232]; adatokhoz való hozzáférés és kutatás[233]; kockázatértékelés és átláthatósági követelményekre online óriásplatformot üzemeltető szolgáltatóknál[234];

[229] vö. DSA (10) preambulumbekezdés második bekezdése
[230] DSA (10) preambulumbekezdés, illetve a DSA 2. cikk (4) g) pontja
[231] DSA (68)-(69) preambulumbekezdés és DSA 26. cikk (3) bekezdése
[232] (71) preambulumbekezdés és DSA 28. cikk (1)–(4) bekezdései
[233] (97) preambulumbekezdés és DSA 40. cikk
[234] DSA (81) preambulumbekezdés; (94) preambulumbekezdés; DSA 34. cikk (1) bekezdése

magatartási kódexek alkalmazására[235]; vagy bejelentési és cselekvési mechanizmusokra[236], melyek alább tárgyalásra kerülnek, hogy azok alkalmazása hogyan viszonyul az európai uniós adatvédelmi szabályokhoz, illetőleg a DSA és annak alkalmazása hogyan egészíti az európai uniós adatvédelmi szabályokat.

3.2.1 Adatkezelési jogalap a DSA hatálya alatt

Az adatkezelés jogszerűsége, a jogalap kérdése és ennek jelentősége az adatvédelmi jog hatálya alatt a 2.3.1 pont alatt bemutatásra került a jelen értekezésben.

A DSA elsődleges célja a jogellenes tartalom, az átláthatóság, és a platformok felelősségének szabályozása, nem közvetlenül az adatkezelési jogalapok meghatározása. 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[237]. Ezzel kapcsolatosan kiemelendő, hogy a DSA online 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) pont) online platformok részére, amely nem biztosít mérlegelést a személyes adatok kezelésével kapcsolatosan a szolgáltatók részére.

3.2.1.1 A hozzájárulás alkalmazása és annak korlátjai a DSA hatálya alatt

A hozzájárulás, mint adatkezelési jogalap alkalmazásával kapcsolatosan 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. preambulumbekezdése 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

[235] DSA (103) preambulumbekezdés és DSA 5. cikk (1) bekezdése
[236] DSA (52) preambulumbekezdés
[237] vö. Domingos Soares Farinho - Personal Data Processing by Online Platforms and Search Engines: The Case of the EU Digital Services Act, p. 43.

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.

Másrészről a DSA 26. cikk (3) bekezdése tiltja a különleges kategóriájú személyes adatok (mint például az egészségügyi adatok, politikai vagy a vallási meggyőződés) felhasználását profilalkotáson alapuló ún. targetált hirdetések céljára. A célzott hirdetés olyan reklámozási forma, amelynek célja, hogy a hirdető által népszerűsített termékeket vagy szolgáltatásokat egy meghatározott közönségnek, bizonyos jellemzők alapján irányítsák. Ez a célzás különböző tényezőkön alapulhat, például demográfiai adatokon (életkor, nem, gazdasági helyzet), viselkedési adatokon (megtekintett oldalak, keresett kifejezések, látogatási gyakoriság), vagy érdeklődési körökön (kedvelések, követések). A célzott hirdetés eszközei közé tartoznak a sütik, nyomkövető képpontok, közösségi média modulok, amelyek segítségével a felhasználók online azonosítói, mint például IP-címek vagy sütiazonosítók, alapján követik a felhasználói tevékenységeket. Ezek révén egyedi profilt alakítanak ki, amely lehetővé teszi a személyre szabott hirdetések megjelenítését. 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[238]. Ezt a tilalom általános és a jogalkotó a Crambrige Analytica ügy[239] és egyéb egészségügyi adatokkal való célzott hirdetésekkel kapcsolatos visszaélések[240] miatt vezette be. Ez a tilalom bármely különleges kategóriájú személyes adatra vonatkozik, azaz a származtatott adatokra („inferred data”[241]) is kiterjed, ha annak alapján különleges kategóriájú személyes adatokra lehet következtetni. Az Európai Adatvédelmi Testület 8/2020. sz. iránymutatásának[242] 124. pontja foglalkozik ezzel a problémával, mely szerint „*a közösségi média felhasználóinak megcélzásáról a nagy mennyiségű információ és a különleges kategóriájú adatokon alapuló célzás megelőzésére*

[238] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 26. Rn 45; p. 320
[239] 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)); https://www.europarl.europa.eu/doceo/document/TA-8-2018-0433_HU.html; lehívás: 2024.09.11
[240] 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); https://edri.org/our-work/algorithms-of-trauma-new-case-study-shows-that-facebook-doesnt-give-users-real-control-over-disturbing-surveillance-ads/; lehívás: 2024.09.10
[241] A provided, observed és inferred data megkülönböztetésről lásd: Article 29 Working Party Guidelines on the right to data portability Adopted on 13 December 2016; pp. 8-9.
[242] Európai Adatvédelmi Testület - 8/2020. sz. iránymutatás a közösségi média felhasználóinak megcélzásáról 2.0. változat Elfogadás időpontja: 2021. április 13.; https://www.edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_hu_0.pdf; lehívás: 2024.09.11

irányuló intézkedések hiánya azt jelenti, hogy különleges adatkategóriák kezeléséről van szó. Ugyanakkor önmagában az a tény, hogy egy közösségimédia-szolgáltató nagy mennyiségű olyan adatot kezel, amely potenciálisan felhasználható különleges adatkategóriák megállapításához, nem jelenti automatikusan azt, hogy az adatkezelés az általános adatvédelmi rendelet 9. cikkének hatálya alá tartozik. A 9. cikk nem alkalmazható, ha a közösségimédia-szolgáltató által végzett adatkezelés nem vezet különleges adatkategóriák levezetéséhez, és ha a közösségimédia-szolgáltató intézkedéseket hozott annak megakadályozására, hogy az ilyen adatok levezethetők vagy célzási célokra felhasználhatók legyenek." Az iránymutatás rámutat arra, hogy a felhasználókra vonatkozó nagyszámú személyes adat kezelése különleges kockázatokkal járhat a természetes személyek jogaira és szabadságaira nézve, amelyeket a GDPR 32. cikkében előírt megfelelő biztonsági intézkedések végrehajtásával, valamint a GDPR 35. cikke szerint elvégzendő adatvédelmi hatásvizsgálat eredményének figyelembevételével kell kezelni.

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, 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 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 DSA 71. preambulumbekezdése szerint az adatminimalizálás elvével összhangban ez a tilalom nem vezethet ahhoz, hogy az online platformot üzemeltető szolgáltató több személyes adatot tároljon, szerezzen meg vagy kezeljen, mint amennyivel már rendelkezik, annak értékelése érdekében, hogy a szolgáltatás igénybe vevője kiskorú-e. Ezért ez a kötelezettség nem ösztönözheti az online platformot üzemeltető szolgáltatókat arra, hogy a szolgáltatás igénybe

vevőjének életkorára a használat előtt rákérdezzenek. Ez a követelmény a gyakorlatban azt jelenti, hogy a szolgáltató támaszkodhat az adatminimalizálási követelményekre, ha nem kérdez rá az életkorra és ennek megfelelően számára nem lesz ismert a felhasználó kiskorúsága. Ez azonban targetált hirdetések esetében ellentétben állhat a szülői hozzájárulás követelményével, ha a szolgáltató ezt a hozzájárulást elmulasztja beszerezni, ezért a gyakorlatban várhatóan olyan megoldások alkalmazását igényli, ami a kiskorúságra vonatkozó adatok kezelése nélkül (pl. kontextus alapon) korlátozza a targetált hirdetések alkalmazását gyermekek részére szóló szolgáltatások / tartalmak esetében.[243]

Az Európai Bíróság a *Meta Platforms Inc. és társai kontra Bundeskartellamt ügyben*[244] foglalkozott a platformok által kezelt különleges kategóriájú személyes adatok kezelésének kérdésével és ennek korlátaival, mikor a platform erőfölényes helyzetben van az online közösségi hálózatok piacán, amely szintén befolyásolja a hozzájárulás érvényességét. A Bíróság egyértelművé tette, hogy azon körülmény, hogy valamely online közösségi hálózat üzemeltetője erőfölényben van az online közösségi hálózatok piacán, önmagában nem zárja ki, hogy az ilyen hálózat felhasználói érvényesen hozzájárulhassanak a személyes adataik ezen üzemeltető általi kezeléséhez. E körülmény azonban fontos tényezőnek minősül annak meghatározása szempontjából, hogy a hozzájárulást ténylegesen érvényesen, és különösen szabadon adták-e meg, amit az említett üzemeltetőnek kell bizonyítania. Ez összhangban van az elszámoltathatóság követelményével, mellyel kapcsolatosan tehát az Európai Bíróság nem zárja ki a hozzájárulás érvényességét, de szigorúbb feltételeket szab olyan platformokkal szemben, melyek erőfölényes helyzetben vannak, melyet ennek megfelelően figyelembe kell venni a hozzájárulás érvényességének elbírálásakor.[245]

Az Európai Adatvédelmi Testület 2024. április 17. napján véleményt[246] fogadott el a személyes adatoknak az online óriásplatformok által alkalmazott „hozzájárulási vagy fizetési” modellek

[243] vö. Müller-Terpitz / Köhler- DSA Kommentar – Artikel 28. Rn 48; p. 347.
[244] Európai Unió Bírósága, C-252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság (ECLI:EU:C:2023:537);
https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1; lehívás: 2024.08.25
[245] Európai Unió Bírósága C-673/17. számú, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH ügyben hozott, 2019. október 1-i ítélete (ECLI:EU:C:2019:801)
[246] 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; https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf; lehívás: 2024.08.20

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. Ami az online óriásplatformok által alkalmazott „hozzájárulási vagy fizetési" modelleket illeti, az Európai Adatvédelmi Testület úgy véli, hogy a legtöbb esetben nem lesz lehetőségük megfelelni az érvényes hozzájárulásra vonatkozó követelményeknek, ha a felhasználók csak a személyes adatok viselkedési célú hirdetési célú kezeléséhez való hozzájárulás és a díjfizetés közötti választással szembesülnek. Az Európai Adatvédelmi Testület úgy vélte, hogy a személyes adatok viselkedési célú hirdetési célú kezelésével járó szolgáltatásokkal szemben csak fizetett alternatívát kell kínálni az adatkezelők számára. Az alternatív megoldások kidolgozásakor az online óriásplatformoknak fontolóra kell venniük, hogy az egyének számára olyan „egyenértékű alternatívát" biztosítsanak, amely nem jár díjfizetéssel. Ha az adatkezelők úgy döntenek, hogy díjat számítanak fel az „egyenértékű alternatívához" való hozzáférésért, jelentős figyelmet kell fordítaniuk arra, hogy további alternatívát kínáljanak. Ez az ingyenes alternatíva nem tartalmazhat viselkedésalapú reklámot, például olyan hirdetési formával, amely kevesebb vagy semmilyen személyes adat kezelését foglalja magában. Ez különösen fontos tényező az érvényes hozzájárulás GDPR szerinti értékelésében.

Az Európai Adatvédelmi Testület hangsúlyozza[247], hogy a hozzájárulás megszerzése nem mentesíti az adatkezelőt attól, hogy betartsa a GDPR 5. cikkében meghatározott valamennyi elvet, például a célhoz kötöttséget, az adatminimalizálást és a tisztességes eljárás elvét. Emellett az online óriásplatformoknak mérlegelniük kell a szükségesség és az arányosság elvének való megfelelést is, és felelősek annak bizonyításáért, hogy adatkezelésük általában összhangban van a GDPR-ral. Ami a hozzájárulás ingyenességének szükségességét illeti, a következő kritériumokat kell figyelembe venni: feltételesség, hátrány, a hatalom kiegyensúlyozatlansága és a szemcsésség. Az Európai Adatvédelmi Testület például rámutat arra, hogy a felszámított díjak nem kényszeríthetik az egyéneket arra, hogy beleegyezésüket érezzék. Az adatkezelőknek eseti alapon értékelniük kell, hogy a díj egyáltalán megfelelő-e, és hogy az adott körülmények között mennyi a megfelelő összeg. Az online óriásplatformoknak azt is mérlegelniük kell, hogy

[247] Európai Adatvédelmi Testület - A „hozzájárulás vagy fizetés" modelleknek valódi választási lehetőséget kell kínálniuk; https://www.edpb.europa.eu/news/news/2024/edpb-consent-or-pay-models-should-offer-real-choice_hu; lehívás: 2024.09.07

a hozzájárulás megtagadására vonatkozó döntés negatív következményekkel járhat-e, mint például a kiemelkedő szolgáltatásból való kizárás, a szakmai hálózatokhoz való hozzáférés hiánya, vagy a tartalom, vagy a kapcsolatok elvesztésének kockázata. Az Európai Adatvédelmi Testület megjegyzi, hogy az online óriásplatformok esetében valószínűsíthetők az ilyen negatív következmények, ha az adatkezeléshez való hozzájárulás megszerzéséhez „hozzájárulási vagy fizetési” modellt használnak, ami az elszámoltathatósági követelmények szigorodásával járnak.

3.2.1.2 Szerződéses jogalap alkalmazása

A DSA nem módosítja közvetlenül a GDPR szerződéses jogalapjának (GDPR 6. cikk (1)(b) pont) alkalmazását. A DSA 45. preambulumbekezdése rögzíti, hogy a közvetítő szolgáltatók szerződési szabadságát főszabály szerint tiszteletben kell tartani, de az átláthatóság, a szolgáltatást igénybe vevők védelme, illetve a tisztességtelen és önkényes megoldások elkerülése érdekében ajánlott bizonyos szabályokat meghatározni az ilyen szolgáltatók szerződési feltételeinek tartalmára, alkalmazására és érvényesítésére vonatkozóan. A DSA 14. cikke a szerződési feltételekkel kapcsolatosan transzparencia szabályokat alkalmaz, és ezen átláthatóságra és felhasználói jogokra vonatkozó előírásai megnehezítik az online platformok számára annak érvényesítését, hogy bizonyos típusú adatkezelés (pl. viselkedési nyomkövetés, célzott hirdetések) "szükséges" a szerződés teljesítéséhez. A DSA ezt tovább erősíti azzal, hogy megköveteli az online platformoktól az adatkezelés céljainak és terjedelmének világos megfogalmazását, megnehezítve azt, hogy az adatkezelést másodlagos célok (például célzott hirdetések) érdekében is szükségesként állítsák be. A DSA által előírt átláthatóság, felhasználói jogok és platform elszámoltathatósági rendelkezések tehát korlátozza a platformok azon lehetőségét, hogy a GDPR 6. cikk (1) bekezdés b) pontjára (szerződéses jogalap) hivatkozva kezeljék a felhasználói személyes adatokat, különösen a célzott hirdetésekkel, tartalom személyre szabásával és ajánlórendszerekkel kapcsolatos tevékenységek esetében. A platformoknak alaposabban kell igazolniuk, hogy az adatkezelés szigorúan szükséges a szolgáltatás nyújtásához, ami a szerződéses adatkezelési jogalap konzervatívabb értelmezését teszi szükségessé.

3.2.1.3 Kötelező adatkezelések

A DSA számos jogi kötelezettségeket rögzíti személyes adatok kezelésére. A jogellenes tartalommal szembeni fellépést előíró 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 B2C piacteret üzemeltető online platform szolgáltatóknak ugyanis kötelességük biztosítani, hogy a kereskedők személyes adatai megfelelően nyomon követhetők és tárolhatók legyenek a jogellenes kereskedelmi tevékenységek azonosítása érdekében, és a kapcsolódó adatok szerződéses időtartam alatti kezelését és azt követő hat hónapig való biztonságos tárolását is előírja a DSA, melyet követően az adatokat törölni kell[248], ami szintén egy eltérést nem engedő jogszabályi kötelezettségnek való megfelelésnek minősül és a szolgáltatás felfüggesztésével is kikényszerítendő[249]. 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

[248] vö. DSA 30. cikk (5) bekezdés
[249] vö. DSA 30. cikk (2) bekezdés

szolgáltatni az ehhez szükséges adatokat, beleértve a személyes adatokat is, ha azokra a vizsgálat során szükség van. Mindezek a rendelkezések kötelező adatkezelési műveleteket fogalmaznak meg, ami azt jelenti, hogy a személyes adatok kezelésével kapcsolatosan nincs mérlegelési és eltérési lehetősége az online platformoknak.

3.2.2 Platformok felelőssége

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.

3.2.2.1 Adatvédelmi jogsértésért való felelősség

Az online platform felelős az adatvédelmi szabályok megsértésért, 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, az adatbiztonsági rendelkezéseket, a beépített és alapértelemzett adatvédelem elvét vagy akár az érintetti jogokat. 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*[250] és a *Wirtschaftsakademie* ügyben döntött arról, hogy a keresőprogramok működtetői, illetőleg a közösségi média platformok adatkezelőnek minősülnek-e a személyes adatok védelmére vonatkozó szabályozás alapján. Mindkét esetben

[250] Európai Unió Bírósága 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 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 a CJEU a Wirtschaftsakademie 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 adatkezelés jogszerűségéért felelősnek minősülnek.

3.2.2.2 Platformok (közvetítő szolgáltatók) felelőssége és mentesülése

A közvetítő szolgáltatóként eljáró platformok általában automatikus adatkezelés útján kezelnek különböző tartalmakat, 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.

A tartalomszolgáltatók, felhasználók online környezetben jellemzően valamely közvetítő szolgáltató eszközeinek felhasználásával valósítanak meg jogsértést, amelynek megtörténtéről a közvetítő szolgáltató a szolgáltatás műszaki jellemzőiből adódóan jellemzően nem rendelkezik tudomással. 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[251].

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[252]. A rendeleti szabályozásból következően ezek a rendelkezések immár közvetlen hatállyal rendelkeznek valamennyi EU tagállamban és teljes harmonizációt valósítanak meg[253]. A DSA 3. cikk a pontja a rendelet alkalmazását „az információs társadalom szolgáltatására" és ezzel kapcsolatosan nyújtott közvetítő szolgáltatásokra szűkíti, illetve a közvetítő szolgáltatások fogalmát a DSA 3. cikk g) pontja információs társadalom szolgáltatásaiból „egyszerű továbbításra": „gyorsítótárazásra" és „tárhelyszolgáltatásra" szűkíti és ezáltal határozza meg a DSA alkalmazási körét. „Az információs társadalom szolgáltatása" fogalma az (EU) 2015/1535 irányelv 1. cikke (1) bekezdésének b) pontjában meghatározott szolgáltatásra utal, amely fogalommeghatározás szerint „szolgáltatás": az információs társadalom bármely szolgáltatása, azaz bármely, általában térítés ellenében, távolról, elektronikus úton és a szolgáltatást igénybe vevő egyéni kérelmére nyújtott szolgáltatás. E fogalommeghatározás alkalmazásában „távolról" azt jelenti, hogy a szolgáltatást a felek egyidejű jelenléte nélkül nyújtják; „elektronikus úton" azt jelenti, hogy a szolgáltatás kezdőpontjától való elküldése és célállomásán való fogadása adatok feldolgozására (beleértve a digitális tömörítést is) és tárolására szolgáló elektronikus berendezés útján történik, valamint annak elküldése, továbbítása és vétele teljes egészében vezetéken, rádión, optikai vagy egyéb elektromágneses eszköz útján történik; „a szolgáltatást igénybe vevő egyéni kérelmére" azt jelenti, hogy az adatok továbbításával nyújtott szolgáltatás egyéni kérelemre történik. E fogalommeghatározásból eredően a DSA alkalmazása és a közvetítő szolgáltató mentesülése nem vonatkozik azokra a szolgáltatásokra, melyeket nem üzleti, gazdaságilag orientált

[251] vö. Müller-Terpitz / Köhler- DSA Kommentar, 60. o., 25. sarokpont
[252] A DSA 89. cikk (1) bekezdése hatályon kívül helyezte az elektronikus kereskedelemről szóló irányelv 12-15. cikkeit, amit ezt a kérdést szabályozta.
[253] vö. DSA rendelet (9) preambulumbekezdése: „Ez a rendelet teljes mértékben harmonizálja a belső piacon a közvetítő szolgáltatásokra alkalmazandó szabályokat azzal a céllal, hogy biztonságos, kiszámítható és megbízható online környezetet biztosítson, kezelve a jogellenes tartalmak online terjesztését és azokat a társadalmi kockázatokat, amelyeket a dezinformáció vagy más tartalmak terjesztése okozhat, és ahol a Chartában rögzített alapvető jogok hatékony védelemben részesülnek és elősegítik az innovációt. Ennek megfelelően a tagállamok nem fogadhatnak el és nem tarthatnak fenn további nemzeti követelményeket az e rendelet hatálya alá tartozó kérdésekre vonatkozóan, kivéve ha e rendelet kifejezetten előírja, mivel ez érintené az e rendelet célkitűzéseinek megfelelően a közvetítő szolgáltatókra alkalmazandó, teljes mértékben harmonizált szabályok közvetlen és egységes alkalmazását."

„szolgáltatásként” nyújtanak, amely az európai uniós jogalkotó ezzel kapcsolatos szabályozási kompetenciájának hiányából következik[254].

A DSA technológiasemleges, horizontális szabályok létrehozásával mentesíti a közvetítő szolgáltatókat a felhasználóik által elkövetett cselekmények alóli felelősség alól, mégpedig függetlenül attól, hogy polgári jogi, büntetőjogi vagy pedig közigazgatási/közjogi alapon áll fenn a jogsértés és ez a felelősség alóli mentesülés adatvédelmi jogokat sértő információkért való felelősségre is kiterjed. A szabályozás lényege, hogy a közvetítő szolgáltatók főszabály szerint felelősséggel tartoznak a szolgáltatásaik révén elkövetett jogsértésekért, ideértve az adatvédelmi jogszabályokat sértő tartalmakat is, azonban bizonyos feltételek mellett mentesülhetnek a felelősség alól ún. "safe harbor" szabályok alapján. A közvetítő szolgáltatók felelősségének kérdésében két megközelítés lehetséges: a szigorú, objektív megközelítés alapján a közvetítő szolgáltatóval szemben a harmadik személy által elkövetett jogsértésért a szolgáltató felróhatóságától függetlenül lehetséges bizonyos igények érvényesítése, ami az objektív szankciók felelősségtől független alkalmazhatóságának uniós jogi előírásában tükröződik. A második megközelítés a felróhatósági alapú felelősségi elmélet, amikor a közvetítő szolgáltató csak abban az esetben felel, ha tud, illetve a körülmények alapján tudnia kell a jogsértésről. Az elektronikus kereskedelemről szóló irányelv safe harbor-szabályok létrehozása útján az utóbbi felelősségi elmélet alapján áll, és a következő elvek alapján határozza meg a közvetítő szolgáltatókkal szembeni fellépés kereteit: (i) a közvetítő szolgáltatók főszabály szerint felelnek a szolgáltatásaik útján elkövetett jogsértésért; azonban (ii) bizonyos safe harbor-szabályok alapján és ott rögzített feltételek teljesítése/teljesülése esetén mentesülnek a felelősség alól; (iii) a mentesülés ellenére bizonyos megelőző jellegű intézkedések, függetlenül a közvetítő szolgáltató mentesülésétől, továbbra is elrendelhetőek a szolgáltatóval szemben.

A felelősség alóli mentesülés szempontjából a közvetítő szolgáltatók tevékenységének négy típusát határozza meg a jogszabály. A DSA 4. cikke szabályozza az „egyszerű továbbítást” [*mere conduit*] végző szolgáltatók felelősség alóli mentesülését, akik adatátviteli és hozzáférési szolgáltatást nyújtanak, azaz az igénybe vevő által biztosított információt távközlő hálózaton továbbítják [*network provider*], vagy hozzáférést biztosítanak a hálózathoz [*access provider*].

[254] vö. Müller-Terpitz / Köhler- DSA Kommentar; 60. o., 23. sarokpont

A DSA 5. cikke szabályozza a gyorsítótárazást végző szolgáltatók felelősségét, akik gyorsítótárolási funkciót látnak el, amelynek célja az információ továbbításának hatékonyabbá tétele, különösen más igénybe vevők kezdeményezésére. A DSA 6. cikke szabályozza a tárhelyszolgáltatást végző szolgáltatók felelősségét, amely során a szolgáltató az igénybe vevő által biztosított információkat tárolja, illetve keresési funkciókat is nyújt. A DSA nem szabályozza külön az online keresőprogram-szolgáltatók felelősség alóli mentesülését, azonban ezek a szolgáltatások is a felelősség alóli mentesülés hatálya alá esnek a DSA alapján.[255] Az ún. online keresőprogram-szolgáltató felelősség alóli mentesülését Magyarországon az Elkertv. 7. §. (3) bekezdése külön is szabályozza, azonban ezzel kapcsolatosan a jogirodalom szerint[256] funkciótól függően az egyszerű továbbítást, gyorsítótárazást vagy tárhelyszolgáltatást végző közvetítő szolgáltatók körébe tartozhatnak, attól függően, hogy az online keresőprogram-szolgáltató milyen funkciójáról van szó, amely az adott ügy egyedi tényállásától függ[257]. Itt rögzítendő, hogy számos online szolgáltató egyidejűleg több, akár különböző szabályozási rezsim alá tartozó szolgáltatást is nyújthat, ami közvetlenül befolyásolja az adott tevékenységgel kapcsolatos felelősségét is. Így egy közvetítő szolgáltató egyrészről eljárhat tartalomszolgáltatóként (mint egy online újság) – amellyel kapcsolatos szolgáltatásokért közvetlen felelősséggel tartozik –, míg ezzel szemben online fórum vonatkozásában már tárhelyszolgáltatóként jár el.

A közvetítő szolgáltató a DSA (és az Elkertv. online keresőprogram-szolgáltatóra vonatkozó) szabályai szerint akkor mentesülhet a felelősség alól, ha a jogellenes cselekmény minden elemét ugyan megvalósítja, de nem rendelkezik tényleges tudomással vagy ellenőrzéssel a rendszerén keresztül továbbított vagy tárolt jogellenes tartalom vagy információ felett. Ez azt jelenti, hogy a szolgáltató tevékenysége pusztán *technikai, automatikus és passzív jellegű*, és ebben az esetben a szolgáltató nem vonható felelősségre a jogellenes tartalmakért[258]. Kiemelendő, hogy platformok és online piacterek kettős szerepet tölthetnek be. Egyrészről tartalomszolgáltatóként járhatnak, amikor saját áruikat forgalmazzák és hirdetik, másrészt online közvetítőként is működhetnek, amikor kereskedőknek, felhasználóknak vagy egyéb harmadik feleknek nyújtanak megjelenési lehetőséget és értéknövelt szolgáltatásokat. A fő kérdés minden esetben az, hogy a szolgáltató szerepe semleges marad-e, tehát tevékenysége csupán *technikai,*

[255] vö. Müller-Terpitz / Köhler- DSA Kommentar; 84. o., 50. sarokpont
[256] vö. Müller-Terpitz / Köhler- DSA Kommentar; 64-65. o., 48. sarokpont
[257] vö. Müller-Terpitz / Köhler- DSA Kommentar; 84. o., 51. sarokpont
[258] vö. Müller-Terpitz / Köhler- DSA Kommentar; 59. o., 19. sarokpont

automatikus és passzív jellegű-e, ami azt jelenti, hogy nincs tényleges ismerete vagy ellenőrzése a tárolt adatok felett. A közvetítő szolgáltatók ennek megfelelően akkor tehetők felelőssé a felhasználók által kezelt és megosztott személyes adatokért, ha a DSA 4 - 6. cikkének, illetőleg online keresőprogram-szolgáltató esetén az Elkertv. 7. § (3) bekezdése szerinti feltételek nem teljesülnek. Gyorsítótárazást, tárhelyszolgáltatást és online keresőprogram-szolgáltatás esetén annak van jelentősége, hogy a szolgáltató tudomást szerzett-e a jogellenes tartalomról és ezt követően haladéktalanul eltávolította, illetőleg hozzáférhetetlenné tette-e a jogellenes tartalmat[259].

Fontos megjegyezni, hogy bár a közvetítő szolgáltató mentesülhet a felelősség alól, ennek ellenére követelhető tőle a jogsértés megelőzése vagy megszüntetése[260]. 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. 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.

3.2.2.3 Kellő gondossági követelmények megsértéséért való felelősség

Mint fentebb bemutatásra került, 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[261] 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 szerint az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak gondosan azonosítaniuk, elemezniük és értékelniük kell a

[259] vö. DSA 5. cikk (1) bek. e) és 6. cikk (1) bek. b) pontot, illetőleg Elkertv. 7. § (3) b) pontot
[260] vö. DSA rendelet 4. cikk (3) bekezdése; 5. cikk (2) bekezdése, 6. cikk (4) bekezdése
[261] vö. Domingos Soares Farinho im p. 44.

szolgáltatásaik és a kapcsolódó rendszerek – többek között az algoritmikus rendszerek – kialakításából vagy működéséből vagy a szolgáltatásaik használatából eredő rendszerszintű kockázatokat, mellyel kapcsolatosan a DSA külön nevesíti a személyes adatok védelmét. A DSA 35. cikke szerint e kockázatértékelés alapján azonosított rendszerszintű kockázatok alapján az online óriásplatformot vagy nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak észszerű, arányos és hatékony kockázatcsökkentési intézkedéseket kell bevezetniük azonosított egyes rendszerszintű kockázatokra szabva. Ez a gyakorlatban azt jelenti, hogy ha az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltató a személyes adatok kezelése tekintetében kockázatértékelést nem végeznek, illetve a kockázatértékelés alapján nem teljesítik azt a kötelezettséget, hogy ezekre tekintettel észszerű, arányos és hatékony kockázatcsökkentési intézkedéseket, akkor a GDPR 5. cikk (2) bekezdése és 24. cikkének (1) és (2) bekezdése szerinti elszámoltathatósági követelményeket is megsérthetik, melynek alapján a felelősségük a DSA 4.-6. cikkében rögzített mentesülés ellenére is fennállhat, mely esetben a DSA és a GDPR szerinti felelősség átfedésben van egymással.[262] 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[263], mely kockázatkátokat a DSA 35. cikkében foglaltaknak megfelelően kell csökkenteni, melyhez a GDPR 35. cikke szerinti adatvédelmi hatásvizsgálatnak[264] és adott esetben 36. cikk szerinti előzetes konzultációnak kell párosulnia, ha az azonosított magas kockázatok nem csökkenthetők elfogadható szintre. A DSA 41. cikk (7) bekezdése szerint a vezető testületnek elegendő időt kell fordítania a kockázatkezeléssel kapcsolatos intézkedések mérlegelésére. Emellett aktívan részt kell vennie a kockázatkezeléssel kapcsolatos döntésekben, és biztosítania kell, hogy megfelelő erőforrásokat fordítsanak a DSA 34. cikkel összhangban azonosított kockázatok kezelésére, ami szintén megszigorítja az érintett szolgáltatók elszámoltathatósági kötelezettségeit.

[262] vö. Domingos Soares Farinho - im p. 44.
[263] vö. Müller-Terpitz / Köhler: DSA-Kommentar. Artikel 34, 403. o., 27-28. sarokpontok
[264] vö. Müller-Terpitz / Köhler- DSA Kommentar; Artikel 35, 410. o., 5. sarokpont

3.2.3 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. Mivel e tevékenységek felhasználói személyes adatok kezelésével járnak, azoknak közvetlen adatvédelmi implikációjuk van és bizonyos mérlegelést igényel a közvetítő szolgáltatók részéről.

3.2.3.1 „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 9, 16. és 23. cikkek) központi fogalma. A DSA 12. preambulumbekezdése 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. Az elektronikus kereskedelemről szóló irányelv 3. cikkében meghatározott „származási ország elve"[265] a DSA hatálya alatt is alkalmazandó marad. A DSA 38.

[265] A származási ország elvéről vö. Lodder, Arno R., European Union E-Commerce Directive - Article by Article Comments (2017). Guide to European Union Law on E-Commerce, Vol. 4. Update from 2016 (published 2017) of the 2001 (published 2002) version, published in EU Regulation of E-Commerce. A Commentary Elgar Commentaries series, 2017, pp. 15-58., 2.2.2.3; p. 10.SSRN: https://ssrn.com/abstract=1009945; lehívás: 2024.09.15.

preambulumbekezdés alapján a származási ország elve nem vonatkozik a hatóságok és bíróságok jogellenes tartalmakkal kapcsolatos végzéseire, mivel ezek a tartalomra, nem pedig a szolgáltatóra irányulnak, így nem korlátozzák a szolgáltatók határokon átnyúló szolgáltatásnyújtását. Az ilyen rendelkezések esetében tehát nincs szükség az elektronikus kereskedelemről szóló irányelv 3. cikk (4) bekezdésében foglalt kivételek alkalmazására. 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)[266] ügyben a blokkolási rendelkezések alkalmazási körét kiterjesztette az értelmileg azonos, hasonló tartalmakra is.

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

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

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.[267] 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, illetve az emberi felülvizsgálat kötelező biztosítását ilyen eszközök igénybe vétele esetén. Ezek a személyes adatok kezelésével járó tevékenységek jogkorlátozást valósítanak meg az érintett viszonylatában, ezért a DSA ún. alapjogi teszt hatálya alá rendeli ezek alkalmazását. Az Európai Unió Bírósága és a magyar bíróságok a DSA alkalmazandóvá válását megelőzően kialakított és a következő pontokban bemutatandó joggyakorlata alaposan feltehetően irányadó marad ebben a körben.

3.2.3.2 Általános nyomon követés és egyéb proaktív intézkedések előírásának tilalma

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

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

összhangban. A DSA szerint tehát nem állapítható meg olyan általános kötelezettség, amely szerint 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, ezekben 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.[268]

Az általános nyomonkövetési kötelezettség közvetítő szolgáltatókra irányadó tilalmát korábban az elektronikus kereskedelemről szóló irányelv korábbi 15. cikke rögzítette, és a DSA 8. cikke gyakorlatilag változatlanul vette át ezt a rendelkezést. A jogszabály vonatkozó rendelkezéseinek az általános monitoring gyakorlati kivitelezhetetlensége mellett az is indoka, hogy egy szűrőrendszer bevezetése gyakorlatilag internetes cenzúrát valósítana meg, illetőleg szükségtelenül és aránytalanul sértené a felhasználók magánélethez, adatvédelemhez fűződő jogait. Ez a tilalom mindazonáltal csak általános jellegű kötelezettségek elrendelésére vonatkozik, így ez nem érinti az egyedi esetben alkalmazandó (specifikus) nyomonkövetési kötelezettségeket. Ugyanitt említendő, hogy a közvetítő szolgáltatók felelősségének korlátozásai nem érintik olyan bírósági vagy közigazgatási határozatok (ideiglenes intézkedések) meghozatalának a lehetőségét, amelyek valamilyen jogsértés abbahagyását vagy megelőzését – ideértve a jogellenes adat eltávolítását vagy az ahhoz való hozzáférés

[268] 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.; http://www.sztnh.gov.hu/kiadv/ipsz/201303-pdf/01.pdf; lehívás: 2024.09.15.

megszüntetését – rendelik el.[269] Az Európai Unió Bíróság az elektronikus kereskedelemről szóló irányelv 15. cikke értelmezése kapcsán a megelőző jellegű intézkedések alkalmazási körével elsőként a L'Oréal v. eBay-ügyben[270] foglalkozott: a Bíróság szerint az online piactér üzemeltetőjével szemben meghozható bírósági eltiltó határozat nem csupán létező, az online piac révén okozott jogsértések megszüntetéséhez, hanem olyan intézkedések meghozatalára is irányulhat, amelyek az új jogsértések megelőzéséhez is hatékonyan járulnak hozzá (lásd a L'Oréal v. eBay-határozat 131. pontját). A Bíróság szerint mindazonáltal tekintettel kell lenni azokra a korlátozásokra, miszerint nem várható el a szolgáltatótól, illetve nem szükséges és nem arányos az az intézkedés, ami valamennyi ügyfél adatai összességének tevőleges nyomonkövetését (általános nyomonkövetési kötelezettség) írja elő a szellemitulajdon-jogok megsértésének jövőbeli megelőzése érdekében (139. pont). Ezen jogsértésekkel összefüggésben a szűrő-, illetve blokkolóintézkedések bevezetésének kezdeményezésével bizonyos tartalomhoz való hozzáférés megszüntetését próbálják meg elérni a jogtulajdonosok. Ez azonban arányossággal, kommunikációs szabadságokkal és magánélet védelmével kapcsolatos kérdéseket vet fel.

Az Európai Unió Bírósága gyakorlatában a szűrésre és blokkolásra vonatkozó intézkedések megítélése eddig több előzetes döntéshozatali ügyben is felmerült és ennek keretében kiemelendő a C70/10. sz. *SABAM vs. Scarlet-ügy* – 2011. november 24-i előzetes döntéshozatali ügyben született ítélet, illetve a C-360/10. sz. *SABAM vs. Netlog-ügy*, melyekben a Bíróság a blokkoló- és szűrőrendszerek alkalmazásának általános/alapjogi korlátjaira mutatott rá.

A Bíróság szerint egy általános nyomonkövetési kötelezettség összeegyeztethetetlen a szellemitulajdon-jogok érvényesítéséről szóló irányelv 3. cikkével, amely kimondja, hogy az irányelvben szereplő intézkedéseknek méltányosaknak és arányosaknak kell lenniük, és nem okozhatnak túlzó költségeket (lásd a L'Oréal-ügyben hozott ítélet 139. pontját). A Bíróság szerint a Scarlet-ügyben a szűrőrendszer létrehozására vonatkozó kötelezettség az internet-hozzáférést nyújtó szolgáltató hálózatán lezajlott teljes elektronikus adatátvitel tevőleges megfigyelését követelné meg, amely kiterjedne az összes továbbítandó információra, és az e

[269] Az elektronikus kereskedelmről 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.
[270] L'Oréal SA v eBay International AG (Case C-324/09) EU:C:2011:474 (CJEU)

hálózatot használó minden ügyfélre. Ezáltal a Bíróság szerint ez az intézkedés az elektronikus kereskedelemről szóló irányelv 15. cikkének (1) bekezdése szerinti általános nyomon követésre kötelezés tilalmába ütközne.

Az Európai Unió Alapjogi Chartája 17. cikkének (2) bekezdése tartalmazza a szellemitulajdon-jogok védelmét, azonban ezen jog védelme nem abszolút. A C-275/06. sz., a *Promusicae-ügyben* 2008. január 29-én hozott ítélet (EBHT 2008., I271. o.) 62–68. pontjából következően a tulajdonhoz való jog védelmét – amely jognak részét képezik a szellemitulajdon-joghoz kapcsolódó jogok – más alapvető jogok védelmével egyensúlyban kell biztosítani (lásd az ítélet 44. pontját). A Bíróság szerint így a nemzeti hatóságok és a bíróságok feladata, hogy a szerzői jog jogosultjainak védelme érdekében elfogadott intézkedések keretében igazságos egyensúlyt biztosítsanak e jog védelme és az intézkedés által érintett személyek alapvető jogainak védelme között. A Bíróság ekként emelte ki a vállalkozás szabadságát, ami az internet-hozzáférést biztosító szolgáltatót is megilleti, és amely a szolgáltató költségén létrehozandó és általa fenntartandó szűrőrendszer létrehozásával súlyosan sérülne, mivel az nem tartja be az igazságos egyensúlyt a szellemitulajdon-jog és a vállalkozás szabadságának védelme között. Másrészről a Bíróság azt emelte ki, hogy a szűrőrendszer a felhasználók jogait, így azok személyes adatok védelmére és szólásszabadságra vonatkozó jogukat is sértené, mivel a szűrés tartalomelemzést, valamint azon felhasználók IP-címének összegyűjtését és azonosítását vonná maga után, akik a jogellenes tartalmat a hálózatra küldték; másrészről a szűrőrendszer alaposan feltételezhetően jogszerű tartalmú adatátvitel blokkolását is kiválthatja, ami ellentétes az információs szabadságokkal. A Bíróság az „igazságos egyensúly” megtalálását a nemzeti bíróság hatáskörébe utalta.

A 2012. február 16-án a C-360/10. számú, a *SABAM vs. Netlog* előzetes döntéshozatal ügyében született ítéletében az Európai Unió Bírósága az információ tárolását végző tárhelyszolgáltatók vonatkozásában erősítette meg a Scarlet-ügyben kimondott alapelvet, miszerint a közvetítő szolgáltató nem kötelezhető általános nyomon követésre.

A belga közös jogkezelő SABAM a Netlog közösségi portál ellen indított keresetet, mivel annak felhasználói a SABAM repertoárjába tartozó műveket használtak fel, illetve tettek hozzáférhetővé engedély nélkül. A SABAM keresetében kérte a Netlog kötelezését a jogsértés megszüntetésére és megelőzésére szűrőrendszer létrehozása útján. A Netlog szerint ez általános

nyomonkövetési kötelezettséget róna rá, illetve sértené a felhasználóik adatvédelmi jogait is. A belga bíróság előzetes döntéshozatal iránti kérelemmel fordult az Európai Unió Bíróságához, és kérte annak megválaszolását, hogy *in abstracto* és *megelőző jelleggel*, a tárhelyszolgáltató saját költségére időbeli korlátozás nélkül védett művek felhasználását megakadályozó szűrőrendszer az Európai Unió joga alapján álló tagállami jogban bevezethető-e. Az Európai Unió Bírósága emlékeztetett arra, hogy a szellemitulajdon-jog jogosultjai eltiltás elrendelését kérhetik az online közösségi hálózati felületet üzemeltető szolgáltatókkal, így a Netloggal szemben, amely intézkedés nem csupán a jogsértés megszüntetésére, hanem új jogsértések megelőzésére is irányulhat. Ezen intézkedéseknek, amelyekre a tagállami jog irányadó, tiszteletben kell tartaniuk bizonyos korlátozásokat, melyeket az Európai Unió joga állapít meg. Ez vonatkozik különösen arra, hogy a közvetítő szolgáltató nem kötelezhető jogsértések általános nyomon követésére, így különösen arra, hogy valamennyi ügyfele adatai összességét tevőlegesen nyomon kövesse annak érdekében, hogy megelőzze a szellemitulajdon-jogok jövőbeni megsértését. Az ilyen általános nyomonkövetési kötelezettség a Bíróság szerint összeegyeztethetetlen a jogérvényesítési irányelv[271] 3. cikkével, amely kimondja, hogy az említett irányelvben szereplő intézkedéseknek méltányosaknak és arányosaknak kell lenniük, és azok nem lehetnek túlságosan költségesek. A Bíróság szerint a szűrés a felhasználók által tárolt fájlok tevőleges megfigyelését követelné meg, és az a tárhelyszolgáltató által tárolt információk döntő többségére, illetve az összes felhasználóra kiterjedne, mely vonatkozásban a Bíróság a Scarlet-ügyben meghozott ítélet 39. pontjára hivatkozott analógiaként. Így a vonatkozó rendszer az általános nyomonkövetési kötelezettség tilalmába is ütközne. Másrészről nem hanyagolható el a szűrőrendszer létrehozásának alapjogi vetülete sem. a szűrőrendszer sértheti a tárhelyszolgáltató felhasználóinak alapvető jogait is, nevezetesen a személyes adatok védelméhez való jogukat, valamint információk fogadásának és közlésének szabadságát, melyet a Charta szintén védelemben részesít. A személyes adatok sérelmét a felhasználói profilokra vonatkozó információk azonosítása, rendszerszerű elemzése és kezelése jelentené, míg a szólásszabadság azáltal sérülne, hogy a rendszer nem lenne képes különbséget tenni a jogellenes és a jogszerű tartalom között, ebből következően pedig az „igazságos egyensúly” sérülne.

[271] Az Európai Parlament és a Tanács 2004/48/EK irányelve (2004. április 29.) a szellemi tulajdonjogok érvényesítéséről; HL L 157., 2004.4.30, pp. 45–86.

Az Európai Unió Bírósága a Glawischnig-Piesczek v. Facebook Ireland Limited (C-18/18)[272] ügyben mondta ki, amely egy osztrák politikus által indított keresetre épült, hogy a tagállami bíróságok elrendelhetik az online platformok számára az olyan bejegyzések eltávolítását, amelyek hasonló tartalmúak egy már törölt, jogsértő tartalomhoz. Ugyanakkor a Bíróság hangsúlyozta, hogy az ilyen intézkedések nem vezethetnek általános monitoring kötelezettség előírásához.

Az Európai Unió Bíróságának a C-275/06 ügyszámú Telefónica vs. Promusicae-ügyben[273] arról kellett döntenie, hogy kötelezhető-e egy közvetítő szolgáltató a felhasználói személyes adatainak feltárására szellemitulajdon-jogok érvényesítése érdekében. A Productores de Música de España (Promusicae) olyan nonprofit szervezet, amely hangfelvétel-előállítókat és hanglemezkiadókat, illetve audiovizuális hanghordozó-előállítókat és -kiadókat képvisel, míg a Telefónica de España SAU (Telefónica) internet-hozzáférést nyújtó szolgáltató. Az ügy tényállása szerint a spanyol Promusicae az általa képviselt jogosultak nevében ideiglenes intézkedés iránti kérelmet terjesztett elő a Telefónica ellen, hogy a bíróság kötelezze adatszolgáltatásra a Telefónicát a Kazaa peer-to-peer fájlcserélő program olyan felhasználói azonosságának feltárására, akik részére internet-hozzáférést biztosít, és akik megosztott könyvtárukban olyan hangfelvételekhez való hozzáférést biztosítanak, amelyek felhasználási jogával a Promusicae tagjai rendelkeznek. Az adatszolgáltatás céljaként a Promusicae a szerzői jogok érvényesítésére szolgáló perindítást jelölte meg. A bíróság az ideiglenes intézkedésnek helyt adott, ami ellen a Telefónica azzal fellebbezett, hogy a törvény nem teszi lehetővé az adatok kiadását polgári eljárás keretében vagy ilyen eljárásra irányuló ideiglenes intézkedés címén. Az eljáró spanyol bíróság az eljárást felfüggesztette, és előzetes döntéshozatal keretében az Európai Unió Bíróságához fordult annak a kérdésnek a tisztázása érdekében, hogy az elektronikus kereskedelemről szóló irányelv, az infosoc-irányelv és a szellemitulajdon-jogok érvényesítéséről szóló irányelv lehetővé teszi-e, illetve előírja-e a személyes adatokra vonatkozó adatszolgáltatást. A Bíróság 2008. január 29-én kelt döntésében megállapította, hogy az ePrivacy irányelvben rögzített, a személyes adatok bizalmassága alól felmentést biztosító kivételek közül (nemzetbiztonság, a nemzetvédelem és a közbiztonság védelme) egyik sem tűnik olyan helyzetekre vonatkozónak, amely a jelen ügyre vonatkozna vagy amelyben

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

[273] Európai Unió Bírósága, Promusicae-ügy, C-275/06, Productores de Música de España (Promusicae) vs. Telefónica de España SAU. [ECLI:EU:C:2008:54]

egyébként polgári eljárást lehetne indítani. Ezt meghaladóan azonban az irányelv utalt a személyes adatok védelméről szóló 95/46/EK irányelv 13. cikkének (1) bekezdésére, ami felhatalmazta a tagállamokat arra, hogy intézkedéseket fogadjanak el a személyes adatok bizalmasságának megőrzésére vonatkozó kötelezettség korlátozására, amennyiben erre többek között mások jogainak és szabadságának védelme érdekében szükség van. A Bíróság ennek alapján arra a következtetésre jutott, hogy az ePrivacy irányelv nem zárja ki a személyes adatok szolgáltatására kötelezést, azonban nem is írja elő azt. A Bíróság rögzítette, hogy az elektronikus kereskedelemről szóló irányelv[274], az infosoc irányelv[275] és a jogérvényesítési irányelv célja, hogy a tagállamok biztosítsák többek között az információs társadalomban a szellemitulajdon-jogok és különösen a szerzői jog hatékony védelmét. Az Európai Alapjogi Charta szerint pedig a tulajdonhoz való jog, amelynek részét képezi a szellemitulajdon-jog mint a szerzői jog és a hatékony jogorvoslathoz való alapjog, a közösségi jog általános alapelvének minősül, másrészről azonban a charta garantálja a személyes adatok védelméhez, így a magánélet tiszteletben tartásához való jogot is. A Bíróság szerint ezeket a jogokat az irányelveket átültető tagállamoknak igazságos egyensúlyba kell hozniuk egymással, és ennek keretében olyan értelmezésre szükséges törekedni, ami nem sérti más alapvető jogelv, így különösen az arányosság követelményét. A Bíróság ezzel a döntés lehetőségét a kérdést előterjesztő nemzeti bíróság, illetve a tagállamok hatáskörébe utalta, tehát nem döntötte el a kérdést.

A *Bonnier ügyben*[276] szintén ez merült fel, hogy a szellemitulajdon-jogok érvényesítéséről szóló irányelv 8. cikke alapján meghozott nemzeti jogszabályra alapítottan a jogsértők személyazonosságának feltárására kérték kötelezni az elektronikus hírközlési szolgáltatót és hogy ez jogszerűnek minősül-e. Az Európai Unió Bíróságának azt a kérdést kellett megválaszolnia, hogy az adatmegőrzési irányelv kizárja-e az olyan tagállami bírói intézkedést, amely a jogosultak indítványára a szellemi tulajdont sértő személyek előfizetői adatai (így IP-cím) szolgáltatására kötelezi az elektronikus hírközlési szolgáltatókat. A Bíróság megállapítása szerint a jelen ügy nem tartozik az adatmegőrzési irányelv tárgyi hatálya alá, mivel az egy adott

[274] 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, pp. 1–16

[275] Az Európai Parlament és a Tanács 2001/29/EK irányelve (2001. május 22.) az információs társadalomban a szerzői és szomszédos jogok egyes vonatkozásainak összehangolásáról; HL L 167., 2001.6.22, pp. 10–19

[276] Európai Unió Bírósága, C-461/10. – Bonnier Audio AB és társai v. Perfect Communication Sweden AB [ECLI:EU:C:2012:219] (2012)

tagállam nemzeti jogának megfelelően az illetékes nemzeti hatóságok számára való adattovábbításokra vonatkozik. Ezzel szemben a jelen ügy tárgya polgári eljárás keretében történő adattovábbítás a szerzői jogi jogosult részére a szellemitulajdon-jogok megsértésének megállapítása céljából, ami a szellemitulajdon-jogok érvényesítéséről szóló irányelv hatálya alá tartozik. A Bíróság ismételten megerősítette azt, amit a Promusicae-ügyben korábban kimondott, hogy a tagállamok a személyes adatok magánszemélyekkel való közlésére vonatkozó kötelezettséget állapíthatnak meg a szerzői jogok megsértése miatti polgári peres eljárás indításának lehetővé tétele érdekében, utalt azonban arra, hogy az Európai Unió joga nem is ír elő ilyen kötelezettséget a tagállamok számára. A Bíróság ezzel összefüggésben rámutatott, hogy az ePrivacy irányelv, továbbá a szellemitulajdon-jogok érvényesítéséről szóló irányelv átültetése során a tagállamoknak ügyelniük kell arra, hogy ez utóbbiak olyan értelmezésére kell támaszkodniuk, amely lehetővé teszi az uniós jogrend által védett különböző alapvető jogok megfelelő egyensúlyának biztosítását. A Bíróság szerint a nemzeti bíróság a fentiek alapján – az eset egyedi körülményeit és az arányosság elvét figyelembe véve– maga mérlegelheti az ellentétes érdekeket. Ennek alapján valószínűsíthető az, hogy a nemzeti jogszabály alkalmas a szerzői jogi jogosultat megillető szellemitulajdon-jog védelme, illetve az előfizető magánszemély személyes adatai, magánélet (privacy) védelme közötti megfelelő egyensúly biztosítására (lásd az ítélet 60. pontját).

A magyar Kúria a BH 2017.1.20 szám[277] alatt közzétett ügyben a fenti európai uniós bírósági gyakorlatot tükröző döntést hozott, amely a szerzői jogi törvény adatszolgáltatást előíró (Szjt.) 94. § (1) bekezdés d) pontja értelmezését érintette. Az ügy központi kérdése, hogy az internetszolgáltató kötelezhető-e a szerzői jogsértéssel kapcsolatos jogi eljárás keretében személyes adatok kiadására anélkül, hogy az érintett személyek ehhez hozzájárultak volna. A Kúria megállapította, hogy az internetszolgáltató, mint közvetítő szolgáltató nem kötelezhető a szerzői jogsértés miatt indított polgári eljárásban az IP-címekhez tartozó személyek nevének és címének kiadására. Az internetszolgáltató csak akkor kötelezhető adatszolgáltatásra, ha erre törvény kifejezetten lehetőséget biztosít, például nemzetbiztonsági, bűnüldözési célokból, de a polgári eljárások keretében erre nem kötelezhető, kivéve, ha az érintett hozzájárulását adta, összhangban az Elkertv. 13/A. § (6) bekezdésével, amelynek értelmében a szolgáltatás igénybevételével kezelt felhasználói adatok nem kapcsolhatók össze az igénybe vevő azonosító

[277] Kúria Pfv.IV. 20.133/2016/5.

adataival és az igénybe vevő hozzájárulása nélkül nem adhatók át harmadik személy számára. Az ítélet alapvető jogelvi jelentősége a *személyes adatok védelmének elsőbbségét* hangsúlyozza. Az adatszolgáltatás személyes adatkezelést jelent, amelyre szigorú feltételek vonatkoznak az adatvédelmi jogszabályok alapján. Az ítélet szerint az IP-címen keresztül az internetezési és felhasználói szokásokból levonható ún. profilírozó következtetés a konkrét személyhez köthető, az egyén személyiségéhez tartozó legszemélyesebb adat, amely adott esetben a különleges adat fogalmát is kimerítheti, így annak kezelésére a személyes adatkezelés körében szigorúbb szabályok vonatkoznak. A döntvény szerint „*Méltányolható érdeke fűződik tehát az érintett személynek ahhoz, hogy a személyiségének jellemzőire vonatkozó ismeret nyilvánosságra hozatala saját elhatározása vagy hozzájárulása alapján történjen. A szerzői jogában sértett fél részére ugyanakkor nem kizárólagossággal áll rendelkezésre a polgári jogi igényérvényesítés, illetve ezen belül az internetszolgáltató adatszolgáltatásra kötelezésének igénye. Ezért a fenti érdekek egybevetése alapján nem férhet kétség ahhoz, hogy adott esetben a különleges kategóriájú személyes adatokat is magában foglaló személyes adatok védelméhez fűződő jog korlátozása nem áll arányban a szerzői jogból fakadó igény érvényesítésének érdekével”.* Ezért erre hivatkozással a bíróság elutasította a jogosult adatszolgáltatási kérelmét a közvetítő szolgáltatóval szemben.

3.2.3.3 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 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 követelményeinek – beleértve a DSA rendeletben foglalt követelményeket – való megfeleléshez szükséges intézkedéseket hoznak. Ez a rendelkezés amiatt lényeges, mert bár nem írható elő és nincs általános nyomon követési kötelezettség és a jogellenes tartalomra vonatkozóan proaktív intézkedésekre szolgáltatók nem kötelezhetők, azonban 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 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 felelősségkorlátozás alkalmazását akadályozta. Ezen a szolgáltatók számára hátrányos lehetett, akik igyekeztek önkéntesen feltárni és eltávolítani a jogsértő tartalmakat.[278]

A felelősségkorlátozás csak azoknak a szolgáltatóknak kedvez, akik „önkéntesen", „jóhiszeműen", „gondossággal" és a nemzeti jog, az uniós jog, különösen pedig a DSA rendelkezéseinek megfelelően járnak el. A DSA 26. preambulumbekezdése szerint annak puszta ténye, hogy a szolgáltatók ilyen tevékenységeket folytatnak, nem jelenti azt, hogy a felelősség alóli, ebben a rendeletben meghatározott mentességekkel nem lehet élni, amennyiben ezekre a tevékenységekre jóhiszeműen, kellő gondosság mellett kerül sor. Ezért a szolgáltató esetleges ilyen tevékenységeit és intézkedéseit nem kell figyelembe venni annak meghatározásakor, hogy a szolgáltató igénybe veheti-e a felelősség alóli mentességet, különösen abban a tekintetben, hogy a szolgáltató semleges szolgáltatást nyújt-e, és ezért a releváns rendelkezés hatálya alá tartozhat-e, anélkül azonban, hogy ez a szabály azt jelentené, hogy a szolgáltató szükségszerűen élhet a mentességgel.

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 megítélni. A 26. preambulumbekezdés 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.

[278] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 7., 1. sarokpont; p. 108.; vö. Koltay András, Szikora András, Lapsánszky András, Tóth András (szerk.) - Nagykommentár a DSA rendelethez, Wolters Kluwer, 2024; 7. cikk; 77. oldal

Az „önkéntes” megfigyelési intézkedések akkor valóban önkéntesek, és saját kezdeményezés alapján történnek, ha ezek alkalmazása nem jogszabályból, bírósági vagy hatósági határozatból származó kötelezettségen alapulnak[279]. Az önkéntesség feltételezi, hogy a szolgáltatónak van választási lehetősége, hogy végrehajt-e megfigyelési intézkedéseket vagy sem és ezek közé tartozhatnak azon intézkedések is, amelyek a felhasználási feltételekben előre bejelentésre kerülnek, és amelyekhez a felhasználó a szolgáltatás igénybevételekor hozzájárulást adott. Az egyenlő bánásmód feltételezi, hogy az önkéntes intézkedéseket jóhiszeműen, gondosan, objektíven, nem diszkriminatív módon és arányosan hajtják végre. Ezeknek az intézkedéseknek tiszteletben kell tartaniuk az érintett személyek jogait és jogos érdekeit, és meg kell hozniuk minden szükséges intézkedést a jogszerű tartalmak indokolatlan eltávolításának elkerülésére[280]. A hivatkozott 26. preambulumbekezdés itt utal arra, hogy az e célból az érintett szolgáltatóknak például észszerű intézkedéseket kell hozniuk annak biztosítására, hogy amennyiben automatizált eszközök használatával kerül sor ilyen tevékenységek végzésére, a vonatkozó technológia *by-design* kellően megbízható legyen ahhoz, hogy a lehető legminimálisabbra csökkentse a hibaarányt.

A „gondossági” követelmény azt feltételezi, hogy a szolgáltató az érintett összes fél jogos érdekeit figyelembe veszik és mérlegelik, mielőtt egy tartalmat jogellenesként azonosítanak és eltávolítanak. Ez magában foglalja az Európai Bíróság joggyakorlata szerint, mint azt fentebb bemutattuk, az méltányos egyensúly biztosítását a szellemi tulajdonhoz fűződő jogok, az érintett személyiségi jogai, ideértve a személyes adatok védelméhez való jog, a vállalkozás szabadsága, valamint az információk szabad fogadásának vagy terjesztésének joga között. A gondossági követelmény megköveteli, hogy a szolgálató minden technikailag lehetséges és ésszerű intézkedést meg kell tegyen annak érdekében, hogy elkerülje a tartalmak téves jogellenes minősítését[281]. A szoftveres eszközöket mindig a technológia állása szerint kell konfigurálni, és megfelelő biztonságot kell nyújtaniuk a tartalom téves jogellenes minősítése elkerülése érdekében. Az ilyen intézkedéseket tehát – figyelemmel arra, hogy azt jogszabály nem írja elő – jogos érdek és pozitív jogos érdek teszt alapján és figyelembe véve az érintettek jogait és szabadságait, azt kímélve lehet végezni. Az önkéntes vizsgálatokkal kapcsolatos intézkedések jogszerűségének megítélésére ugyanazon elveket lehet alkalmazni, mint amelyet

[279] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 7. Rn 17; pp. 111-112.
[280] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 7. Rn 20; p. 112.
[281] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 7. Rn 24; p. 113.

az Európai Unió Bíróságának gyakorlata szűrőszoftverek kialakításával kapcsolatosan kialakított, mert nem különböznek ahhoz képest, hogy azokat önkéntesen vagy kötelezően telepítik. A jogsértések felismeréséhez szükséges szoftver megbízhatósága alapvető fontosságú, hogy elkerüljék a jogszerű tartalmak indokolatlan eltávolítását, ami kritikus fontosságú a kezelt személyes adatok adatvédelmi pontosság alapelvének megfelelő biztosításában. Az ilyen intézkedésekkel kapcsolatosan és figyelemmel az érintettek jogaival kapcsolatos feltehető magas kockázatokra, a GDPR 35. cikk (1) bekezdése szerinti adatvédelmi hatásvizsgálat elvégzése is indokolt és a hatásvizsgálat kötelező lehet akkor, ha az ilyen intézkedés profilozást, pontozást, joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal vagy módszeres megfigyelést igényel, mely adatkezelések a Nemzeti Adatvédelmi és Információszabadság Hatóság GDPR 35. cikk (4) bekezdése alapján közzétett hatásvizsgálati feketelistáján[282] szerepelnek.

Az Európai Adatvédelmi Biztos a DSA-val kapcsolatos véleménye 27. pontjában maga is emlékeztet arra, hogy még 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 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.

3.2.3.4 Tartalom moderálással kapcsolatos 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 foglalj az ilyen

[282] NAIH Hatásvizsgálati lista GDPR 35. cikk (4) bekezdés, https://naih.hu/hatasvizsgalati-lista, vö. 5, 10, 11, 13, 14 pontok; lehívás: 2024.09.15

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 és azok célja a tartalommoderálási gyakorlatok, beleértve a személyes adatok kezelésével járó intézkedések átláthatóságának további növelése.[283] A DSA alatt a tartalom moderálással kapcsolatos transzparencia követelményei jelentős adatvédelmi relevanciával bírnak. 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 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

[283] vö. EDPS DSA vélemény 33. sarokpontja

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. A 29. cikk szerinti adatvédelmi munkacsoport transzparencia iránymutatása szerint[284] az információ-túlterhelés elkerülése érdekében az adatkezelőknek hatékony és tömör módon kell folytatniuk a tájékoztatást/kommunikációt. Ezt a tájékoztatást egyértelműen el kell különíteni az egyéb, nem adatvédelemmel kapcsolatos tájékoztatástól, például a szerződéses rendelkezésektől vagy általános felhasználási feltételektől. Ez a szolgáltatók részére azt jelenti, hogy a szerződési feltételekben szereplő tartalommoderációs intézkedésekről, azok adatkezelési jogalapjáról, a kapcsolódó jogos érdekekről és adatvédelmi jogorvoslati jogokról külön adatkezelési tájékoztatást kell alkalmazni és az adatvédelmileg releváns rendelkezések nem süllyeszthetők el a szerződési feltételekben. A gyakorlatban ez azt jelenti, hogy a tartalommoderálási intézkedésekről mind a szerződési feltételekben, mind pedig az adatkezelési tájékoztatóban egyaránt tájékoztatást kell adni.

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. és 17. cikke a bejelentési és cselekvési mechanizmusokra, valamint az indokolási kötelezettségre vonatkozó szabályokat határoz meg az tárhelyszolgáltatókra, köztük az online platformok számára. Ezen a rendelkezések személyes adatok kezelésével és adott esetben az

[284] vö. Transzparencia iránymutatás 8. pontja

automatizált döntéshozatali folyamatokkal járnak és emiatt érintik a felhasználók, ideértve a felhasználók vagy a bejelentés által érintett személyek személyes adatait. A 2011/93/EU európai parlamenti és tanácsi irányelv (26) 3–7. cikkében említett bűncselekményekkel kapcsolatos bejelentések benyújtásának kivételével e mechanizmusoknak fel kell szólítaniuk a bejelentést tevő magánszemélyt vagy szervezetet, hogy a visszaélések elkerülése érdekében közölje személyazonosságát.

A DSA 16. cikk azt is megköveteli, hogy a tárhelyszolgáltatóknak (ideértve az online platformokat is) 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.[285]

A DSA 17. cikke előírja, hogy amikor egy tárhelyszolgáltató (ideértve az online platformokat is) 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 16. és 17. cikkeinek rendelkezései és a GDPR automatizált döntéshozatalt szabályozó 22. cikkének szabályai közötti kapcsolat elsősorban transzparencia szabályok útján jelenik meg, mivel az automatizált eszközök használatára vonatkozó tájékoztatási kötelezettségek azt biztosítják, hogy a felhasználók tisztában legyenek az ilyen eszközök szerepével a tartalom moderálásában. A tárhelyszolgáltatóknak (ideértve az online platformokat is) lehetőséget kell

[285] vö. DSA 15. cikk (6) bekezdése

biztosítaniuk arra, hogy bárki bejelentést tehessen jogellenes tartalomról. E mechanizmusoknak könnyen hozzáférhetőnek és felhasználóbarátnak kell lenniük, valamint lehetővé kell tenniük a bejelentések kizárólag elektronikus úton történő benyújtását. Az ilyen bejelentések tekintetében a szolgáltatónak meg kell könnyítenie, hogy a bejelentés pontos és kellően alátámasztott legyen ahhoz, hogy a szolgáltató fel tudja mérni a tartalom jogellenességét. Ilyen bejelentés fogadása esetén úgy kell tekinteni, hogy a tárhelyszolgáltató tudomást szerzett a jogellenes tartalomról, amennyiben a bejelentés lehetővé teszik a megfelelő gondossággal eljáró tárhelyszolgáltató számára, hogy részletes jogi vizsgálat nélkül azonosítsa az adott tevékenység vagy információ jogellenességét. Elérhetőség információk megadása esetén a szolgáltatónak a bejelentés kézhezvételének megerősítését is le kell küldenie az adott magánszemélynek vagy szervezetnek, aki a bejelentést tette, illetőleg indokolatlan késedelem nélkül értesítenie kell az adott magánszemélyt vagy szervezetet a bejelentés tárgyát képező információkkal kapcsolatos döntéséről, tájékoztatást nyújtva az e döntéssel kapcsolatos jogorvoslati lehetőségekről is. A DSA 16. cikk (6) bekezdése értelmében a szolgáltatók automatizált eszközöket is használhatnak a bejelentések kezelésére vagy az azokkal kapcsolatos döntéshozatalra. Ebben az esetben tájékoztatniuk kell a bejelentést benyújtó személyt az automatizált eszközök használatáról, feltéve, hogy az értesítés tartalmazza az érintett személy nevét és e-mail címét. A DSA 17. cikke előírja, hogy a tárhelyszolgáltatóknak világos és konkrét indokolást kell adniuk minden olyan döntésükről, amely a szolgáltatás felhasználói által közzétett információ eltávolítására vagy hozzáférésének megszüntetésére vonatkozik, függetlenül attól, hogy ezt a döntést milyen módon, automatizáltan vagy manuálisan hozták meg.

A bejelentési és cselekvési mechanizmusok és a kapcsolódó indokolási kötelezettségek transzparenciáját segíti elő 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 (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.

A DSA 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 felhasználásáról, 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 Európai Adatvédelmi Biztos a DSA véleményében utalt arra[286], 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.[287] 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 is 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.

3.2.3.5 Bűncselekmények gyanújának bejelentése

A DSA 18. cikke előírja, hogy a tárhelyszolgáltatóknak és online platformoknak haladéktalanul tájékoztatniuk kell a bűnüldözési vagy igazságügyi hatóságokat, ha olyan információ jut a tudomásukra, amely alapján komoly *bűncselekmény gyanúja* merül fel, amely *személyek életét vagy biztonságát fenyegeti*. A tájékoztatásnak tartalmaznia kell minden releváns információt, amely a platform rendelkezésére áll, ezt azonban a DSA nem határozza meg és csak a DSA 56. preambulumbekezdése utal arra, hogy a szolgáltatónak minden rendelkezésére álló releváns információt meg kell adnia, beleértve adott esetben a szóban forgó tartalmat és – amennyiben

[286] EDPS Opinion 1/2021 on the Proposal for a Digital Services Act, 42. pont, p.11
[287] vö. 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához; WP251rev.01, 21. oldal

rendelkezésre áll – a tartalom közzétételének időpontját a hivatalos időzónával együtt, a gyanú magyarázatát, valamint a szolgáltatás érintett igénybe vevőjének megtalálásához és azonosításához szükséges információkat.

Az Európai Adatvédelmi Biztos a DSA véleményében javasolta, hogy egyértelműen meg kell határozni a „releváns információ" fogalmát, felsorolva azokat az adatkategóriákat, amelyeket az online platformoknak közölniük kell, illetve megőrizniük a további nyomozások érdekében[288], erre azonban a jogalkotási folyamat során nem került sor. Amennyiben bejelentés szükséges, ez a személyes adatok kötelező adatkezelésének minősül. Azt az Európai Adatvédelmi Biztos véleménye is kiemeli, hogy ez a rendelkezés *nem ad jogalapot és lehetőséget a platformoknak arra, hogy felhasználói profilozást végezzenek a bűncselekmények azonosítása érdekében*[289] és ugyanezt a DSA 56. preambulumbekezdése is megerősíti. Ezt meghaladóan a magyar adatvédelmi jog sem biztosít megfelelő adatvédelmi jogalapot a bűnügyi személyes adatok kezelésére, melyekre az az információs önrendelkezési jogról és az információszabadságról 2011. évi CXII. törvény értelmében a különleges adatok kezelésének feltételeire (vö. GDPR 9. cikk) vonatkozó szabályokat és korlátokat rendeli alkalmazni és ezzel együtt adatvédelmi hatásvizsgálat köteles tevékenységnek minősül a GDPR 35. cikk (2) b) pontja és a NAIH hatásvizsgálati feketelistája alapján a GDPR 35. cikk (4) bekezdésének megfelelően.

3.2.3.6 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, például, 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

[288] EDPS Opinion 1/2021 on the Proposal for a Digital Services Act; 61. sarokpont; p. 14.
[289] EDPS Opinion 1/2021 on the Proposal for a Digital Services Act; 59. sarokpont; p. 14.

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 DSA 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)[290]. 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.

3.2.4 Profilozási tilalmak és 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 jellemzőinek értékelése, mikor a profilalkotás együtt jár a személyre vonatkozó valamilyen

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

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.[291] 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 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 aláásható 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.[292]

A platformok gyakran használják a személyes adatokat arra, hogy testre szabják a felhasználói élményt és javítsák a tartalommoderálást, ugyanakkor ezek az adatok jobb reklámszolgáltatásokat is lehetővé tesznek 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

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

alapuló ajánlások között. Ezek az intézkedések erősítik az online adatvédelem szintjét és elősegítik a transzparenciát a digitális szolgáltatások területén.

3.2.4.1 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 forgalmazott, míg a YouTube 29 milliárd USD-t) és a több szolgáltatást is átfogó, személyes adatok tömeges és extenzív gyűjtésével járó jellege[293]. 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[294] részletesen foglalkozott a közösségi média felhasználóinak megcélzásával és az egyes célzási módszerek elemzésével, az egyes szereplőkkel és azok felelősségével.

3.2.4.1.1 A hirdetés fogalma, targetált hirdetések szereplői és annak kockázatai

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[295], mint a kereskedelmi kommunikáció fogalma, mivel politikai vagy társadalmi célú (fizetett) „hirdetése" is beletartozhat. Másrészről ez a fogalommeghatározás *szűkebb*[296], 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 ennek fejében.

---

[293] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 26. Rn 1-2; pp. 311-312.
[294] Európai Adatvédelmi Testület 8/2020. sz. iránymutatása a közösségi média felhasználóinak megcélzásáról, 2.0. változat, elfogadás időpontja: 2021. április 13.; https://www.edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_hu_0.pdf; lehívás: 2024.09.14.
[295] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 3. Rn 125; p. 48.
[296] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 3. Rn 123; p. 123.

Az *ellentételezés* elemmel kapcsolatosan rögzítendő, hogy annak nem szükséges pénzmozgás formájában jelentkeznie. Így az Európai Unió Bírósága a C-51/96 és C-191/97 számú, Deliège-ügyben[297] elfogadta, hogy az EKSz. (EUMSz.) szerinti szolgáltatás ellentételezése nem szükséges, hogy közvetlen pénzmozgásként jelenjen meg (lásd 55-57. pontokat). Az EUB további gyakorlata alapján továbbá az ellentételezés nem szükséges, hogy közvetlenül attól származzon, akinek a szolgáltatást nyújtják (ld. C-291/13. számú Papasavvas-ügy[298], 28-29. pontok); valamint ellentételezésnek minősülhet az is, ha maga a részszolgáltatás ingyenes, de annak a költsége a termék / szolgáltatás árába valahol máshol be van építve (vö. 352/85. számú Bond van Averteerders és mások[299], 16. pont; C-484/14. számú Mc Fadden-ügy[300], 42-43. pontok), viszont a DSA szerint *kifejezetten* az ilyen információ népszerűsítéséért kell részesülnie ebből az online platformnak. Nem minősülnek viszont „hirdetésnek" azok az esetek, mikor nem az online platform szolgáltatója, hanem egy harmadik fél (így platformon kommunikáló influenszer) kap ellentételezést az üzenet népszerűsítésére szolgáló információ terjesztésért. Másrészről „*kifejezetten ilyen információ népszerűsítéséért*" történő ellentételezések relevánsak, míg a platform használatáért fizetendő átalánydíjak (pl. prémium feliratkozási díj) már nem[301]. Tehát csak akkor tekinthető egy harmadik személy üzenetének megjelenítése „hirdetésnek" a DSA értelmében, ha az üzenet megjelenítéséért ellentételezést (ami tehát pénzbeli vagy egyéb szolgáltatás is lehet) közvetlenül az online platform szolgáltatója kapott, és az ellentételezés nála jelentkezik. A hirdetés meghatározásának ezen fogalmi elemei tehát jelentősen szűkítik a DSA 26. cikk alkalmazásának és kiskorúaknak szóló targetált hirdetések vonatkozásában DSA 28. cikk (2) bekezdés szerinti tilalom hatályát. Ezen szakasz jelentős értelmezési kérdéseket vett fel és az elhatárolás további finomításra szorul majd a gyakorlatban.

A profilozáson alapuló célzott hirdetés a hirdetés olyan formája, amely specifikus közönségre irányul a reklámozó által népszerűsített termék vagy szolgáltatás alapján. A célzás különböző

[297] Európai Unió Bírósága, C-51-96 and C-191/97 Deliège ügy, ECLI:EU:C:2000:1999
[298] Európai Unió Bírósága, C-291/13 Sotiris Papasavvas v O Fileleftheros Dimosia Etairia Ltd, 11 September 2014, ECLI: EU:C:201,
[299] Európai Unió Bírósága, Case 352/85; 26 April 1988. Bond van Adverteerders and others v The Netherlands State; ECLI:EU:C:1988:196.
[300] Európai Unió Bírósága, C-484/14 Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, 15 September 2016; ECLI:EU:C:2016:689
[301] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 3. Rn 124; p. 48.

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 akár 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[302]. 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. 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[303]. Ezek a kérdések különösen a Cambridge-Analytica botrány ürügyén merültek

[302] vö. Európai Adatvédelmi Testület 8/2020. sz. iránymutatása a közösségi média felhasználóinak megcélzásáról; 9.-18. sarokpontok.
[303] EDRI - Sex, religion and race are advertising taboos, except for power-hungry politicians - By Civil Liberties Union For Europe · May 31, 2023; https://edri.org/our-work/sex-religion-and-race-are-advertising-taboos-except-for-power-hungry-politicians/; lehívás: 2024.09.14.

fel és azzal a következménnyel jártak, hogy az online platformok korlátozni kezdték az egyes célzási opciókat.[304]

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.[305]

A targetált hirdetések szereplői között több különböző fél található[306]. 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

[304] Facebook: Removing Certain Ad Targeting Options and Expanding Our Ad Controls; Announcements; November 9, 2021 https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls; lehívás: 2024.09.14

[305] vö. 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához; WP251rev.01, 23-24. oldal

[306] vö. Európai Adatvédelmi Testület 8/2020. sz. iránymutatása a közösségi média felhasználóinak megcélzásáról; 19.-29. sarokpontok.

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 rámutat az EUB vonatkozó ítélkezési gyakorlatára és különösen a Wirtschaftsakademie (C-210/16. számú ügy), a Jehova tanúi (C-25/17. számú ügy[307]) 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.

3.2.4.1.2 Targetált hirdetések szabályozása a DSA hatálya alatt

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.[308]

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

[307] Európai Unió Bírósága a C-25/17. számú ügyben hozott 2018. július 10-ei Jehovan todistajat-ítélet, C-25/17, EU:C:2018:551
[308] vö. DSA (68) preambulumbekezdés harmadik mondatát

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. 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 kapcsolatos átláthatósági, illetve tájékoztatási követelményeket, valamint az automatizált egyedi döntéshozatalt, beleértve a profilalkotást és a hatásvizsgálati kötelezettséget. Ezek a rendelkezések nem érinti az ePrivacy irányelv rendelkezéseit és alkalmazását sem, különösen, amelyek az információk végberendezésben történő tárolására, valamint az ott tárolt információkhoz való hozzáférésre vonatkoznak.[309]

Bár a célzott hirdetések és a profilalkotás önmagában nem tilos a GDPR szerint, a DSA azonban szigorúbbá tette a vonatkozó előírásokat, ha különleges kategóriájú személyes adatokról vagy kiskorúak a címzettek. 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.

[309] ACN - DSA Guidelines - Due diligence obligations for intemediary services - Netherlands Authority for Consumers and Markets; 188. sarokpont.

Ez az intézkedés fontos szerepet játszik a felhasználók védelmében, különösen az úgynevezett manipulatív technikák elleni harcban, amelyek célja a felhasználók kihasználása.[310] 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 megkülönböztetés révén. Az online platformok különösen érzékenyek ezekre a kockázatokra. Ennek megfelelően tilos a személyes adatok különleges kategóriáinak felhasználásával történő profilalkotás alapú hirdetések megjelenítése. Ez a tilalom nem befolyásolja az uniós adatvédelmi jogszabályok szerinti kötelezettségeket, amelyek a hirdetések terjesztésében részt vevő szolgáltatókra és hirdetőkre vonatkoznak.

Itt rögzítendő, hogy az Európai Bizottság civil szervezetek panasza[311] alapján 2024. március 24-én küldött adatkérést[312] a LinkedIn részére annak gyanúja miatt, hogy a LinkedIn megsérti a különleges kategóriájú adatokon alapuló targetált hirdetések tilalmát, mivel hirdetők számára lehetővé tette a személyes adatok különleges kategóriái alapján, azaz faji vagy etnikai származás, politikai vélemények, vallási vagy filozófiai meggyőződés, illetve szakszervezeti tagság alapján célozzák meg a szolgáltatás igénybe vevőit, ahogy azt a felhasználók LinkedIn csoportokban való részvétele feltárhatta. Az Európai Bizottság közleménye[313] szerint ezt a gyakorlatot a LinkedIn időközben megszüntette.

3.2.4.2 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,

[310] vö. Domingos Soares Farinho - im p. 51.
[311] EDRI - Civil society complaint raises concern that LinkedIn is violating DSA ad targeting restrictions; February 26, 2024; https://edri.org/our-work/civil-society-complaint-raises-concern-that-linkedin-is-violating-dsa-ad-targeting-restrictions/; lehívás: 2024.09.15
[312] Commission sends request for information to LinkedIn on potentially targeted advertising based on sensitive data under Digital Services Act, 14 March 2024; https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-linkedin-potentially-targeted-advertising-based-sensitive-data; lehívás: 2024.09.15
[313] Statement by Commissioner Breton on steps announced by LinkedIn to comply with DSA provisions on targeted advertisement; 07 June 2024; https://digital-strategy.ec.europa.eu/en/news/statement-commissioner-breton-steps-announced-linkedin-comply-dsa-provisions-targeted-advertisement; lehívás: 2024.09.15

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 hivatkozott preambulumbekezdés szerint a kiskorúak által használt online platformot üzemeltető szolgáltatóknak megfelelő és arányos intézkedéseket kell hozniuk a kiskorúak védelme érdekében, például úgy, hogy online interfészeket vagy azok részeit adott esetben úgy alakítják ki, hogy alapértelmezés szerint a magánéletet védő [privacy-by desing], legmagasabb szintű biztonságot és védelmet garantálják, vagy a kiskorúak védelmére vonatkozó normákat fogadnak el, vagy részt vesznek a kiskorúak védelmét szolgáló magatartási kódexekben. A DSA 46. preambulumbekezdése rögzíti, hogy azoknak a közvetítő szolgáltatóknak, amelyek elsősorban kiskorúakat céloznak meg, például a szolgáltatás tervezése vagy forgalmazása révén, vagy amelyeket túlnyomórészt kiskorúak vesznek igénybe, különös erőfeszítéseket kell tenniük annak érdekében, hogy szerződési feltételeik magyarázatát a kiskorúak számára könnyen érthetővé tegyék.

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”[314] 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 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, míg a DSA a "kiskorú" fogalmát, amely az uniós jogrendszerekben azoknak az adatalanyoknak a kategóriáját jelenti, akik még nem rendelkeznek teljes cselekvőképességgel[315]. Fentebb bemutattuk a hozzájárulás alkalmazásának korlátait gyermekek esetében. A GDPR 8. cikke szerint a gyermekek 16 éves kortól (vagy ennél fiatalabb kortól, ha a nemzeti jog ezt megengedi) járulhatnak hozzá az

[314] vö. a „hirdetés” DSA fogalmával kapcsolatos fogalommeghatározást a 3.2.8.1.1 pontban
[315] vö. Domingos Soares Farinho im. p. 52.

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[316] 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.

Megjegyzendő, hogy a DSA 28. cikk (4) bekezdése szerint a Bizottság további iránymutatást bocsáthat ki az online platformot üzemeltető szolgáltatóknak a megfelelő és arányos intézkedéseket alkalmazásához.

3.2.4.3 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

[316] Lásd NAIH hatásvizsgálati lista 20. pontját.

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 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.[317]

Az ajánlórendszerek vagy online hirdetések kapcsán a profilalkotás és a mikrocélzás kockázatait az Európai Adatvédelmi Biztos már felvetette az online manipulációról és a személyes adatokról szóló véleményében[318]. 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.[319] Az egyes platformok is a személyes relevanciával írják le az ajánlórendszerek célját[320]. Az ilyen rendszerek alapvetően profilalkotáson alapulhatnak, amely során a felhasználók viselkedési adatait (például korábbi keresések, interakciók, kedvelések,

---

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

[318] Lásd az Európai Adatvédelmi Biztos 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*."). https://www.edps.europa.eu/data-protection/our-work/publications/opinions/online-manipulation-and-personal-data_en; lehívás: 2024.09.14

[319] vö. Marta Micheli, Modeling User Personality Traits for Recommender Systems, Conference Paper, January 2023; Conference: CHItaly 2023 - Crossing HCI and AI; https://ceur-ws.org/Vol-3481/paper1.pdf, lehívás: 2024.09.14

[320] vö. Facebook feed recommendations AI system; June 21, 2024; https://transparency.meta.com/features/explaining-ranking/fb-feed-recommendations/; lehívás: 2024.09.14

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 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.[321] Ez a DSA szabály a személyes adatok felhasználásának korlátozását célozza, és összhangban van a GDPR 21. és 22. cikkeivel.[322] VLOP-k és VLOSE esetében a DSA 34. cikk szerinti

[321] EDPS Opinion 1/2021 on the Proposal for a Digital Services Act; 73-74. sarokpontok; 16-17. oldal
[322] vö. Domingos Soares Farinho, im. p. 53.

kockázatértékelés dönti el, hogy az ajánlórendszerek szigorúbb alkalmazása indokolt-e a DSA 35. cikke alapján.

3.2.5 Online interfész design – sötét tervezési minták

A DSA 25. cikke egy újabb védelmi réteget, egy generálklauzulát[323] 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.[324] 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[325] 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

[323] vö. Müller-Terpitz / Köhler- DSA Kommentar – Artikel 25. Rn 11; p. 308.
[324] EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them; p. 4.
[325] 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, pp. 22–39

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 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 67. preambulumbekezdése utal a sötét minták fogalmára és úgy határozza meg azokat, hogy azok „olyan gyakorlatok, amelyek akár szándékosan, akár ténylegesen jelentősen torzítják vagy korlátozzák a szolgáltatás igénybe vevőinek azon képességét, hogy önálló és megalapozott döntéseket hozzanak”. Ezek a gyakorlatok arra használhatók, hogy a felhasználókat olyan nem kívánt magatartásra vagy döntések meghozatalára vegyék rá, amelyek negatív következményekkel járhatnak rájuk nézve. A hivatkozott preambulumbekezdés számos példáját nyújtják az ilyen sötét mintáknak. Így nevesíti azt a tilalmat, hogy az online platformokat üzemeltető szolgáltatóknak, hogy megtévesszék vagy manipulálják a felhasználókat („nudging”), illetve, hogy az online felületek szerkezetén, kialakításán vagy funkcióin keresztül torzítsák vagy akadályozzák a felhasználók autonómiáját, döntéshozatalát vagy választását. Ez magában foglalja a visszaélésszerű kialakításokat, amelyek a felhasználót a szolgáltató számára előnyös, de a felhasználó számára nem feltétlenül kedvező tevékenységek felé terelik, illetve a választási lehetőségek nem semleges bemutatását. Ide tartozik továbbá a felhasználók többszöri felkérése a választásra, a lemondás megnehezítése, valamint egyes választási lehetőségek szándékos bonyolítása vagy időigényessé tétele; a vásárlások törlésének vagy egy adott platformról történő kijelentkezés megnehezítése, a felhasználók megtévesztése az ügyletekkel kapcsolatos döntéshozatalra való ösztönzéssel, illetve olyan alapértelmezett beállítások alkalmazása, amelyek nehezen módosíthatók, és indokolatlanul torzítják a felhasználók döntéshozatalát. 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.[326]

3.2.6 Különleges 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[327], 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[328]. 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[329] 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

[326] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 25. Rn 25; p. 309.
[327] vö. DSA 33. cikk (1) bekezdés
[328] Az eddig azonosított VLOP és VLOSE szolgáltatók listája itt elérhető: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses; lehívás: 2024.09.15.
[329] Müller-Terpitz / Köhler- DSA Kommentar – Artikel 35. Rn 5; p. 410.

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 35. cikke és a DSA 35. cikke sem írja elő 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 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[330], 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 lehetőséget 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.

[330] European Commission Guidelines for providers of VLOPs and VLOSEs on the mitigation of systemic risks for electoral processes, Publication 26 April 2024;https://digital-strategy.ec.europa.eu/hu/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes; lehívás: 2024.09.15

A VLOP-oknak és VLOSE-oknak a DSA 37. cikke alapján 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.

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. Ezen különleges kötelezettségeket tételesen bemutattuk a jelen 3.2 fejezetben és adatvédelmi szempontból *szigorúbb elszámoltathatósági sztenderdet* jelentenek online óriásplatformok és nagyon népszerű online keresőprogramok részére, melyek jelentéstételi és transzparencia kötelezettségekkel párosulnak. Megjegyzendő, hogy az Európai Bizottság a DSA alkalmazandóvá válása óta számos eljárást indított[331] a DSA feltehető megsértése miatt online óriásplatformok és nagyon népszerű online keresőprogram üzemeltetők ellen.

3.3 Adatokhoz való hozzáférés és kutatók hozzáférése

[331] Supervision of the designated very large online platforms and search engines under DSA; https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses, lehívás: 2024.09.15

DSA 40. cikke értelmében az online óriásplatformok (VLOP) és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók 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. Emellett ellenőrzött kutatók („vetted researcher"), ha megfelelnek 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[332] és melyet ezt követően a szabályozó hatóságok a szolgáltatók ellenőrzésére felhasználhatnak. Mind a digitális szolgáltatási koordinátor vagy a Bizottság, illetőleg mind a kutatók hozzáférése azt szolgálja, hogy a VLOP és VLOSE szolgáltatók elszámoltathatók legyenek a rendszerszintű kockáztok azonosítása, illetőleg a kockázatcsökkentés tekintetében.

3.3.1 Tudományos kutatás a GDPR hatálya alatt

Az ellenőrzött kutatók tevékenységének értékeléséhez elengedhetetlen az általuk végzett tevékenység megértése és a tudományos kutatás fogalmának elemzése. A *tudományos kutatás fogalmát* 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.

[332] vö. DSA 40. cikk (4) bekezdése

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 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.

Az Európai Adatvédelmi Testület a tudományos kutatással kapcsolatos iránymutatás kiadását tervezi, amely jelenleg egyeztetés alatt van. A német DSK, a német adatvédelmi hatóságok

grémiuma 2024. szeptember 11. napján állásfoglalást[333] adott ki a tudományos kutatásról. A DSK véleménye szerint a tudományos kutatásnak szisztematikus és módszeres megközelítést kell követnie, figyelembe véve az adott tudományterület sajátosságait. A kutatás célja új ismeretek szerzése, és nem elegendő csupán meglévő ismeretek alkalmazása vagy tudományos módszerek használata felügyeleti, szervezési vagy reklámcélokra. A tudományos kutatás alapvető kritériuma az ellenőrizhetőség, ami azt jelenti, hogy az eredmények nem tarthatók szándékosan titokban, hogy elkerüljék a szakmai közösség általi vizsgálatot. A kutatási tevékenységnek függetlennek és önállónak kell lennie, bár a megbízók befolyásolhatják a kutatás irányát, de nem szabad veszélyeztetniük a kutatók autonómiáját. Végül a DSK állásfoglalás azt is rögzíti, hogy a kutatásnak a közérdeket kell szolgálnia, és nem lehet kizárólag kereskedelmi vagy egyéni érdekeket szolgáló célú, hiszen a GDPR által biztosított kivételek csak közérdekű kutatásokra alkalmazhatók.

3.3.2 Platformok és kutatói adat-hozzáférés

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.[334]

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

[333] DSK - 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 - https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_DSK_Positionspapier%20_Wissenschaftliche_Forschungszwecke.pdf, lehívás: 2024.09.15

[334] Mathias Vermeulen - Researcher Access to Platform Data: European Developments Journal of Online Trust and Safety, p. 3.; https://tsjournal.org/index.php/jots/article/view/84/31; lehívás: 2024.09.15

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 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.[335]

Ahhoz, hogy a kutatók hozzáférjenek a VLOP és VLOSE szolgáltatók online interfészén nyilvánosan hozzáférhetők adatokhoz a DSA 40. cikkének (12) bekezdése alapján, teljesíteniük kell bizonyos feltételeket. Így (i) függetleneknek kell lenniük üzleti érdekektől, (ii) fel kell tárniuk a kutatásuk finanszírozását, és (iii) képeseknek kell lenniük az adatvédelmi és bizalmas adatkezelési követelmények betartására és a személyes adatok védelmére, és e célból megfelelő technikai és szervezési intézkedéseket vezetnek be; (iv) emellett csak olyan adatokat érhetnek el és csak arra az időre, amelyek arányosak és szükségesek a rendszerszintű kockázatok észleléséhez, azonosításához és megértéséhez, ahogy azt a DSA 34. cikk (1) bekezdése meghatározza. Ahhoz, hogy az ilyen kutatók „ellenőrzött kutatóvá" váljanak, és hozzáférjenek a nem nyilvános adatokhoz is a DSA 40. cikk (4) bekezdése alapján, további feltételeket is teljesíteniük kell. Az ilyen kutatóknak (i) kutatóhelyhez kell tartozniuk[336]; (ii) a kutatási tevékenységeiknek a rendszerszintű kockázatok azonosítására vagy a kockázatcsökkentő intézkedések értékelésére kell irányulniuk; továbbá (iii) vallaniuk kell a kutatási eredmények ingyenes nyilvánosságra hozatalát ésszerű időn belül, és figyelemmel a szolgáltatás érintett igénybe vevőinek jogait és érdekeit.

[335] European Centre for Algorithmic Transparency - FAQs: DSA data access for researchers - https://algorithmic-transparency.ec.europa.eu/news/faqs-dsa-data-access-researchers-2023-12-13_en, lehívás: 2024.09.15
[336] A kutatóhely fogalmát az (EU) 2019/790 irányelv 2. cikkének 1. pontja határozza meg.

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[337]. A kutatók adat-hozzáférési kérelmüket benyújthatják vagy ahhoz a tagállami digitális szolgáltatási koordinátorhoz (DSC), amelyhez a kutatószervezetük tartozik, vagy közvetlenül ahhoz a DSC-hez, ahol a VLOP vagy VLOSE szolgáltatója be van jegyezve, amelynek adataihoz hozzáférést kérnek. Mindkét esetben az adat-hozzáférési kérelemről való döntés a VLOP vagy VLOSE szolgáltatójának bejegyzése szerinti DSC hatáskörébe tartozik. Amikor a kutató a „helyi" DSC-hez nyújtja be kérelmét, az a kérelmet és annak kezdeti értékelését továbbítja a bejegyzés szerinti DSC-nek. A letelepedési hely szerinti digitális szolgáltatási koordinátor indokolatlan késedelem nélkül határozatot hoz az ellenőrzött kutatói státusz odaítéléséről. Az érintett szolgáltatók a DSA 40. cikk (5) bekezdése alapján kérhetik a hozzáférési kérelmek módosítását, ha úgy vélik, hogy a kért adatokhoz való hozzáférés aggályokat vet fel. A DSA 97. preambulumbekezdése egyértelművé teszi azonban, 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

[337] European Commission - Delegated Regulation on data access provided for in the Digital Services Act; https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13817-Delegated-Regulation-on-data-access-provided-for-in-the-Digital-Services-Act_en; lehívás: 2024.09.15

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.

3.3.3 Aktuális kritikák és hatósági eljárások

A DSA hozzáférésre vonatkozó rendelkezéseit egyes kutatók amiatt kritizálják[338], 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), 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.

Az Európai Adatvédelmi Biztos a DSA véleményében hangsúlyozta, hogy a tudományos kutatás fontos szerepet játszik a demokratikus társadalomban, és az adatvédelmet nem szabad erre való visszaélésként használni felhasználni. Az etikai irányelvek szerint működő ellenőrzött kutatóknak hozzáférést kell biztosítaniuk a szükséges adatokhoz és API-khoz, megfelelő jogi alapon, az arányosság elvének és a megfelelő biztosítékok figyelembevételével. Az Európai Adatvédelmi Biztos javasolta a "szisztematikus kockázatok" és a "társadalmi károk" fogalmainak további tisztázását, mivel ezek kulcsfontosságúak a platformok átláthatósága és a

[338] 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.; https://ssrn.com/abstract=4484052 vagy http://dx.doi.org/10.2139/ssrn.4484052, lehívás: 2024.09.15

közbizalom fenntartása szempontjából. Végezetül, az Európai Adatvédelmi Biztos arra ösztönözte a jogalkotót, hogy támogassák az általános közérdekű kutatásokat, különösen akkor, ha azok nyilvános hozzáférést biztosítanak az API-khoz, és ha a kutatás valóban közérdekű célokat szolgál.

2024. április 5-én az Európai Bizottság kiadott egy jelentést, amely összefoglalja kutatók számára Európában és az Egyesült Államokban jelenleg elérhető platformok adathozzáférési mechanizmusait. A jelentés a személyes adatok védelmével kapcsolatosan feltárja, hogy az egyes platformok hogyan implementálták a kutatók hozzáférését. Számos esetben igazolást kérnek a kutatók adatvédelmi terveivel kapcsolatosan, és olyan kérdéseket tartalmaznak, mint a technikai és szervezeti intézkedések leírása, „erős jelszópolitika" és „hozzáférési naplózás" bevezetése, illetve ki a felelős a GDPR-megfelelésért, illetőleg az etikai irányelvek leírását kérik, amelyek között szerepel a személyes adatok védelme. Néhány hozzáférési mechanizmus megköveteli, hogy a kutatók tanúsítványokat vagy független értékelő jelentését nyújtsa be a kutató, amely igazolja, hogy a kutató szervezete képes teljesíteni az adatbiztonsági és bizalmassági követelményeket.[339]

Számos DSA megsértésével kapcsolatos hatósági eljárás van folyamatban a kutatók hozzáférésével kapcsolatosan. 2024. január 18-án az Európai Bizottság adatkérést[340] küldött 17 VLOP-nak és VLOSE-nak arról, milyen intézkedéseket tettek annak érdekében, hogy megfeleljenek a kutatók számára nyilvánosan elérhető adatokhoz való hozzáférés biztosítására vonatkozó kötelezettségnek. Azóta ezzel kapcsolatosan eljárások indultak az AliExpress[341], a Meta[342] és a TikTok[343] ellen, amelyek mindegyikénél felmerült a gyanú, hogy hiányosságok vannak a kutatók számára a nyilvánosan elérhető adatokhoz való hozzáférés biztosításában és a DSA 40. cikkének való megfelelés tekintetében. Ezt meghaladóan az Európai Bizottság

[339] European Commission - Status Report: Mechanisms for Researcher Access to Online Platform Data; Publication 05 April 2024; p. 7.; https://ec.europa.eu/newsroom/dae/redirection/document/104117; lehívás: 2024.09.15.
[340] Commission sends requests for information to 17 Very Large Online Platforms and Search Engines under the Digital Services Act; Press release, 18 January 2024; https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-17-very-large-online-platforms-and-search-engines-under; lehívás: 2024.09.15
[341] Commission opens formal proceedings against AliExpress under the Digital Services Act; 14 March 2024; https://ec.europa.eu/commission/presscorner/detail/en/IP_24_1485; lehívás: 2024.09.15
[342] Commission sends request for information to Meta under the Digital Services Act, Publication 16 August 2024; https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-2; lehívás: 2024.09.15
[343] Commission opens formal proceedings against TikTok under the Digital Services Act; 19 February 2024 https://ec.europa.eu/commission/presscorner/detail/en/IP_24_926; lehívás: 2024.09.15

előzetes megállapításokat hozott nyilvánosságra az X elleni eljárásban[344], amelyek szerint X nem biztosít hozzáférést nyilvános adataihoz a kutatók számára. Különösen az a megállapítás, hogy X megtiltja a jogosult kutatóknak a nyilvános adatok önálló hozzáférését, például scraping útján, ahogyan azt az általános szerződési feltételeiben rögzíti. Emellett X eljárása az API-n való hozzáférés biztosítására olyan akadályokat állított, amelyek elrettentik a kutatókat kutatási projektjeik megvalósításától, vagy arra kényszerítik őket, hogy aránytalanul magas díjakat fizessenek, ami a DSA megsértésének gyanúját veti fel.

[344]Commission sends preliminary findings to X for breach of the Digital Services Act; 12 July 2024; https://ec.europa.eu/commission/presscorner/detail/en/IP_24_3761; lehívás: 2024.09.15

4. EGYÜTTMŰKÖDÉS, SZANKCIÓK ÉS VÉGREHAJTÁS AZ ADATVÉDELMI REZSIM ÉS 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.

4.1 Az EU adatvédelmi szabályok és a DSA végrehajtásának összehangolása a digitális piacon

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)[345], 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 esetében 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.

4.2 A felügyelet széttagoltságának veszélye

[345] Digitális Szolgáltatások Európai Testülete; https://digital-strategy.ec.europa.eu/hu/policies/dsa-board; legívás: 2024.09.15

A digitális szolgáltatásokról szóló csomagról és az adatstratégiáról szóló, 2021. november 18. napján kibocsátott nyilatkozatában[346] 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

[346] Európai Adatvédelmi Testület - Nyilatkozat a digitális szolgáltatásokról szóló csomagról és az adatstratégiáról - Az elfogadás időpontja: 2021. november 18.; https://www.edpb.europa.eu/system/files/2022-04/edpb_statement_on_the_digital_services_package_and_data_strategy_hu.pdf, lehívás: 2024.09.10

összeegyeztethetetlen módon, és ebből következően jogbizonytalansághoz vezethetnek.[347] 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.[348]

4.3 A lojális együttműködés kötelezettsége – a Bundeskartellamt ügy tanulságai

A DSA és a GDPR (ePrivacy irányelv) együttes alkalmazásával és a hatóságok együttműködésével kapcsolatosan lényeges megállapításokat tartalmaz az Európai Bíróság a Meta Platforms Inc. és társai kontra Bundeskartellamt ügyben hozott 2023-as ítélete. 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 Unió Bíróságának döntése a Bundeskartellamt és a Meta (korábban Facebook) közötti ügyben alapvetően arra vonatkozott, hogy a versenyhatóságok figyelembe vehetik-e a GDPR rendelkezéseit a versenyjogi döntéshozataluk során. A Bundeskartellamt 2019-es döntésében megtiltotta a Metának, hogy a felhasználók hozzájárulása nélkül több forrásból származó adatokat egyesítsen. A Meta fellebbezett e döntés ellen, és az ügy a düsseldorfi Felsőbb Regionális Bíróság elé került, amely előzetes döntéshozatali kérelmet nyújtott be az Európai Unió Bíróságához. A Bíróság ítéletében elismerte, hogy az adatvédelmi felügyeleti hatóságok és a nemzeti versenyhatóságok eltérő feladatköröket látnak el, és saját célokat követnek (ítélet 44. pont). Ugyanakkor a versenyhatóságok vizsgálhatják azt is, hogy egy adott vállalkozás magatartása megfelel-e más normáknak, például a GDPR-nak, amennyiben ez

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

[348] vö. 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, http://dx.doi.org/10.2139/ssrn.4794182; lehívás: 2024.09.10

szükséges a versenyjogi visszaélés megállapításához (lásd ítélet 48. pont). A versenyhatóságok ugyanakkor nem helyettesíthetik az adatvédelmi hatóságokat, és nem vehetik át azok hatásköreit, különösen a GDPR alkalmazása és érvényesítése terén (lásd ítélet 49. pont). Amikor a versenyhatóság szükségesnek tartja, hogy vizsgálja, vajon egy vállalkozás adatkezelési gyakorlata megfelel-e a GDPR-nak, együtt kell működnie az illetékes adatvédelmi felügyeleti hatósággal, hogy biztosítsák a GDPR egységes alkalmazását (ítélet 49. pont). A Bíróság emlékeztetett arra is, hogy a nemzeti hatóságok kötelesek lojálisan együttműködni egymással az EUSZ 4. cikk (3) bekezdésének megfelelően (ítélet 54-59. pontok). A versenyhatóságok nem térhetnek el az adatvédelmi hatóságok vagy bíróságok döntéseitől a GDPR értelmezése tekintetében, de levonhatják saját következtetéseiket a versenyjogi szabályok alkalmazása kapcsán (ítélet 54-59. pontok). Amennyiben a versenyhatóságnak kétségei merülnek fel az adatvédelmi hatóság értékelésével kapcsolatban, konzultálnia kell az érintett hatósággal. Ha a hatóság észszerű időn belül nem válaszol, a versenyhatóság folytathatja saját vizsgálatát (ítélet 54-59. pontok).

A Bíróság döntésének lényege, hogy a versenyhatóság megállapíthatja, hogy egy vállalkozás adatkezelési gyakorlata nem felel meg a GDPR-nak, amennyiben ez szükséges az erőfölénnyel való visszaélés megállapításához. Ugyanakkor ebben az esetben is köteles együttműködni az adatvédelmi hatóságokkal, és nem térhet el azok határozataitól (ítélet 62-63. pontok). Ha kétségek merülnek fel a hatósági döntés hatályával kapcsolatban, konzultálni kell az érintett adatvédelmi hatósággal, és csak észszerű időn belüli válasz hiányában folytathatja a versenyhatóság saját vizsgálatát (ítélet 63. pont).

A Bundeskartellamt ügy megállapításai aggálytalanul alkalmazhatók az adatvédelmi felügyeleti hatóságok és a DSC-k közötti együttműködésre is, figyelemmel arra, hogy sem a GDPR, ePrivacy irányelv, sem a DSA nem rögzít együttműködési mechanizmusokat a DSC-k és az adatvédelmi hatóságok között. Ez a gyakorlatban azt jelenti, hogy DSC-k, amennyiben az adatvédelmi jogszabályok megsértését vizsgálják, nem térhetnek el az adatvédelmi hatóságok döntésétől és megállapításaitól és indokolt esetben ki kell kérni a felügyeleti hatóság állásfoglalását. Figyelemmel az EUMSZ 16. cikkének (2) bekezdésére és az Európai Unió Alapjogi Chartája 8. cikkének (3) bekezdésére, amely előírja, hogy a személyes adatok kezelésének felügyeletét független adatvédelmi hatóságokra kell bízni, a DSC-k ezáltal nem kerülhetik meg az adatvédelmi hatóságokat megillető hatásköröket, ez azonban nem

akadályozza azt, hogy saját önálló hatáskörüket gyakorolják. A Bundeskartellamt ügy gyakorlati alkalmazásával kapcsolatosan a magyar Gazdasági Versenyhivatal Viber ügyében hozott határozat hozható fel példaként, ahol a magyar Versenyhivatal a magyar Nemzeti Adatvédelmi és Információszabadság hatóság állásfoglalását és vele való konzultációt követően hozott kötelezettségvállalás elfogadásával kapcsolatos határozatot[349] és figyelembe vette az Európai Adatvédelmi Testület hozzájárulás vagy fizetési modellekkel kapcsolatos iránymutatását is. Ezzel kapcsolatosan az lehet előremutató, hogy a DSA szoros adatvédelmi kapcsolódásai és kereszthivatkozásai miatt, melyek emiatt az Európai Adatvédelmi Testület és az Európai Adatvédelmi Biztos álláspontja szerint a felügyelet fragmentációjának veszélyével járnak, a DSC-k együttműködési megállapodást kötnek az adatvédelmi felügyeleti hatóságokkal az adatvédelmi jogszabályok egységes alkalmazása tekintetében és figyelembe veszik az európai uniós joggyakorlati fejleményeket.

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.

[349] GVH VJ/6/2020. sz ügy; https://www.gvh.hu/dontesek/versenyhivatali_dontesek/dontesek_2020/vj-62020142; lehívás: 2024.09.15

5. VÉGKÖVETKEZTETÉSEK ÉS SZAKMAI JAVASLATOK

Részletesen bemutatásra került, hogy egyrészt a DSA *lex specialis* szerepet tölt be a GDPR-ral és az ePrivacy irányelv szabályaival szemben, másrészt kiegészíti annak rendelkezéseit. Ezért elemeztük: (1) a platformok szabályozásával kapcsolatos szabályozási igényt; (2) az adatvédelmi jogszabályok és az adatvédelmi alapelvek általános alkalmazását platformokra; (3) azt, hogy a DSA milyen új adatvédelmi követelményeket támaszt platformok részére, ideértve a DSA alkalmazásával összhangban álló adatkezelési jogalapokat, gyermekek védelmét, fogyatékkal élő személyek online platform használatának elősegítését, az online platformok felelősségét; a GDPR és a DSA kapcsolatát a "dark patterns" (manipulatív tervezési minták) tekintetében, és az új adatkezelési tilalmakat, melyeket a DSA új követelményei indokolnak és a kapcsolódó, új adatvédelmi kötelezettségeket, valamint (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 gyermekek 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 érzékeny 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.

Az intézményi együttműködés szempontjából a DSA új intézményi keretet is kialakít, amely a tagállamokban a digitális szolgáltatások koordinátorainak szerepét erősíti, amelyek adatvédelmi szabályozói feladatokat is elláthatnak. Ez az új keret koordinációt igényel a GDPR felügyeleti hatóságai és a DSA koordinátorai között. Az értekezés arra is rámutat, hogy további elemzések szükségesek, különösen a sötét tervezési minták, jogok gyakorlása és intézményi

együttműködés területén a GDPR és a DSA összefüggéseiben, amit a felügyeleti hatóságok, az Európai Adatvédelmi Testület és az Európai Bíróság részéről további részletezés szükséges.

Az európai uniós adatvédelmi szabályozás és a DSA közötti kölcsönhatás vizsgálatakor kulcsfontosságú olyan szakpolitikai ajánlások kidolgozása, amelyek biztosítják, hogy mindkét keretrendszer harmonizált, koherens és képes legyen az adatvédelem fokozására, miközben előmozdítja az átláthatóságot, az elszámoltathatóságot és a felhasználói jogokat a digitális térben. Az alábbiakban szakpolitikai szempontból néhány kulcsfontosságú ajánlásra vonatkozó javaslat található:

i. Az adatvédelmi szabályok és a DSA végrehajtása közötti szinergiák fokozása

- **Az adatvédelmi felügyeleti hatóságok és a digitális szolgáltatási koordinátorok közötti együttműködés és koordináció:** A DSA alapján létrehozott digitális szolgáltatási koordinátoroknak szorosan együtt kell működnie az Európai Adatvédelmi Testülettel és a nemzeti adatvédelmi hatóságokkal annak biztosítása érdekében, hogy a DSA és a GDPR által átfedő felelősségi köröket következetesen kezeljék, különösen akkor, ha a végrehajtási intézkedések adatvédelmi kérdéseket és a DSA betartását egyaránt érintik. Egyértelmű és hivatalos együttműködési csatornák létrehozása szükséges az adatvédelmi hatóságok és a digitális szolgáltatási koordinátorok között annak biztosítása érdekében, hogy mind az adatvédelmi szabályozás, mind pedig a platformok elszámoltathatósága megfelelő módon érvényesüljön. Ezt az együttműködést közös iránymutatásokkal, közös ellenőrzésekkel és információmegosztási mechanizmusokkal lehetne elősegíteni. Koordinációt igényel az adatvédelmi hatóságok és a DSC-k együttes, illetve párhuzamos eljárása, különös figyelemmel a kétszeres eljárás tilalmára is.

- **Az egymást átfedő jogszabályi kötelezettségek pontosítása:** DSA és GDPR / ePrivacy követelmények együttes alkalmazása további tisztázást és iránymutatást igényel. Az EDPB és az Digitális Szolgáltatások Európai Testület közös iránymutatásai segíthetnének a platformokkal szembeni megfelelési elvárások tisztázásában. Ezeknek az iránymutatásoknak ki kell terjedniük a legfontosabb metszéspontokra, például a személyes adatokat tartalmazó tartalom moderálására, az algoritmikus

elszámoltathatóságra és az adatvezérelt szolgáltatások átláthatóságára. A GDPR (például az adatkezeléssel kapcsolatos hozzájárulás) és a DSA (például az algoritmikus döntéshozatal átláthatósága) szerinti kötelezettségek egyértelmű összehangolására van szükség az ellentmondások elkerülése és annak biztosítása érdekében, hogy a platformok mindkét szabályozás elvárásainak egyaránt meg tudjanak felelni. A GDPR és a DSA közötti kölcsönhatásra vonatkozó szakpolitikai ajánlásoknak, útmutatóknak a fokozott átláthatóságot és a felhasználók jogainak védelmét kell előtérbe helyezniük. A kötelezettségek összehangolása döntő fontosságú olyan koherens szabályozási keret fenntartásához, amely mind az adatvédelmet, mind a digitális platformok jogszerű működését szolgálja. Ezek az útmutatók konkrét példákkal és gyakorlati helyzetekkel segíthetnék a platformokat abban, hogy hogyan értelmezzék és alkalmazzák a jogszabályokat és hogyan feleljenek meg a szabályozó hatósági elvárásoknak egyidejűleg. A szabályozási harmonizációra irányuló erőfeszítéseket kell tenni a kötelezettségek ésszerűsítése érdekében, ahol azok átfedik egymást.

- **Magyarországon** tisztázandó a NAIH szerepe az ePrivacy követelmények alkalmazásával kapcsolatosan és a DSA követelményei alkalmazásával kapcsolatosan megerősített együttműködés kialakítása javasolt a Nemzeti Adatvédelmi és Információszabadság Hatósággal.

ii. Algoritmikus átláthatóság és adatvédelem

A DSA megköveteli, hogy a platformok átláthatóságot biztosítsanak az algoritmikus döntéshozatalról, míg a GDPR a személyes adatok kezelésének átláthatóságára összpontosít. Meg kell követelni a platformoktól, hogy tegyék közzé, hogyan használják fel a személyes adatokat az algoritmusok képzéséhez vagy tartalmi ajánlások készítéséhez, biztosítva, hogy a felhasználók megértsék e rendszerek logikáját és adatvédelmi következményeit. A platformokat kötelezni kell arra, hogy világos és érthető tájékoztatást adjanak az automatizált döntésekről, a profilalkotásról és a személyre szabott tartalomról, beleértve az adatvédelmi megfontolásokat is. További iránymutatás és jó gyakorlatokra vonatkozó ajánlások szükségesek arról, hogy az online platformok a DSA és a GDPR szerinti transzparencia kötelezettségeiknek hogyan tudnak egymást kiegészítve és oly módon eleget tenni, hogy mindkét rezsimnek megfeleljenek.

iii. Koordinált kockázatértékelés és kockázatcsökkentés

A DSA és a GDPR egyaránt hangsúlyozza a kockázatkezelést, így a DSA esetében a rendszerszintű kockázatok kezelését (pl. a jogellenes tartalom terjedése), a GDPR pedig az adatvédelmi kockázatok kockázatarányos kezelését. A kockázatértékelés a DSA szerint a rendszerszintű kockázatokra, míg a GDPR szerinti kötelezettség adatvédelmi hatásvizsgálatra terjed ki és a jogszabály nem tisztázza ezek viszonyát. Ezzel kapcsolatos módszertani útmutató kialakítása egyszerűsítené a megfelelést, és a kockázatcsökkentés holisztikusabb megközelítését ösztönözné.

iv. Tartalom-moderálás és adatvédelem

Amennyiben a (DSA által előírt) tartalommoderálási folyamatok személyes adatokat tartalmaznak, a tartalomeltávolítási folyamatoknak tiszteletben kell tartaniuk az adatvédelmi jogokat, ugyanakkor biztosítani kell a DSA jogellenes tartalom elleni küzdelemre vonatkozó kötelezettségeinek. Ezen a területen kulcsfontosságú olyan hatósági iránymutatások kibocsátása, melyek a paltformok részére legjobb gyakorlatként szolgálhatnak az ezzel kapcsolatos ellentétes érdekek mérlegelésében. Tisztázást igényel, hogy az automatizált eszközök alkalmazása és az önkéntes vizsgálatok milyen adatkezelések, korlátozások és megfigyelések bevezetését teszi lehetővé, ami összhangban van az adatminimalizálás és a célhoz kötöttség követelményével.

v. Adatminimalizálás és célzott hirdetések

A DSA foglalkozik a reklámozás átláthatóságának szükségességével, különösen a profilalkotáson alapuló célzott hirdetések tekintetében. Az ajánlásoknak hangsúlyozniuk kell az e követelmények és a GDPR adatminimalizálásra és célhoz kötöttségre vonatkozó elvei közötti egyértelműbb kapcsolatot. Az adatvédelmi felügyeleti hatóságoknak és a digitális szolgáltatási koordinátoroknak közösen kell ösztönözniük a viselkedési adatokra való kevesebb támaszkodást, és ösztönözniük kell a digitális reklámozás adatvédelmi szempontból kedvezőbb formáit.

vi. Online interfész tervezés és sötét minták

A GDPR és a DSA egyaránt foglalkozik a megtévesztő tervezésen keresztül történő felhasználói manipulációval, az úgynevezett „sötét mintákkal”. Figyelemmel arra, hogy ez a kérdés a fogyasztóvédelmi jogérvényesítést, digitális szolgáltatási koordinátorokat és az adatvédelmi felügyleti hatóságokat egyaránt érinti, biztosítani kell, hogy ezen szereplők joggyakorlata egységes legyen ezen a területen és koordináltan kezeljék ezeket a problémákat.

vii. A felhasználói jogok és jogorvoslati mechanizmusok megerősítése

Mind a DSA, mind pedig a GDPR jogokat állapít meg a felhasználók számára - a GDPR az adatvédelemre, a DSA pedig a jogellenes tartalmakra vonatkozóan. Indokolt lenne egy egységes, felhasználóbarát rendszer létrehozása mindkét rendelet szerinti jogsértésekkel kapcsolatos panaszok benyújtására, biztosítva, hogy a felhasználók jogorvoslatot kérhessenek olyan ügyekben, amelyek mind az adatvédelemmel, mind a platformok DSA szerinti felelősségével kapcsolatosak.

viii. Platformok fokozott elszámoltathatósági intézkedései

A GDPR és a DSA hatálya alá tartozó platformoktól meg kell követelni, hogy a két szabályozásnak való megfelelést fokozott belső elszámoltathatósági mechanizmusok révén bizonyítsák. Ez magában foglalhatná az adatkezelést, az adatvédelmi hatásvizsgálatokat és a DSA tartalmi moderálási szabályainak való megfelelést felügyelő, több funkciót átfogó csoportok kialakítását.

ix. Tudatosító kampányok

A tudatos felhasználói szokások kialakítása érdekében javasolt az egyes felügyeleti hatóságok általi közös tudatosságnövelő kampányok megfontolása mind a felhasználók, mind az online platform üzemeltetők felé, hangsúlyozva az egyes kötelezettségeket és felhasználói jogokat.

6. SUMMARY

The aim of this thesis is to present the relationship between the EU Digital Services Act[350] (DSA) and the EU data protection rules, namely the General Data Protection Regulation[351] (GDPR) and the ePrivacy Directive[352], with a special focus on the operation of online platforms and their obligations and responsibilities regarding the processing of personal data in the context of the DSA.

6.1 THE REGULATORY ISSUES FOR PERSONAL DATA PROCESSING ON DIGITAL PLATFORMS

Digital platforms collect data extensively, in particular by monitoring and profiling user activities and using targeted advertising. Such data processing practices entail significant privacy and data security risks. Tracking users' activities provides platforms with the opportunity not only to gain economic benefits but also to influence user behaviour, raising the risk of abuse and manipulation. This is particularly important for political communication and the spread of fake news, which can influence electoral processes and the shaping of public opinion. Self-regulation has failed in this area, requiring the European legislator to strictly regulate the activities of platforms in relation to the processing of personal data, or to lay down specific rules for intermediary service providers in the field of digital services. The DSA aims to modernise the liability regime for online platforms, in particular the treatment of illegal content, content hosting and the protection of users' rights in this respect. In this context, questions arise as to how EU data protection rules should be applied in the context of the DSA and what the implications of the application of the DSA are for the data protection rights of the users concerned, and what the consequences of regulatory overlaps, including enforcement, are.

---

[350] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act); OJ L 277, 27.10.2022, p. 1–102

[351] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance); OJ L 119, 4.5.2016; *p. 1–88*

[352] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); OJ L 201, 31.7.2002, p. 37–47

6.2 The Relationship and Interplay Between EU Data Protection Rules and DSA and Their Application to Digital Platforms

Since the European Union's GDPR became applicable in 2018, it provides a strict data protection framework for the operation of digital platforms. Such service providers, as data controllers or, where applicable, joint controllers, must ensure compliance with data protection principles in relation to the processing of personal data, including the requirements of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, integrity and confidentiality, accountability and respect for the rights of the data subject. In comparison, the ePrivacy Directive sets out specific rules for the online space, including the storage of and access to data on users' devices, such as the use of cookies and tracking devices, which complement and clarify the rules of the GDPR.

In comparison, the provisions of the DSA complement the EU data protection rules by imposing additional or, in some cases, stricter obligations on intermediary service providers covered by the DSA, but without affecting the data subjects' rights under the data protection rules and without undermining the application of the data protection rules. The DSA contains several references to the processing of personal data and the GDPR rules. These references can be grouped around different topics, such as the relationship between the GDPR, the ePrivacy Directive and the DSA; profiling and restrictions on targeted advertising; provisions on the protection of minors; data access and research; risk assessment and transparency requirements for very large online platforms; or notice and action mechanisms. From this perspective, the thesis presents how the application of these rules interplay with EU data protection rules and how the DSA complements the application of EU data protection rules, with a special focus on lawful processing, liability and specific data protection obligations under certain DSA rules, and also covering the issue of institutional cooperation.

6.3 The Role of Lawful Processing in the DSA

The DSA has a significant impact on data processing practices, as the obligations contained in the DSA affect the legal basis on which service providers can rely to process personal data. The legal basis for consent plays an important role in the context of the use of targeted advertising. The information requirements for online advertising do not affect the relevant provisions of the

GDPR, including consent and the rules on automated decision-making. The DSA imposes strict restrictions on the processing of special categories of personal data, as the DSA prohibits the processing of such data by online platforms for the purpose of targeted advertising based on profiling. In the case of minors, the DSA also restricts the use of consent by online platform providers to display profiling-based advertisements using the data of service users. Beyond this, the DSA sets out several data processing obligations that are mandatory data processing activities, i.e. they require platforms to process users' data in certain situations, such as when taking action against unlawful content, and therefore have no discretion over the processing of personal data.

6.4 Liability and Immunity for Breach of Data Protection Rules Under the DSA

The liability of online platforms varies depending on whether it is a liability for a breach of data protection rules or a breach of the DSA, or whether it is a breach committed by the online platform in relation to the activities carried out by the platforms or by the user of the online platform, where the liability relates to the activities of the users or the illegal content uploaded.

An online platform is liable for a breach of data protection rules when the platform itself processes the data and acts as a controller (joint controller) and its processing operations do not comply with the GDPR. Intermediary service providers typically carry out automated processing of content provided by third parties, and the content provider is primarily liable for any related breaches. The DSA and the Hungarian Act on E-Commerce[353] regulate the liability of intermediary service providers, under which they may be exempted if they are not aware of the infringements and their activities remain automatic, technical and passive, or if they deal with the infringing content immediately after becoming aware of it. The DSA does not impose a general monitoring obligation on intermediary service providers, so they are not obliged to monitor content passing through the system, which also has data protection implications, as such measures could disproportionately infringe the data protection rights of the users concerned. However, such a claim against an intermediary service provider may be pursued in court to prevent or stop an individual infringement.

[353] Act CVIII of 2001 on Electronic Commerce and on Information Society Services; Promulgated on 24 December 2001

An area where GDPR and DSA liability may overlap is when providers of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) services fail to comply with their so-called due diligence obligations under the DSA with respect to the processing and protection of personal data, where the DSA requires these providers to identify, assess and mitigate systemic risks.

6.5 Platform-specific Data Protection Obligations Under the DSA

The DSA regulates the handling of illegal content, the conditions for content hosting and clarifies the absence of general monitoring and active fact-finding obligations for service providers and the possibility of voluntary, own-initiative investigations, which is closely linked to the liability and exemption from liability of service providers. The DSA introduces strict obligations for online platforms regarding the transparency of content moderation and use of automated systems. Platforms must provide users with detailed information on the content moderation tools they use, including automated decision-making processes. The provisions of the DSA reinforce users' rights and ensure that content monetisation, automated decision-making processes, online advertising, referral systems are transparent, and lay down specific rules on the protection of minors, the application of data minimisation rules and the use of profiling-based advertising to minors. The DSA states that service providers operating an online platform must not design or operate their online interface in a way that may deceive or manipulate users or distort their decision-making ability. Beyond this, the DSA sets a stricter accountability standard for VLOP and VLOSE operators regarding the processing of personal data, with one important control mechanism being access to data and data access by researchers, the rules for which are set out in the DSA and safeguards for the protection of personal data.

6.6 Institutional Cooperation and Policy Proposals

In terms of institutional cooperation, the DSA also develops a new institutional framework that strengthens the role of Digital Services Coordinators in the Member States, which may also encounter data protection supervision issues. This new framework requires coordination between data protection supervisory authorities and Digital Services Coordinators, taking into account the risk of fragmentation of supervision and considering the decision of the Court of

Justice of the European Union in Case C-252/21[354], which builds on the duty of loyal cooperation in relation to the relationship with data protection supervisory authorities. The thesis also points to the need for further analysis, in particular concerning dark design patterns, exercise of user / data subject rights and institutional cooperation in the context of the GDPR and the DSA. In this context, the thesis makes policy recommendations for synergies, cooperation and coordinated implementation between data protection rules and the application of the DSA.

*****

[354] Judgment of the Court Grand Chamber of 4 July 2023, Meta Platforms and Others General terms of use of a social network, C-252/21 ; 04 July 2023; ECLI:EU:C:2023:537

FORRÁSHIVATKOZÁSOK

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
- Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), Datenschutzrecht. DSGVO mit BDSG (Nomos 2019), 1. Auflage
- Knyrim (Hrsg), Praxishandbuch Datenschutzrecht, 4. Auflage; Manz; 2020
- 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) pp. 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
- Arcangelo Leone de Castris - Types of Platform Transparency: An Analysis of Discourse Around Transparency and Global Digital Platforms; Public Integrity; Published online: 01 Feb 2024; Online: https://doi.org/10.1080/10999922.2024.2304741
- Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. 2021. What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 360, pp. 1–18. https://doi.org/10.1145/3411764.3445610
- 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

- Marta Micheli, Modeling User Personality Traits for Recommender Systems, Conference Paper, January 2023; Conference: CHItaly 2023 - Crossing HCI and AI; Online: https://ceur-ws.org/Vol-3481/paper1.pdf
- 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., 506-510.
- Adam Liber – Tamás Bereczki - The state of web scraping in the EU; 3 July 2024; IAPP publication; https://iapp.org/news/a/the-state-of-web-scraping-in-the-eu
- Liber Ádám - Közvetítő szolgáltatók felelőssége szellemi tulajdon megsértéséért az Európai Unióban, in Iparjogvédelmi és Szerzői Jogi Szemle, 2013. június, pp. 5-42.
- Marc Ivaldi, Nicolas Petit, Selçukhan Ünekbaş - Killer acquisitions in digital markets may be more hype than reality - Centre for Economic Policy Research
- Stewart, Room – Data Protection and Compliance in Context – BCS, 2007
- Anu Bradford, The Brussels Effect: How the European Union Rules the World, Columbia Law School (2019); Online: https://doi.org/10.1093/oso/9780190088583.001.0001
- Lothar Determann's Field Guide to Data Privacy Law – International Privacy Compliance – Fifth Edition – Elgar (2022)

- Russell R. Densmore (Exec. Editor) - Privacy Program Management - Tools for Managing Privacy Within Your Organization – (2019) by the International Association of Privacy Professionals (IAPP)
- Lodder, Arno R., European Union E-Commerce Directive - Article by Article Comments (2017). Guide to European Union Law on E-Commerce, Vol. 4. Update from 2016 (published 2017) of the 2001 (published 2002) version, published in EU Regulation of E-Commerce. A Commentary Elgar Commentaries series, 2017, pp. 15-58., 2.2.2.3; p. 10.SSRN: https://ssrn.com/abstract=1009945

HIVATKOZOTT JOGSZABÁLYOK

- 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, pp. 1–16
- Az Európai Parlament és a Tanács 2001/29/EK irányelve (2001. május 22.) az információs társadalomban a szerzői és szomszédos jogok egyes vonatkozásainak összehangolásáról; HL L 167., 2001.6.22, pp. 10–19.
- Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési adatvédelmi irányelvről. HL L 201, 31.7.2002, pp. 37–47.
- 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, pp. 11–36.
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyek adatainak védelméről és a szabad áramlásáról (Általános Adatvédelmi Rendelet – GDPR). HL L 119, 4.5.2016, pp. 1–88.
- Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatásokról szóló jogszabály (Digital Services Act – DSA). HL L 277, 27.10.2022, pp. 1–102.
- 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, pp. 1–44.
- 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, pp. 1–66.

- 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
- 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
- 270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről
- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (EGT-vonatkozású szöveg), PE/32/2022/REV/2, HL L 333., 2022.12.27., 80—152. o.
- Az Európai Parlament és a Tanács 2004/48/EK irányelve (2004. április 29.) a szellemi tulajdonjogok érvényesítéséről; HL L 157., 2004.4.30, pp. 45–86.
- 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, pp. 22–39;
- European Commission - Delegated Regulation on data access provided for in the Digital Services Act; https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13817-Delegated-Regulation-on-data-access-provided-for-in-the-Digital-Services-Act_en

- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről;
- 2023. évi CIV. törvény az internetes közvetítő szolgáltatások egyes szabályairól

HIVATALOS DOKUMENTUMOK, IRÁNYMUTATÁSOK

- Európai Bizottság - Európa digitális jövőjének alakítása; https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_hu
- European Commission: Shaping Europe's digital future - The Digital Services Act package: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package; https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en;
- Európai nyilatkozat a digitális évtizedben érvényre juttatandó digitális jogokról és elvekről; (2023/C 23/01); https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32023C0123(01)
- EDPS Opinion 3/2018 on online manipulation and personal data; https://www.edps.europa.eu/sites/default/files/publication/18-03-19_online_manipulation_en.pdf
- 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.; https://www.edps.europa.eu/sites/default/files/publication/17-03-14_opinion_digital_content_en_1.pdf
- EDPS Opinion 1/2021 on the Proposal for a Digital Services Act
- Global Privacy Assembly - Montreux (Switzerland), 14th to 16th September 2005, Resolution on the Use of Personal Data for Political Communication; https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Personal-Data-for-Polictical-Communication.pdf
- European Commission - Proposal for an ePrivacy Regulation; https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation
- 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; https://www.acm.nl/system/files/documents/guidelines-dsa-due-diligence-obligations-for-intermediary-services.pdf;

- Európai Adatvédelmi Testület 2/2019 iránymutatása a személyes adatoknak az általános adatvédelmi rendelet 6. cikke (1) bekezdésének b) pontja szerinti kezeléséről az érintettek részére nyújtott online szolgáltatások összefüggésében
- 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; https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf
- Federal Trade Commission - Statement of Commissioner Alvaro M. Bedoya On the 6(b) Report Examining the Data Practices of Social Media and Video Streaming Services; https://www.ftc.gov/system/files/ftc_gov/pdf/bedoya-statement-social-media-6b-report.pdf
- European Commission - Data protection: Commission adopts new rules to ensure stronger enforcement of the GDPR in cross-border cases; https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3609
- 29. cikk szerinti adatvédelmi munkacsoport személyes adat fogalmáról szóló véleménye - 4/2007 szám (WP 136); https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
- Európai Adatvédelmi Testület 5/2019. számú véleménye 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.; https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_hu.pdf
- 29. cikk szerinti adatvédelmi munkacsoport 2010. június 22-i, 2/2010. számú véleménye az online viselkedésalapú reklámról, WP171
- Datenschutzkommission - DSK, Kurzpapier Nr. 16 (Fn. 27), https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf;
- Der Bayerische Landesbeauftragte für den Datenschutz Gemeinsame Verantwortlichkeit Orientierungshilfe; Version 1.0, Stand: 1. Juni 2024; https://www.datenschutz-bayern.de/infothek/OH_Gemeinsame_Verantwortlichkeit.pdf;

- 29. cikk szerinti adatvédelmi munkacsoport 1/2010. számú véleménye az „adatkezelő” és az „adatfeldolgozó” fogalmáról (WP 169); https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_hu.pdf;
- EDPB Guidelines 05/2020 on consent under Regulation 2016/679; https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
- UK ICO - How should we obtain, record and manage consent? - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/how-should-we-obtain-record-and-manage-consent/;
- EDPB Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive; https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf,
- EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them; Version 2.0; Adopted on 14 February 2023; https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_hu
- 29. cikk szerinti adatvédelmi munkacsoport 06/2014. számú véleménye az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról; WP 217; elfogadás időpontja: 2014. április 9.; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf;
- A 29. cikk szerinti adatvédelmi munkacsoport Iránymutatás az (EU) 2016/679 rendelet szerinti átláthatóságról (wp260rev.01); elfogadás időpontja: 2017. november 29. A legutóbbi felülvizsgálat és elfogadás időpontja: 2018. április 11.; https://ec.europa.eu/newsroom/article29/items/622227/en; lehívás: 2024.09.15
- EDPB - Report of the work undertaken by the Cookie Banner Taskforce; Adopted on 17 January 2023
- CNIL - Guide de configuration de la solution Contentsquare exemptée de recueil du consentement (“ Exemption Mode”); https://www.cnil.fr/sites/cnil/files/atoms/files/contentsquare_-_guide_de_configuration_solution_de_mesure_daudience_exemptee.pdf
- European Data Protection Board - Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, under public consultation;

https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en;

- 29. cikk szerinti adatvédelmi munkacsoport keresőprogramokkal kapcsolatos adatvédelmi kérdésekről szóló 1/2008. véleménye
- Irish Data Protection Commission - Do I need consent for analytics cookies? https://www.dataprotection.ie/en/faqs/cookies/do-i-need-consent-analytics-cookies
- Európai Adatvédelmi Testület - 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről 2.0 változat Elfogadás időpontja: 2020. október 20.; https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf;
- AEPD - Artificial Intelligence: Transparency; https://www.aepd.es/en/prensa-y-comunicacion/blog/artificial-intelligence-transparency
- 29. cikk szerinti adatvédelmi munkacsoport - Iránymutatás az (EU) 2016/679 rendelet szerinti átláthatóságról; WP260 rev.01
- European Commission - Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation - Final Report; April 2022
- A Bizottság közleménye – Iránymutatás a belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól szóló 2005/29/EK európai parlamenti és tanácsi irányelv értelmezéséhez és alkalmazásához (EGT-vonatkozású szöveg); C/2021/9320; HL C 526., 2021.12.29, pp. 1–129;
- 29. cikk szerinti adatvédelmi munkacsoport „03/2013. számú vélemény a célhoz kötöttségről". WP 203, 2013. április 2.
- Hinweise der DSK – Datenschutzkonformer Online-Handel mittels Gastzugang (Stand 24. März 2022); https://www.datenschutzkonferenz-online.de/media/dskb/20222604_beschluss_datenminimierung_onlinehandel.pdf;
- 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához; WP251rev.01
- UN Guide on Privacy-Enhancing Technologies for Official Statistics; https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf

- CNIL - #Authentification multifacteur. 28 mars 2024. [Clôturée] Authentification multifacteur : consultation publique de la CNIL sur un projet de recommandation; https://www.cnil.fr/fr/cloturee-authentification-multifacteur-consultation-publique-de-la-cnil-sur-un-projet-de, lehívás: 2024.09.11
- NAIH hatásvizsgálati lista GDPR 35. cikk (4) bekezdés - https://naih.hu/hatasvizsgalati-lista; lehívás 2024. 09. 02
- 29. cikk szerinti adatvédelmi munkacsoport - 3/2010. sz. vélemény az elszámoltathatóságról;
- 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)); https://www.europarl.europa.eu/doceo/document/TA-8-2018-0433_HU.html
- Article 29 Working Party Guidelines on the right to data portability Adopted on 13 December 2016;
- Európai Adatvédelmi Testület - 8/2020. sz. iránymutatás a közösségi média felhasználóinak megcélzásáról 2.0. változat Elfogadás időpontja: 2021. április 13.; https://www.edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_hu_0.pdf;
- 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; https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf;
- Európai Adatvédelmi Testület - A „hozzájárulás vagy fizetés” modelleknek valódi választási lehetőséget kell kínálniuk; https://www.edpb.europa.eu/news/news/2024/edpb-consent-or-pay-models-should-offer-real-choice_hu
- Commission sends request for information to LinkedIn on potentially targeted advertising based on sensitive data under Digital Services Act, 14 March 2024; https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-linkedin-potentially-targeted-advertising-based-sensitive-data; lehívás: 2024.09.15
- Statement by Commissioner Breton on steps announced by LinkedIn to comply with DSA provisions on targeted advertisement; 07 June 2024; https://digital-

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

- European Commission Guidelines for providers of VLOPs and VLOSEs on the mitigation of systemic risks for electoral processes, Publication 26 April 2024; https://digital-strategy.ec.europa.eu/hu/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes
- Supervision of the designated very large online platforms and search engines under DSA; https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses
- DSK - 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 - https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_DSK_Positionspapier%20_Wissenschaftliche_Forschungszwecke.pdf
- European Centre for Algorithmic Transparency - FAQs: DSA data access for researchers - https://algorithmic-transparency.ec.europa.eu/news/faqs-dsa-data-access-researchers-2023-12-13_en
- European Commission - Status Report: Mechanisms for Researcher Access to Online Platform Data; Publication 05 April 2024; https://ec.europa.eu/newsroom/dae/redirection/document/104117
- Európai Adatvédelmi Testület - Nyilatkozat a digitális szolgáltatásokról szóló csomagról és az adatstratégiáról - Az elfogadás időpontja: 2021. november 18.; https://www.edpb.europa.eu/system/files/2022-04/edpb_statement_on_the_digital_services_package_and_data_strategy_hu.pdf

HÍRPORTÁLOK ÉS MÉDIAFORRÁSOK

- FTC conducting inquiry into Reddit's AI data-licensing practices ahead of IPO; 2024. március 21; https://www.cnbc.com/2024/03/15/ftc-investigating-reddit-over-ai-data-licensing-practices-ahead-of-ipo.html
- Véleménybuborék élőben: az emberek többsége alig kerül kapcsolatba más pártállásúakkal - https://telex.hu/belfold/2021/11/02/politikai-homofilia-velemenybuborek-fideszesek-es-ellenzekiek-ismeretsegi-kore-idea-kutatas;
- Az online platformok hatása a demokratikus nyilvánosságra; Kutatási trendek és eredmények; https://onlineplatformok.hu/files/30f0f0a7-34ee-4215-8982-42a14f650251.pdf
- Dipayan Ghosh, Ben Scott - Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You; Time.com; March 19, 2018; https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/;
- Access Now, Raising the alarm: online tracking harms human rights; February 2 2020; https://www.accessnow.org/online-tracking-harms-human-rights/
- Captured states – e-Privacy Regulation victim of a "lobby onslaught" By EDRi · May 23, 2019; https://edri.org/our-work/coe-eprivacy-regulation-victim-of-lobby-onslaught/
- Erion Murati - Airbnb and Uber: two sides of the same coin; Case note to CJEU of 19 December 2019 C-390/18 (AHTOP v. AIRBNB Ireland); September 8, 2020; https://www.medialaws.eu/airbnb-and-uber-two-sides-of-the-same-coin/
- Marc Ivaldi, Nicolas Petit, Selçukhan Ünekbaş - Killer acquisitions in digital markets may be more hype than reality - Centre for Economic Policy Research; 15 Sep 2023 - https://cepr.org/voxeu/columns/killer-acquisitions-digital-markets-may-be-more-hype-reality;
- Aisling Redden: Companies are collecting your personal data. Here's what you need to know; Euronews, https://www.euronews.com/next/2023/08/14/companies-are-collecting-your-personal-data-heres-what-to-know
- Ádám Liber – Tamás Bereczki - The state of web scraping in the EU – IAPP; https://iapp.org/news/a/the-state-of-web-scraping-in-the-eu;

- CNBC: FTC conducting inquiry into Reddit’s AI data-licensing practices ahead of IPO; https://www.cnbc.com/2024/03/15/ftc-investigating-reddit-over-ai-data-licensing-practices-ahead-of-ipo.html
- Irish Council for Civil Liberties - The Biggest Data Breach, ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe - 16 May 2022; https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/
- Bereczki Tamás - Az ENSZ Privacy Enhancing Technologies [PET] útmutatója, https://www.linkedin.com/pulse/az-ensz-privacy-enhancing-technologies-pet-%C3%BAtmutat%C3%B3ja-tamas-bereczki/?trackingId=yXWzcHSsSgaPjqiODlxllA%3D%3D
- 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); https://edri.org/our-work/algorithms-of-trauma-new-case-study-shows-that-facebook-doesnt-give-users-real-control-over-disturbing-surveillance-ads/
- EDRI - Sex, religion and race are advertising taboos, except for power-hungry politicians - By Civil Liberties Union For Europe · May 31, 2023; https://edri.org/our-work/sex-religion-and-race-are-advertising-taboos-except-for-power-hungry-politicians/
- Facebook: Removing Certain Ad Targeting Options and Expanding Our Ad Controls; Announcements; November 9, 2021 https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls
- EDRI - Civil society complaint raises concern that LinkedIn is violating DSA ad targeting restrictions; February 26, 2024; https://edri.org/our-work/civil-society-complaint-raises-concern-that-linkedin-is-violating-dsa-ad-targeting-restrictions/
- Facebook feed recommendations AI system; June 21, 2024; https://transparency.meta.com/features/explaining-ranking/fb-feed-recommendations/;

HIVATKOZOTT DÖNTÉSEK

- Európai Unió Bírósága, 2022. október 20-i Digi ítélet, C-77/21, EU:C:2022:805,
- 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
- Európai Unió Bírósága, C-40/17. sz., Fashion ID kontra Facebook Ireland ügyben 2019. július 29-én hozott ítélet (ECLI:EU:C:2019:629).
- Európai Unió Bírósága, 2024 március 07. sz. ítélet, C-604/22. sz. ügy, az IAB Europe és a Gegevensbeschermingsautoriteit (belga adatvédelmi hatóság) között (ECLI:EU:C:2024:214)
- Európai Unió Bírósága, 2023. december 5-i Nacionalinis visuomenės sveikatos centras ítélet, C-683/21, EU:C:2023:949
- Európai Unió Bírósága 2024. július 11-i Meta Platforms Ireland [Képviseleti kereset] ítélet, C-757/22, EU:C:2024:598;
- Európai Unió Bírósága, C-252/21. sz. ügy, Meta Platforms Inc. & Others v német versenyhatóság (ECLI:EU:C:2023:537);
- Európai Unió Bírósága, 2022. február 24-i Valsts ieņēmumu dienests [Személyes adatok adóügyi célból történő kezelése] EUB ítélet, C-175/20, EU:C:2022:124.
- Európai Unió Bírósága C-673/17. számú, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH ügyben hozott, 2019. október 1-i ítélete (ECLI:EU:C:2019:801)
- CNIL - Délibération de la formation restreinte n°SAN-2021-023 du 31 décembre 2021 concernant les sociétés X et Y; https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840062;
- CNIL - Délibération de la formation restreinte no SAN-2020-013 du 7 décembre 2020 concernant la société X; https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635729;
- Európai Unió Bírósága, 2023. december 7-i SCHUFA Holding [Tartozáselengedés] ítélet, C-26/22 és C-64/22, EU:C:2023:958

- Európai Unió Bírósága, Koninklijke Nederlandse Lawn Tennisbond és az Autoriteit Persoonsgegevens C-621/22. sz. ügyben 2024. október 4. napján meghozott ítélet; ECLI:EU:C:2024:857
- Európai Unió Bírósága 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.
- Nemzeti Adatvédelmi és Információszabadság Hatóság határozata - NAIH-6737-1/2024 (NAIH-2900/2023, NAIH-636/2022, NAIH-9230/2021
- CNIL - Délibération de la formation restreinte n° SAN-2023-003 du 16 mars 2023 concernant la société CITYSCOOT; Mardi 28 mars 2023; https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000047346903; https://www.cnil.fr/en/geolocation-rental-scooters-cityscoot-fined-eu125000
- CNIL - Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019; https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042388179;
- Európai Unió Bírósága, 2014. szeptember 17-i Baltic Agro ítélet, C-3/13, EU:C:2014:2227
- Európai Unió Bírósága, 2019. június 6-i Weil ítélet, C-361/18, EU:C:2019:473, 43. Sarokpontja
- Európai Unió Bírósága, 2024. október 4-i Maximilian Schrems és a Meta Platforms Ireland Ltd ítélet, C-446/21, ECLI:EU:C:2024:834, 76-83. pontok.
- Gazdasági Versenyhivatal - VJ/24-185/2020; 2024. november 27.
- Gazdasági Versenyhivatal - VJ/6/2020.; Viber Media S.á.r.l.; 2024. május 16.
- Európai Unió Bírósága, C-184/20. sz. ügy, OT és a közszolgálati összeférhetetlenség megelőzésével foglalkozó litván főbizottság között (ECLI:EU:C:2022:601)
- Nemzeti Adatvédelmi és Információszabadság Hatóság határozata - NAIH-6737-1/2024. számú határozata
- Európai Unió Bírósága; 2021. június 22-i Latvijas Republikas Saeima [Büntetőpontok] ítélet, C-439/19, EU:C:2021:504,

- Európai Unió Bírósága; 2024. január 30-i Direktor na Glavna direktsia »Natsionalna politsia« pri MVR – Sofia ítélet, C-118/22, EU:C:2024:97
- ODPO - Asiakkaaksi rekisteröitymisen edellyttäminen ja henkilötietojen säilyttäminen ostoksen tekemisen yhteydessä verkkokaupassa - TSV/26/2020 - https://www.finlex.fi/fi/viranomaiset/tsv/2024/20242163
- Európai Unió Bírósága, 2019. október-3-i Eva Glawischnig-Piesczek kontra Facebook Ireland Limited-ítélet C 18/18, EU:C:2019:821
- Európai Unió Bírósága, L'Oréal SA v eBay International AG (Case C-324/09) EU:C:2011:474
- Európai Unió Bírósága, Promusicae-ügy, C-275/06, Productores de Música de España (Promusicae) vs. Telefónica de España SAU. [ECLI:EU:C:2008:54]
- Európai Unió Bírósága, C-461/10. – Bonnier Audio AB és társai v. Perfect Communication Sweden AB [ECLI:EU:C:2012:219] (2012)
- Kúria Pfv.IV. 20.133/2016/5. sz. felülvizsgálati ügyben szültetett ítélete
- Európai Unió Bírósága, C-51-96 and C-191/97 Deliège ügy, ECLI:EU:C:2000:1999
- Európai Unió Bírósága, C-291/13 Sotiris Papasavvas v O Fileleftheros Dimosia Etairia Ltd, 11 September 2014, ECLI: EU:C:201,
- Európai Unió Bírósága, Case 352/85; 26 April 1988. Bond van Adverteerders and others v The Netherlands State; ECLI:EU:C:1988:196.
- Európai Unió Bírósága, C-484/14 Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, 15 September 2016; ECLI:EU:C:2016:689
- Európai Unió Bírósága a C-25/17. számú ügyben hozott 2018. július 10-ei Jehovan todistajat-ítélet, C-25/17, EU:C:2018:551

NYILATKOZAT

Alulírott ezennel kijelentem, hogy a doktori fokozat megszerzése céljából benyújtott értekezésem kizárólag saját, önálló munkám eredménye. A benne található – másoktól származó – nyilvánosságra hozott vagy közzé nem tett gondolatok és adatok eredeti lelőhelyét a hivatkozásokban (lábjegyzetekben), az irodalomjegyzékben, illetve a felhasznált források között hiánytalanul feltüntettem.

Kijelentem továbbá, hogy a benyújtott értekezéssel azonos tartalmú értekezést más egyetemen nem nyújtottam be tudományos fokozat megszerzése céljából.

E kijelentésemet büntetőjogi felelősségem tudatában tettem.

Dátum: Budapest, 2024. november 21.

.....

NYILATKOZAT

Alulírott Dr. Liber Ádám (neptun kód: KRE-UD8BYW) nyilatkozom, hogy állam- és jogtudományi (tudományágban) nincs folyamatban fokozatszerzési eljárásom, illetve fokozatszerzési eljárásra való jelentkezésemet két éven belül nem utasították el, továbbá két éven belül nem volt sikertelenül zárult doktori védésem.

Nyilatkozom tovább, hogy nem állok doktori fokozat visszavonására irányuló eljárás alatt, illetve öt éven belül nem vontak vissza tőlem korábban odaítélt doktori fokozatot.

Dátum: Budapest, 2024. november 21.

.....