DOI: 10.59851/imr.12.2.7 IN MEDIAS RES 2023/2. • 7, 146–168

A személyes adatok üzleti célú megszerzésére alkalmazott „sötét minták” elleni fellépés lehetséges formái

Platformjog és adatvédelem[*]

PUSZTAHELYI RÉKA[**]

A tanulmány célja annak feltárása, hogy az Európai Unió jogalkotása lépést tart-e az online platformokon a személyes adatok üzleti célú megszerzése érdekében alkalmazott ún. sötét mintákkal, azaz a felhasználói felület megtévesztő kialakításával. Míg a platformok üzemeltetőinek az algoritmuson alapuló, személyre szabott, célzott marketingtechnikák használatához minél több (és pontosabb) személyes adatra van szükségük, akár kisebb-nagyobb visszaélések árán is, addig a felhasználók érdeke alapvetően ezen adatok titokban tartásához és a felettük való rendelkezési jog megtartásához fűződik. A digitális piacokról és a digitális szolgáltatásokról szóló rendeletek szigorú gondossági kötelezettségeket írnak elő a kapuőrök és a szolgáltatásközvetítők számára, azonban a megtévesztő tervezési megoldások elleni jogi fellépés szélesebb nézőpontot kíván meg, ezért a jelen írás kiterjeszti a vizsgálatot az adatvédelmi jog egyes kérdéseire és az uniós digitális jog *(digital acquis)* bizonyos vívmányaira is. A bevezetést követő első szakasz a megtévesztő interfészkialakítás jogi fogalmával és kategorizálásával foglalkozik. A második szakasz sorra veszi a digitális szolgáltatásokról szóló és a digitális piacokról szóló rendeletnek a megtévesztő interfésztervezési mintákra vonatkozó rendelkezéseit, különösen tekintettel az adatvédelmi összefüggésekre, és megkísérli feltárni azok hiányosságait. A harmadik szakasz összegyűjti és elemzi a jobb szabályozásra vonatkozó nemzetközi ajánlásokat és javaslatokat a tisztességtelen adatszerzési módszerekkel és a növekvő információs aszimmetriával szemben.

Kulcsszavak: sötét minták, fogyasztói személyes adatok védelme, tájékozott és kifejezett adatkezelési hozzájárulás, platformok, GDPR

Dark Patterns in Online Platforms: Illegal Methods for Retrieving Personal Data and the Possible Remedies

The aim of this study is to explore whether EU legislation is keeping pace with the proliferation of dark patterns, i.e., deceptive user interface design, on online platforms to harvest personal data for commercial purposes. While the platform operators need as much (and accurate) personal data as possible for algorithmic, personalised and targeted marketing techniques, even at the cost of minor or major abuses,

[*] Készült az RRF-2.3.1-21-2022-00013 azonosítószámú „Társadalmi Innovációs Nemzeti Laboratórium” elnevezésű projektben, a Magyarország Helyreállítási és Ellenállóképességi Tervének keretében, az Európai Unió Helyreállítási és Ellenállóképességi Eszközének támogatásával.

[**] Egyetemi docens, Miskolci Egyetem Állam- és Jogtudományi Kar Civilisztikai Tudományok Intézete Polgári Jogi Intézeti Tanszék.

the users' interests are to keep their personal data confidential and to preserve the right to control the access to them. The Digital Markets Act and the Digital Services Act introduce obligations on the platform providers and the intermediaries. However, legal action against deceptive design patterns requires a broader perspective, and in this paper, we extend the analysis to certain aspects of the data protection law and the EU digital acquis.
The first section of this paper deals with the legal concept and categorisation of deceptive interface design. The second section lists the provisions of the Digital Markets Act and Digital Services Act on deceptive interface design patterns, particularly regarding the implications for data protection, and tries to identify their shortcomings. The third section gathers and analyses international recommendations and suggestions for better regulation to counter unfair data retrieval practices and growing information asymmetry.

Keywords: deceptive design patterns, consumer privacy, informed and affirmative consent, platforms, GDPR

1. Bevezetés

A „sötét minták” *(dark patterns)* elnevezést Harry Brignull brit *user experience* dizájner alkotta meg 2010-ben, és azzal egymástól jegyeiben, megjelenési formáiban, működésében és hatásában teljesen eltérő, a technológiával együtt folyamatosan fejlődő online interfészmegoldásokat foglalt egybe.[1] Elsőként gyűjtötte össze és jellemezte ezeket, azért, hogy a fogyasztók széles körében tudatosítsa a vállalatok gyakorlatát. Első rendszerezésében dokumentálta például a *bait and switch* (csalogatás és átverés: a felhasználó egy adott dologra készül, de ehelyett egy másik, általa nem akart esemény történik) és a *confirmshaming* mintát (szégyenérzetre, kényelmetlenségre alapított taktikák, amelyek a felhasználót döntése megmásítására késztetik). Itt kell megjegyeznünk, hogy az utóbbi évek szakirodalmi forrásai a *dark patterns* kifejezés helyett a *deceptive design patterns* (megtévesztő tervezési megoldások) összefoglaló megjelölést,[2] vagy ezzel jellemzően azonos értelemben az egyébként ennél semlegesebb *online choice architecture* elnevezést használják. Az online választási struktúra digitális tervezési-szerkesztési megoldás,[3] annak módja, hogy az információt milyen formában, hogyan prezentálva teszik hozzáférhetővé a felhasználó számára, azaz hogyan formálja a tervező *(choice architect)* azt az online környezetet, amelyben a felhasználók döntéseket hoznak.[4]

---

1 A *pattern* itt programtervezési mintát, azaz újrafelhasználható objektumorientált szoftverelemeket jelöl. Harry Brignull: 90 Percent of Everything. Dark Patterns: Dirty Tricks Designers Use to Make People Do Stuff. *90 Percent of Everything,* 2010. július 8., https://bit.ly/3uGRspC.

2 Maga Brignull is, lásd https://bit.ly/40SMmCV.

3 Lásd például *Online Choice Architecture: How Digital Design Can Harm Competition and Consumers. Discussion paper.* Competition and Market Authority, 2022, https://bit.ly/412BIcY.

4 Richard H. Thaler – Cass R. Sunstein – John P. Balz: Choice Architecture. In Eldar Shafir (szerk.): *The Behavioral Foundations of Public Policy.* Princeton, Princeton University Press, 2013, 428. Van olyan álláspont, amely az online választási struktúrának mint semleges halmaznak csupán egyik alcsoportjaként nevesíti a sötét mintákat, értve ez alatt kifejezetten a felhasználói interfész – szándékosan – félrevezető tervezését, továbbá különválasztva attól az ún. *dark nudge* (a felhasználó érdekével ellentétest döntést könnyítő) és a *sludge* (a felhasználó érdekének megfelelő döntést kifejezetten megnehezítő) technikákat. Vö. *Online Choice Architecture* (3. lj.) 15–16.

Az ilyen tervezési megoldások bevetése szokványosan két célból történhet, ahogyan azt a későbbiekben részletesen kifejtjük: vagy a személyes adat megszerzése, az adatkezeléshez való hozzájárulás kieszközlése vagy fenntartása érdekében (ideértve a cookie-k alkalmazását is), vagy a fogyasztó gazdasági döntéseinek az egyszerű ráhatáson, rábíráson túlmutató manipulálásáért. E két cél szorosan összefügg. Az összegyűjtött személyes adatokat elemzéshez és felhasználói profilalkotáshoz, továbbá analitikai, gépi tanulási és kognitív számítástechnikai technológiák alkalmazásához dolgozzák fel.[5] Azonban a személyes adatok feldolgozására vonatkozó hozzájáruló nyilatkozatok az általános adatvédelmi rendelet (GDPR) rendelkezéseibe ütközhetnek.[6] Az így megszerzett adatok mellett a *big data,* a fogyasztónak a digitális környezetben hagyott lábnyoma, az adatbányászat[7] és a profilalkotás segítségével[8] használhatják ki az egyes fogyasztók észlelésében, döntési folyamatában rejlő hiányosságokat, irracionalitást.[9] Ez különösen igaz az ún. második generációs sötét mintákra, amelyek a fogyasztó személyes gyengeségeit, döntési hibáit is képesek kiaknázni.[10]

A személyes adatokat el lehet adni további felhasználáshoz, különösen adatkezelési platformoknak, adatbrókereknek vagy adatelemző és piackutató cégeknek. Emellett programozott célzott hirdetésekhez is felhasználhatók: a marketingesek számára eladható az a lehetőség – például valós idejű licitálással mikroárverésen keresztül –, hogy bizonyos személyeket a körülöttük felépített profilok alapján célozzanak meg.[11] Az utóbbi években megsokasodó, a jelen munkában részben feldolgozott empirikus tanulmányok és kutatási jelentések a technológia fejlődésével újabb és újabb ilyen praktikákat azonosítanak, miközben azok egyre jobban elterjednek, és

---

5 Giovanni Sartor – Francesca Lagioia – Federico Galli: *Regulating Targeted and Behavioural Advertising in Digital Services. How to Ensure Users' Informed Consent.* 2021. szeptember, https://bit.ly/3sTrFdx, 11.

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

7 A felhasználó, fogyasztó által nyújtott adaton kívül a szolgáltatást nyújtója a platform használata, a tranzakció vagy a szolgáltatás igénybevétele során folyamatosan szerez adatokat az adott felhasználóról. Ezért a személyes adat kategóriáját ki kell terjeszteni minden olyan adatra, amely önmagában vagy más információkkal kombinálva egy személyt vagy egy személyt azonosító vagy azzal összekapcsolható vagy észszerűen összekapcsolható eszközt azonosít, vagy azzal összekapcsolható vagy észszerűen összekapcsolható, és magában foglalhat származtatott adatokat és egyedi állandó azonosítókat is. Lásd American Data Privacy and Protection Act javaslat, https://bit.ly/46rm9ws.

8 Ugyanerre figyelmeztet Gellén Klára: Fogyasztók és vállalkozások az új üzleti modellek és a digitális technológiai környezet promóciós tendenciái tükrében. *Gazdaság és Jog,* 2019/7–8., https://bit.ly/3GqpJMz, 7–12.

9 A 2022. november 28. és 2023. február 20. között lefolytatott társadalmi konzultációról adott jelentés egyik elgondolkodtató megállapítása, hogy fogyasztók 35,9%-a (222-ből 79) a legsúlyosabb problémának azt tartotta, hogy az ingyenes digitális szolgáltatáshoz való hozzáféréshez meg kell osztani a fizetési vagy a hitelkártyaadatokat. A második legsúlyosabb probléma 11,4 százalékkal az volt, hogy a személyes adatokat félrevezető módon használták fel és/vagy a fogyasztók sebezhetőségére vonatkozó információkat használták ki. Vö. Fitness Check of EU Consumer Law on Digital Fairness, https://bit.ly/40Xsz5t, 4–5.

10 Francisco Lupiáñez-Villanueva et al.: *Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation. Final Report.* Publications Office of the European Union, 2022, https://doi.org/10.2838/859030, 29.

11 Sartor–Lagioia–Galli i. m. (5. lj.) 11.

nem csak a jelentős piaci részesedéssel rendelkező óriásplatformokon.[12] A mintákat ugyanis a kisebb weboldal-üzemeltető vállalkozások is fokozatosan átveszik, saját piaci érvényesülésük érdekében.

Az Európai Adatvédelmi Testület (European Data Protection Board, EDPB) megvizsgálta a platformokkal kapcsolatos adatvédelmi problémákat. A közösségimédiaplatform-szolgáltatók által alkalmazott megtévesztő interfészmegoldások körében folytatott kiterjedt kutatás nevesítette az alkalmazott sötét megoldásokat, feltárva azt is, hogy az adott technika a GDPR mely rendelkezéseibe ütközhet, továbbá ennek kiküszöbölésére javaslatokat, jó gyakorlatokat is megfogalmazott.[13] A sötét minták alkalmazására adott szabályozási válaszreakció az uniós jog több területét is érinti. E fellépés magában foglalja egyrészt az adatvédelmi,[14] másrészt a fogyasztóvédelmi jog területére eső, harmadrészt pedig a mesterségesintelligencia-rendszerek alkalmazásával kapcsolatos, jelenleg már hatályos vagy még kidolgozás alatt álló jogszabályok releváns rendelkezéseit is.[15]

A digitális piacokról szóló jogszabály (DMA)[16] és a digitális szolgáltatásokról szóló rendelet (DSA) számos kötelezettséget ír elő a platformszolgáltatók vagy a közvetítők számára a manipulatív vagy megtévesztő gyakorlatok elkerülésére, az online interfészek tervezéséről és kialakításáról pedig külön rendelkezik a DSA 25. cikke. E szabályok áttekintése előtt szükséges röviden kitérni a megtévesztő tervezési megoldásokra, azok meghatározására.

2. A megtévesztő tervezési megoldások definiálhatósága, a jogi fogalomalkotás nehézsége

2.1. A definícióalkotás kérdése

A „sötét minta”, „sötét megoldás” kifejezést általában a digitális felület olyan kialakítására használják, amellyel a fogyasztókat vagy a felhasználókat nem a legjobb érdekeiket szolgáló dönté-

12 Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet) (Digital Services Act, DSA) 33. cikk.

13 EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: How to recognise and avoid them, https://bit.ly/46ywpmL.

14 Elsősorban a GDPR, továbbá 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), az ezt felváltó rendelettervezet: Javaslat, az Európai Parlament és a Tanács Rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről (elektronikus hírközlési adatvédelmi rendelet), valamint a kidolgozás alatt álló Data Act, azaz Javaslat. Az Európai Parlament és a Tanács rendelete a méltányos adathozzáférésre és adatfelhasználásra vonatkozó harmonizált szabályokról (adatmegosztási jogszabály).

15 Kiemelendő itt: Javaslat. Az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról (AI Act javaslat).

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) (Digital Markets Act, DMA).

sek meghozatalára késztetik, e célból őket megtévesztik, kényszerítik vagy manipulálják.[17] Az egyes fogalmi elemeket illetően Arunesh Mathur és szerzőtársai széttartó szakirodalmi álláspontokról számolnak be.[18] Kiemelendő, hogy van olyan megközelítés, amely a manipulatív természettől elválaszthatatlan fogalmi elemként hangsúlyozza a rosszindulatú, kártékony jelleget is, mert ezzel válik az adott megoldás nemcsak etikailag megkérdőjelezhetővé, hanem jogellenessé is.[19] Federico Galli például megjegyzi: „minél öncélúbb és jövedelmezőbb a manipulátor indítéka, és minél jelentősebb a manipulációs kísérlet hatékonysága, annál elítélendőbb a manipuláció, és annál indokoltabb a jogi beavatkozás."[20]

A sötét megoldások jogi szabályozása alapvetően azon a nehezen megragadható kérdésen múlik, hogy mikor lépi át a tervezési megoldás a meggyőzés és a manipuláció határvonalát.[21] A technikák közös sajátossága, hogy megtervezésük a pszichológia és a viselkedéstudományok eredményein alapul, kifejezett céljuk az emberi döntéshozatalban rejlő hiányosságok és torzítások, valamint az emberi kognitív képességek korlátolt volta kihasználása. Fejlesztésük, továbbfejlődésük[22] a felhasználói élmény és a válaszreakciók mérésén, tesztelésen és empirikus kísérleteken alapszik.

A DSA (67) preambulumbekezdése szerint „az online platformok online interfészein megjelenő sötét megoldások olyan gyakorlatok, amelyek akár szándékosan, akár ténylegesen jelentősen torzítják vagy korlátozzák a szolgáltatás igénybe vevőinek azon képességét, hogy önálló és megalapozott döntéseket hozzanak". E preambulumbekezdés arra is figyelmeztet, hogy a megtévesztő megoldások akkor is tiltottak, ha a használatuk egyébként nem kifejezetten visszaélésszerű, tehát nem feltétel, hogy az online platformot üzemeltető szolgáltatónak valóban előnyére váljon.[23]

Az amerikai szövetségi törvényjavaslat, a Deceptive Experience to Online Users Reduction (DETOUR) Act[24] jogellenes magatartásként a felhasználói interfész kialakításával összefüggő tisztességtelen és megtévesztő magatartásokat és gyakorlatokat határozza meg *(unfair and*

---

17 Lupiáñez-Villanueva i. m. (10. lj.) 20.

18 Arunesh Mathur – Jonathan Mayer – Mihir Kshirsagar: What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. *CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 2021. május, https://doi.org/10.1145/3411764.3445610, 1–18.

19 Luiza Jarovsky: *Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness.* 2022, https://bit.ly/3N0x1KP.

20 Federico Galli: AI and Consumer Manipulation: What is the Role of EU Fair Marketing Law? 4(2) *Católica Law Review* (2020), https://doi.org/10.34632/catolicalawreview.2020.9320, 39.

21 Lupiáñez-Villanueva i. m. (10. lj.) 40.

22 Esetleg itt számba véve az alkalmazott mesterséges-intelligencia rendszert is, annak a gépi tanulás révén megvalósuló önfejlesztő képességét.

23 Felhívja erre a figyelmet Jürgen Kühling – Cornelius Sauerborn: „Dark patterns" unter der DSGVO und dem DSA – Neue Herausforderung für die digitale Rechtsordnung — Klassifikation und datenschutzrechtliche Steuerungsvorgaben. 38(4) *Computer und Recht* (2022) 226–235., https://doi.org/10.9785/cr-2022-380409, 233. rn. 37. Itt kell megjegyeznünk, hogy a korábbi szövegváltozatban még ez a további feltétel szerepelt.

24 Mark. R. Warner szenátor által a Kongresszus elé először 2019-ben, majd 2021-ben újra benyújtott javaslat a megtévesztő online gyakorlatok visszaszorítása érdekében. Deceptive Experiences to Online Users Reduction Act, https://bit.ly/3GhS5c4.

deceptive acts and practices relating to the manipulation of user interfaces). Ezek a felület olyan megtervezését, módosítását vagy manipulálását jelentik, amelynek célja vagy alapvető hatása a felhasználói autonómia, döntéshozatal, választás háttérbe szorítása, kiforgatása vagy akadályozása a beleegyezés vagy a felhasználói adatok megszerzése érdekében.[25] Egyes szerzők véleménye szerint ez a megközelítés visszatükröződik a DSA rendelkezéseiben is.[26] Látjuk, hogy mind a DETOUR-javaslat, mind a DSA később elemzendő 25. cikke átfogó jelleggel, a konkrét adatvédelmi és/vagy fogyasztóvédelmi jogsértés vizsgálatától függetlenül állítja fel a tilalmat, az alkalmazott eljárással a szakmai gondosság követelményeit súlyosan sértő, a technológia tisztességtelen kiaknázását jelentő magatartással szemben fellépve.

A definícióalkotást behatárolhatja, hogy melyik jogterület felől közelítünk, amennyiben az adott definíció a kitűzött célt vagy az eredményt is fogalmi elemmé minősíti. Így például az Európai Adatvédelmi Testület szerint a közösségimédia-platformokon alkalmazott félrevezető tervezési megoldások célja az, hogy úgy befolyásolják a felhasználót, hogy nem szándékolt, akaratával ellentétes és/vagy reá nézve potenciálisan hátrányos, káros döntést hozzon meg egyes személyes adatai vonatkozásában. Gyakran olyan választási lehetőség felé irányítják, amely a saját érdekeivel ellentétes, de jól szolgálja a közösségimédia-platform üzemeltetőjéit.[27]

A Data Act javaslata szintén úgy írja körül e technikákat, mint amelyek alkalmasak – különösen a kiszolgáltatott – fogyasztók meggyőzésére, hogy általuk nem szándékolt magatartást tanúsítsanak, és félrevezessék őket azáltal, hogy az adataik megosztásával kapcsolatos döntések felé terelik őket, vagy indokolatlanul torzítják a szolgáltatás felhasználóinak döntéshozatalát oly módon, hogy aláássák és gyengítik autonómiájukat, döntéshozatalukat és választásukat.[28] Ezenkívül a javaslat 6. cikke a felhasználó kérelme nyomán adatokat fogadó harmadik felek kötelezettségeiről is szól: a 2. bekezdés a) pontja értelmében a harmadik fél semmilyen módon nem kényszerítheti, vezetheti félre vagy manipulálhatja a felhasználót – többek között a felhasználói digitális interfészen keresztül sem – a felhasználói autonómia, a döntéshozatal vagy a választás aláásásával vagy gyengítésével.[29]

---

25 S.3330 – 117th Congress (2021–2022), Deceptive Experiences to Online Users Reduction Act (DETOUR Act), https://bit.ly/4a70gpp, 3. szakasz. A szövetségi törvényjavaslat 2023 júliusában újból benyújtásra került, jelen szakasz minimális pontosítást (online szolgáltatás) tartalmaz. Vö. S.2708 DETOUR Act – 117th Congress (2023–2024), https://bit.ly/3Re7QqH.

26 Lásd a későbbiekben részletesen.

27 EDPB Guidelines 03/2022 (13. lj.).

28 Data Act (34) preabulumbekezdés.

29 Itt kell megjegyeznünk, hogy az EDPB és az európai adatvédelmi biztos közös véleményében (02/2022) egyébként azt javasolta, hogy a javaslat 6. cikk (2) bekezdés a) pontja kifejezetten tiltsa az érintettek kényszerítésének, megtévesztésének vagy manipulálásának minden formáját (függetlenül attól, hogy a felhasználó egyben az érintett is), mert a döntéshozatalt befolyásoló tényezők eltérők lehetnek attól függően, hogy a felhasználó egyben az érintett személy (adatalany) is vagy sem.

2.2. Sokszínű sötét minta a digitális környezetben

A jogi szabályozáshoz szükséges definícióalkotást befolyásolja az a körülmény, hogy a manipulatív interfésztervezési megoldások rendkívül sokfélék lehetnek, és a digitális felülettől is függ a kialakításuk és a hatásuk. „Digitális felület" alatt itt nemcsak a vizuális felületet, azaz a számítógépről vagy mobileszközről elérhető weboldalakat vagy a mobilapplikációkat érthetjük, hanem az ember és az online szolgáltató között interakciót biztosító bármely interfész ide sorolandó, akár hangalapú technológiáról van szó,[30] akár virtuális vagy kiterjesztett valóságról[31] vagy metaverzumról. Itt kell megjegyezni, hogy a hagyományos audiovizuális hatások mellett (szöveges, kép- vagy hangüzenet, vagy ezek kombinációja) akár már haptikus hatásokkal (VR-szemüveggel vagy a kontroller rezgésével) is befolyásolható a felhasználó magatartása.[32]

A kialakítás szerint is különbséget tehetünk az egyes megoldások között. Megtévesztő tervezési megoldás lehet egy honlapon az üzenet helye vagy elhelyezésének módja, vizuális megjelenítése, akár statikus az (például kiemelés vastagon szedve, pirossal), akár dinamikus (például vibráló, színváltó szövegek, felugró üzenetek, szöveg vagy kép váltakozása), valamint az üzenetek szöveges tartalma és környezete. Maga a honlap felépítése, menürendszere, struktúrája is vizsgálandó. Ezek közül az emberi észlelést erőteljesen zavaró és a kifejezetten agresszív nyomásgyakorlást, ráhatást eredményező megoldások a befolyásolni kívánt alanyból ellenérzést, védekezést válhatnak ki, emiatt már nem jellemzők a gyakorlatban[33] – a kevésbé transzparens, szofisztikáltabb megoldások léptek előtérbe.

Itt kell megjegyeznünk, hogy noha az eltérő technológia és felhasználási módok miatt a digitális felület eltérő modalitása kihat a sötét technikai megoldásokra,[34] azok hatékonyságára és ebből következően elterjedt voltára, az empirikus kutatások során feltárt működési jellemzők általában nem térnek el egymástól, továbbá az elérendő cél is rendszerint ugyanaz, így például az adatvédelmi nyilatkozatok során bevetett manipulálás. Az online szolgáltató tevékenysége vagy a platform típusa szintén befolyásolja némiképp az adott ágazatban széles körben alkalmazott megoldások egymáshoz viszonyított arányát, de az előfordulásukat nem zárja ki.[35]

---

30 Kentrell Owens et al.: Exploring Deceptive Design Patterns in Voice Interfaces. In *2022 European Symposium on Usable Security (EuroUSEC 2022),* September 29–30, 2022, Karlsruhe, Germany. ACM, New York, 2022, https://doi.org/10.1145/3549015.3554213.

31 Veronika Krauss: Exploring Dark Patterns in XR. In *Proceedings of the 1st Workshop on Novel Challenges of Safety, Security and Privacy in Extended Reality,* CHI Extended Abstracts (CHIEA '22). ACM, 2022, https://bit.ly/3RdlPgi.

32 Xian Wang et al.: The Dark Side of Augmented Reality: Exploring Manipulative Designs in AR. *International Journal of Human–Computer Interaction*, 2023, https://doi.org/10.1080/10447318.2023.2188799.

33 A kifejezetten agresszív sötét mintákkal szemben a felhasználóban, fogyasztóban kiváltott ellenérzést és ezzel összefüggésben a kevésbé szembetűnő tervezési megoldások hatékonyabb voltát bizonyította az alábbi kutatás: Jamie Luguri – Lior J. Strahilevitz: Shining a Light on Dark Patterns. 13(1) *Journal of Legal Analysis* (2012), https://doi.org/10.1093/jla/laaa006, 59–66.

34 Vö. különösen Johanna Gunawan et al.: A Comparative Study of Dark Patterns Across Mobile and Web Modalities. In *Proceedings of the ACM 2021 Conference on Computer-Supported Cooperative Work and Social Computing*, Vol. 5, No. CSCW2, Article 377 (2021. október), https://bit.ly/3N2DAg2.

35 Vö. Lupiáñez-Villanueva i. m. (10. lj.) 46.

A brit verseny- és piacfelügyeleti hatóság (Competition and Markets Authority) az online választási struktúrákat három csoportba sorolta annak alapján, hogy az alapvetően a döntéshez szükséges információ torzítását vagy a döntéshozatal meg nem engedett, közvetlen befolyásolását célozza-e. Ily módon különbséget tett a választási struktúra (*choice structure:* a választási struktúrák megtervezése és prezentálása), a választáshoz szükséges információ (*choice information:* a szolgáltatott információk tartalma és beágyazása) és a választásra gyakorolt nyomásgyakorlás (*choice pressure:* a választásokra gyakorolt közvetett befolyás) csoportja között.[36] Christoph Bösch és szerzőtársai szintén a jogi szabályozás irányából, méghozzá az adatvédelem felől határoztak meg taxációs szempontokat. Ők az adatvédelmet erősítő tervezési megoldások, stratégiák *(minimize, hide, separate, aggregate, inform, control, enforce, demonstrate)* ellentétpárjaiként csoportosítják a sötét mintákat (a *maximize, publish, centralize, preserve, obscure, deny, violate* és *fake* kulcsszavakkal jelölve az egyes kategóriákat).[37] Luiza Jarovsky, szintén adatvédelmi szempontból közelítve a sötét mintákhoz, a tájékozott beleegyezéshez vezető döntéshozatali folyamatban az akaratelhatározás hibáit állítja párhuzamba a nyilatkozat érvénytelenségét eredményező akarathibák esetköreivel, vizsgálva azok jogellenes befolyásolása árnyalatait.[38] Jarovsky az európai szerződési jogi alapelvek (PECL) érvénytelenségi okait (tévedés, megtévesztés, fenyegetés és aránytalan vagy tisztességtelen előny) úgy alakította át, hogy megfeleljenek az adatsértést eredményező tipikus sötét mintáknak. Ezek alapján azonosította a félretájékoztatás, a félrevezetés, a nyomásgyakorlás és az akadályozottság csoportjait.[39]

2.3. Meggyőzés vagy manipuláció?

Annak szemléltetésére, hogy mikortól számít egy megoldás jogellenesnek, vegyük a leggyakoribb kereskedelmi üzenet, a reklám etikai elveit. Részben – ahogyan Pázmándi Kinga is rögzíti – a reklámok tisztessége és etikussága felett (ágazatspecifikusan) a reklámszakma önkorlátozó hajlandóságára alapított, önkéntes alávetéssel létrehozott szaketikai normarendszer is őrködik.[40] Egy reklám akkor tisztességes, ha megfelel a gazdasági versenyben általában elfogadott tisztességes piaci magatartás erkölcsi és jogi szabályainak.[41] A jogi szabályozásban azonban már versenyjogi, fogyasztóvédelmi, és a legújabb korban médiaspecifikus, közjogi szempontok is megjelennek.[42]

A reklámot a szakmai gondosság követelményeinek megtartásával és társadalmi felelősségérzettel kell elkészíteni,[43] és az nem vezethet a fogyasztók megtévesztésére. Az így elkészített

36 Competition and Markets Authority i. m. (4. lj.) v.

37 Christoph Bösch et al.: Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies Symposium,* 2016/4., 237–254., https://doi.org/10.1515/popets-2016-0038.

38 Jarovsky i. m. (19. lj.).

39 Uo.

40 Pázmándi Kinga: Médiatartalmak forradalma és a „marketingjog” – újkori fogyasztóvédelem a digitális médiapiacon. *Gazdaság és Jog,* 2021/11–12., https://bit.ly/3R3o58J, 2–6.

41 Az Önszabályozó Reklám Testület Magyar Reklámetikai Kódexe 3. cikk, Alapelvek, https://bit.ly/49R0DnH.

42 Pázmándi Kinga: *A reklám a tisztességtelen verseny elleni jog és a modern reklámjog határán.* PhD-disszertáció, Miskolc, Miskolci Egyetem, 2005, 24.

43 Uo.

reklám tájékoztató és meggyőző funkciója tényeken és érzelmi érveken alapul, a manipulatív célú reklám viszont átlépi ezeket a korlátokat, mert a megtévesztés vagy a tisztességtelen nyomásgyakorlás eszközével törekszik célt érni a reklámozó. Az ezzel szemben támasztott jogi tilalmak és abszolút korlátok közé sorolhatók például a reklámtörvény egyes rendelkezései, így a szerencsejáték népszerűsítése vagy a temetkezési szolgáltatások reklámozására vonatkozó korlátok.[44] A szakmai gondosság és tisztességes eljárás elvei mentén párhuzam vonható a tudatosan nem észlelhető reklám[45] és a sötét minták tudatosan nem észlelhető befolyásoló hatása között.[46] Erre tekintettel egyetérthetünk Francisco Lupiáñez-Villanueva és szerzőtársai álláspontjával, amely szerint a manipulatív jelleg megállapítható akkor, ha 1. a szándék valakinek a feltételezett vagy ismert érdeke ellen irányul; 2. az igazság elferdítésével vagy elhallgatásával jár, és 3. az egyén szabad választási lehetőségét megszünteti vagy csökkenti.[47] Daniel Susser hasonlóképpen jellemzi a manipulatív technikákat: ezek tudatosan elrejtettek, a kognitív, az érzelmi vagy a döntéshozatali folyamatot befolyásoló egyéb további sérülékenység kihasználására irányulnak és célzottak.[48]

2.4. Hogyan képesek manipulálni a piszkos technikák?

Általában igaz, hogy az emberi döntéshozatalt behatárolják az ember kognitív képességei, és hogy az az információgyűjtési és -feldolgozási készség és képesség függvénye. Daniel Kahnemann rendszere alapján azt mondhatjuk,[49] hogy a sötét technikák gyors (prompt, intuitív) gondolkodásra és döntéshozatalra ösztönöznek, szándékosan kerülve vagy kiküszöbölve a lassú (megfontolt, racionális) gondolkodás és döntéshozatali folyamat mozgásba lendülését. Más magyarázat szerint gyakrabban hozunk az optimális helyett az adott helyzetben kielégítő döntést.[50] Önmagában a digitális környezet és a megváltozott fogyasztói attitűd is ezt indukálja, ami a szerződéskötési folyamat felgyorsítását, automatizációját és az önkiszolgáló megoldások preferálását is jelenti.[51] A fogyasztó szituatív és relatív digitális kiszolgáltatottsága[52] szintén

---

44 Vö. 2008. évi XLVIII. törvény a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól (reklámtörvény) 21–22. §.

45 Uo. 11. §.

46 A kérdés további leágazása a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlatok területére vezet. Vö. 2008. évi XLVII. törvény a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról.

47 Lupiáñez-Villanueva i. m. (10. lj.) 40.

48 Daniel Susser – Beate Roessler – Helen F. Nissenbaum: Online Manipulation: Hidden Influences in a Digital World. 4(1) *Georgetown Law Technology Review* (2019) 1–45., http://dx.doi.org/10.2139/ssrn.3306006.

49 Daniel Kahneman: *Gyors és lassú gondolkodás* (ford. Bányász Réka, Garai Attila). Budapest, HVG Könyvek, 2012.

50 Matthew U. Scherer: Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. 29(2) *Harvard Journal of Law & Technology* (2016) 364.

51 Pusztahelyi Réka – Buskó Tímea: A fogyasztói döntéshozatal (kifürkészhetetlen?) útjai a digitális térben a viselkedéstudományok és a pszichológia tükrében. *Publicationes Universitatis Miskolcinensis Sectio Juridica et Politica,* 2022/2., 329–353. A fogyasztói attitűd változásához lásd The 21st Century Customer: Who Is The Modern Consumer? *awardaroo.io,* 2023. február 7., https://bit.ly/3ST5z5u.

52 A fogyasztó digitális sérülékenységét vizsgáló részletes jelentés készült az európai fogyasztóvédelmi szervezet (BEUC) megbízásából, Natali Helberger et al.: *EU Consumer Protection 2.0 Structural asymmetries in digital*

figyelembe veendő tényező.[53] A véleményünk tehát az, hogy a digitális környezetben az online interfésztechnikákkal való visszaélések célja vagy az, hogy a fogyasztót a minél egyszerűbb, gyorsabb és minél alacsonyabb evolúciós szintű döntési séma alkalmazására szorítsák,[54] vagy hogy valamely döntéstől visszatartsák.

Richard H. Thaler és Cass R. Sunstein 2008-ban megjelent munkája nyomán azt a taktikát,[55] hogy valaki alig észrevehetően hatást fejt ki mások döntésére, viselkedésére, *nudge*-nak nevezzük. Ezek a taktikák azonban nem fosztják meg az embert döntési szabadságától.[56] A transzparens *nudge* technikák mellett léteznek olyan, nem transzparens módszerek is *(sludge, dark nudge),* amelyek a személy automatikus viselkedési szokásait úgy célozzák meg, hogy nem fedik fel sem befolyásoló mivoltukat, sem valódi céljukat.[57] Az online környezet egy további dimenzióval gazdagítja a *nugde*-ok elemzését. Amíg Thaler és Sunstein jellemzően változatlan, statikus *nudge*-okat vizsgált, addig, ahogyan arra korábban is utaltunk, a digitális korban már dinamikus, folyamatosan fejlődő, egyre inkább személyre szabott *nudge* technikákkal kell számolnunk. A mindent átható és általában nem transzparens technikákat Karen Yeung nyomán *hypernudge*-nak nevezzük.[58] Yeung rávilágít arra, hogy bármennyire is szofisztikáltak ezek a rendszerek, és komplex működésükben esetleg megjósolhatatlanok, végeredményben egy előre megtervezett és beágyazott befolyásolási működési mechanizmuson alapulnak. A felhasználóhoz eljutó információk konfigurálásával, ezáltal személyre szabásával, tipikusan adatforrások algoritmussal történő elemzésével a megcélzott személy szokásaira, preferenciáira és érdeklődésére vonatkozó belelátással, amelyek alapján a későbbi döntései megjósolhatók, ezek a befolyásolási technikák úgy csatornázzák be a felhasználó döntéseit, hogy az elsősorban nem a felhasználó, hanem az előre beprogramozott választási struktúra szempontjából legyen előnyös.[59]

Yeung *hypernugde*-ai már a fent említett második generációs megtévesztő technikai megoldások közé sorolhatók. Ezeket Lupiáñez-Villanueva és szerzőtársai hivatkozott tanulmánya olyan adatalapú személyre szabási technikákként jellemzi, amelyeket a hagyományos félrevezető technikákkal szemben sokkal nehezebb beazonosítani és vizsgálni, pontosan az egyéniesített, személyre szabott mivoltukból következően, és így a célcsoportnak akár az egyes egyénig való

consumer markets. Brussels, 2021. március, https://bit.ly/3uDGqBy. Lásd továbbá Natali Helberger et al.: Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability. 45(2) *Journal of Consumer Policy* (2022), https://doi.org/10.1007/s10603-021-09500-5, 175–200.

53 Pusztahelyi Réka – Czibrik Eszter: Online kereskedelmi gyakorlatok tisztességtelensége a Booking.com-döntés tükrében. *Miskolci Jogi Szemle,* 2022/1., 78–96., https://doi.org/10.32980/MJSz.2022.1.1939.

54 Vö. Marosán György: A gazdasági döntés evolúciós elméletének néhány kérdése – a döntési helyzet meta- és utóértékelése mint a döntés alapeleme. *Köz-Gazdaság,* 2011/1., 107–121.

55 Richard H. Thaler – Cass R. Sunstein: *Improving Decisions About Health, Wealth, and Happiness*. New Haven, Yale University Press, 2008.

56 Cass R. Sunstein: Nudging: A Very Short Guide. 37(4) *Journal of Consumer Policy* (2014) 583–588.

57 Pusztahelyi Réka: Az „érzelmes MI” felhasználása az online marketing világában. In Török Bernát – Ződi Zsolt (szerk.): *A mesterséges intelligencia szabályozási kihívásai. Tanulmányok a mesterséges intelligencia és a jog határterületeiről.* Budapest, Ludovika, 2021, 439–464.

58 Karen Yeung: Hypernudge: Big Data as a Mode of Regulation by Design. 20(1) *Information, Communication & Society* (2017) 118–136.

59 Uo.

lebontása miatt.[60] E vonatkozásban is különös jelentőséggel bír a DETOUR Act, mert tilalmazza az online szolgáltatások fogyasztóinak csoportokra történő felosztását viselkedéstudományi vagy pszichológiai célú kísérletek vagy az online szolgáltatás felhasználóinak tanulmányozása céljából, kivéve, ha az az érintett felhasználók tájékozott beleegyezésével történik,[61] hiszen e kísérletek célja a viselkedésalapú, pszichológiailag célzott, akár személyre szabott technikák, interfészmegoldások vagy algoritmusok továbbfejlesztése.

3. A megtévesztő interfésztervezési minták a DMA és a DSA tükrében

3.1. A DMA rendelkezései

A digitális piacokról szóló jogszabály a személyes adatok kezelésének jogszerűsége feltételrendszerét bővíti további szempontokkal, nevezetesen a kapuőröket terhelő kötelezettségekkel,[62] tekintettel arra, hogy a kapuőr van abban a helyzetben, hogy az interfésztervezés felett ellenőrzést gyakoroljon, így meghatározhatja a végfelhasználók által látható választási struktúrát,[63] annak tesztelésével pedig mindinkább a saját érdekeinek megfelelő kialakítást érhet el.[64] A DMA (37) preambulumbekezdése ezért egyrészt a végfelhasználók számára felhasználóbarát megoldás alkalmazását írta elő a tájékozott beleegyezés megszerzéséhez, továbbá a manipulatív technikák alkalmazását általánosságban tiltja:

> A kapuőrök nem tervezhetik, szervezhetik vagy működtethetik az online interfészeiket olyan módon, amely megtéveszti vagy manipulálja a végfelhasználókat, vagy más módon jelentősen befolyásolja vagy korlátozza az önkéntes hozzájárulásuk megadásának lehetőségét. Különösen nem engedhető meg a kapuőröknek az, hogy a végfelhasználókat évente egynél többször ösztönözzék arra, hogy hozzájárulásukat adják ugyanazon adatkezeléshez, amelyhez eredetileg nem járultak hozzá, vagy amelyre vonatkozóan visszavonták a hozzájárulásukat.

A jogszabály 5. cikke értelmében a kapuőr a személyes adatokat nem kezelheti online hirdetési szolgáltatások céljából, nem kapcsolhatja össze más szolgáltatásból eredő adatokkal, azokat nem

---

60 Lupiáñez-Villanueva i. m. (10. lj.) 40.

61 DETOUR Act javaslat 3. szakasz a) cikk 2. bekezdés.

62 A DMA 6. cikk (10) bekezdése értelmében az üzleti felhasználóknak a kapuőr csak akkor köteles vagy jogosult hozzáférést biztosítani a személyes adatokhoz és csak abban az esetben teheti lehetővé azok felhasználását, ha az adatok közvetlen összefüggésben vannak az adott üzleti felhasználó által az érintett alapvető platformszolgáltatáson keresztül kínált termékek vagy szolgáltatások végfelhasználói általi használatával, és ha a végfelhasználók a hozzájárulásuk megadásával beleegyeznek az ilyen adatmegosztásba. Továbbá a 13. cikk (5) bekezdése értelmében a kapuőrnek elő kell segítenie, hogy az üzleti felhasználók a személyes adatok kezeléséhez (gyűjtés, keresztfelhasználás, megosztás) maguk beszerezhessék a szükséges hozzájárulást vagy anonimizált adatokat nyújtson.

63 Itt kell megjegyeznünk, hogy a végelhasználó nemcsak természetes személyt (fogyasztót), hanem jogi személyt is takarhat, az üzleti felhasználó kivételével.

64 Alexandre de Streel et al.: *Making the Digital Markets Act More Resilient and Effective*. CERRE, 2021. május, http://dx.doi.org/10.2139/ssrn.3853991, 55.

használhatja fel egyéb szolgáltatások céljából, és a végfelhasználókat sem léptetheti be a kapuőr más szolgáltatásaiba személyes adatok összekapcsolása céljából, kivéve, ha a végfelhasználó ehhez konkrét választási lehetősége mellett a GDPR szerinti tájékozott beleegyezését adta.[65] A DMA 13. cikk (6) bekezdése értelmében a kapuőr nem ronthatja le az olyan alapvető platformszolgáltatások feltételeit vagy minőségét, amelyeket olyan üzleti felhasználók vagy végfelhasználók részére nyújt, akik élnek a DMA 5., 6. és 7. cikkében megállapított jogokkal vagy választási lehetőségekkel. Továbbá e jogok vagy választási lehetőségek érvényesítését nem nehezítheti meg indokolatlan mértékben, többek között azáltal, hogy a végfelhasználók számára nem semleges módon biztosít választási lehetőséget vagy egyéb módon aláássa a végfelhasználók vagy az üzleti felhasználók autonómiáját, döntéshozatalát vagy szabad választását a felhasználói interfész egészének vagy részének felépítése, kialakítása, funkciója vagy működési módja révén. E kötelezettség megsértése esetén a Bizottság a 20. cikk alapján eljárást indíthat a kapuőr ellen.

A 15. cikk értelmében a profilalkotásra alkalmazott technológiát a kapuőr köteles auditáltatni és a Bizottságnak benyújtani annak auditált leírását,[66] amelyet az továbbít az Európai Adatvédelmi Testületnek. A (72) preambulumbekezdés tükrében azonban úgy tűnik, hogy a személyes adatok kezeléséhez való hozzájárulás körében alkalmazott sablonizált megoldásokra, interfészkialakításokra e kötelező leírás kifejezetten nem terjed ki. Összességében megállapíthatjuk, ahogyan az európai fogyasztóvédelmi szervezet 2022. évi jelentésében is rámutatott, hogy a DMA rendelkezései körében a sötét minták szabályozásának egyetlen célja, hogy a kapuőr ezek segítségével se játszhassa ki a DMA-ban foglalt kötelezettségeit, így e fenti rendelkezéseknek nem célja a „piszkos megoldások” általános tiltása. Mindez természetesen azt is jelenti, hogy a DMA nem zárja ki sem a GDPR, sem a tisztességtelen kereskedelmi gyakorlatokról szóló irányelv alkalmazását.[67]

---

65 E szakasz jelentőségére hívta fel a figyelmet Ződi Zsolt: Az Európai Unió digitális szolgáltatásokról és digitális piacokról szóló új rendelettervezetei. *Gazdaság és Jog,* 2021/1., https://bit.ly/3T9kGrv, 12–14. Vö. DMA 5. cikk (2) bekezdés: „A kapuőr: a) nem kezelheti online hirdetési szolgáltatások nyújtása céljából olyan végfelhasználók személyes adatait, akik a kapuőr alapvető platformszolgáltatásait igénybe vevő harmadik felek szolgáltatásait veszik igénybe; b) a releváns alapvető platformszolgáltatásokból származó személyes adatokat nem kapcsolhatja össze sem az általa nyújtott bármely további alapvető platformszolgáltatásból vagy az általa nyújtott bármely egyéb szolgáltatásból származó személyes adatokkal, sem pedig harmadik fél által nyújtott szolgáltatásokból származó személyes adatokkal; c) a releváns alapvető platformszolgáltatásokból származó személyes adatokat nem használhatja fel általa külön nyújtott egyéb szolgáltatások – például egyéb alapvető platformszolgáltatások – céljára, és fordítva; és d) a végfelhasználókat nem léptetheti be a kapuőr más szolgáltatásaiba személyes adatok összekapcsolása céljából, kivéve, ha a végfelhasználó számára konkrét választási lehetőséget kínáltak fel, és a végfelhasználó az (EU) 2016/679 rendelet 4. cikke 11. pontjának és 7. cikkének értelmében a hozzájárulását adta.”

66 A DMA (72) preambulumbekezdése részletezi ennek az auditált leírásnak a tartalmát: „1) milyen alapon végzik a profilalkotást, beleértve azt is, hogy az (EU) 2016/679 rendelettel összhangban felhasználnak-e személyes adatokat vagy a felhasználói tevékenységből származó adatokat; 2) az adatkezelés módjáról; 3) arról, hogy milyen célból készül a profil és végső soron milyen célra használják; 4) a profilalkotás időtartamáról; 6) az ilyen profilalkotás által a kapuőr szolgáltatásaira gyakorolt hatásról; 7) arról, hogy milyen lépésekre került sor annak érdekében, hogy a végfelhasználók ténylegesen tisztában legyenek az ilyen profilalkotás releváns alkalmazásával; 8) továbbá arról, hogy milyen lépések történtek a végfelhasználók hozzájárulásának beszerzése, valamint a hozzájárulás megtagadásának, illetve visszavonásának a végfelhasználók számára való lehetővé tétele céljából.”

67 *„Dark Patterns” and the EU Consumer Law Acquis. Recommendations for better enforcement and reform.* The European Consumer Organisation (BEUC), 2022, https://bit.ly/3sUqF8X, 11.

3.2. A DSA vonatkozó rendelkezései

A kapcsolódó rendelkezések közül kiemelendő a DSA 25. cikke, amely uniós szinten először rögzít előírásokat kifejezetten a sötét minták elleni fellépés érdekében. Ez a jelentős újítás a 2021. novemberi tanácsi szövegváltozattal került be a rendelkezések közé, amelyet a 2022. januári európai parlamenti állásfoglalás tovább finomított.[68] A cikk így rendelkezik az online interfész tervezéséről és kialakításáról:

> Az online platformot üzemeltető szolgáltatók nem tervezhetik meg, alakíthatják ki vagy üzemeltethetik online interfészeiket oly módon, amely megtéveszti vagy manipulálja a szolgáltatásaikat igénybe vevőket, vagy más módon lényegesen torzítja vagy gyengíti a szolgáltatásaikat igénybe vevők szabad és tájékozott döntéshozatalra való képességét.

A 25. cikk (2) bekezdése azonban e tilalom (és annak következményei) alkalmazását kizárja azokban az esetekben, amikor az adott nem kívánatos gyakorlatra a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlatok tilalmáról szóló irányelv[69] vagy a GDPR az irányadó. E szabályozási átfedést kizáró rendelkezés hátterében az a megfontolás állhat, hogy az adott tervezési megoldás jogellenes voltát alapvetően e két jogterület rendelkezései tükrében szükséges megítélni, ennek viszont logikailag némileg ellentmond az (1) bekezdésben foglalt általános tilalom, valamint az a körülmény, hogy ez a szakasz nem említi az elektronikus hírközlési adatvédelmi irányelvet sem,[70] tehát a feltételezett szabályozási módszer végigvitele sem hibátlan. Itt kell megjegyeznünk, hogy a DSA 4. cikk (2) bekezdése egyébként tételesen felsorolja azokat az uniós jogi aktusokat, amelyek hatályát a rendelet nem érinti; ezek között szerepel az elektronikus hírközlési adatvédelmi irányelv is. Markus Rössel szerint a DSA 25. cikkében megfogalmazott tilalom ezáltal alapvetően a nem kereskedelmi szektorra, valamint a kereskedők vagy a fogyasztók egymás közötti kapcsolataira szorítkozik.[71] A 25. cikkben megfogalmazott tilalom általános jellegét tovább korlátozza, hogy a DSA hatálya a belső piacon nyújtott közvetítő szolgáltatásokra terjed ki, ezáltal kizárólag az itt alkalmazott megtévesztő interfészmegoldásokat kívánja szabályozni.

A 25. cikk (2) bekezdésében foglalt korlátozás azzal a problémával járhat, hogy jelenleg sem a GDPR, sem a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlatokról szóló irányelv – amely a tisztességtelen üzleti gyakorlatok széles körű tiltása révén a sötét mintákra is vonatkozhat – (még) nem alkalmas teljes mértékben az online jogsértések visszaszorítására. Abban az esetben viszont, ha ez a két jogszabály (vagy azok gyakorlata) nagyobb teret engedne a sötét minták elleni fellépésnek, akkor egyes vélemények szerint a (2) bekezdés értelmében a

---

68 Lásd részletesen Kühling–Sauerborn i. m. (23. lj.) 233–234.

69 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 (Irányelv a tisztességtelen kereskedelmi gyakorlatokról).

70 Lásd 14. lj.

71 Markus Rössel: Digital Services Act – Eingehende Analyse und Überprüfung der regulatorischen Neuerungen aus dem Trilog und potentieller Lücken. 54(2) *Zeitschrift für das gesamte Medienrecht. Archiv für Presserecht* (2023) 101.

DSA végrehajtása viszonylag szűk kérdéskörre korlátozódna, például a cookie-khoz való hozzájárulásra.

Véleményünk szerint nem ez lenne a helyes, vagy legalábbis nem az egyetlen célravezető megoldás. A kérdésünk az, hogy a rendelkezésre álló kutatási jelentésekből, tanulmányokból, iránymutatásokból összeállítható-e a listája az olyan megtévesztő interfészmegoldásoknak, amelyek alkalmazása mind az adatvédelem, mind a fogyasztóvédelem (közelebbről a tisztességtelen kereskedelmi gyakorlat tilalma) szempontjából jogellenesnek minősül. Ezáltal az adott megoldás bármely célra irányul is kifejezetten, egy általános, a DSA szerinti tilalomba ütközhet az adott platformszolgáltatás szempontjából, még ha a sötét technikákkal szembeni szabályozás csupán az online közvetítő szolgáltatást nyújtó platformüzemeltetőkre korlátozódik is. Itt kell kitérnünk a szakirodalom azon megállapítására, mely szerint az adatvédelmi szabályok alkalmazásának jelentős korlátja az, hogy elvileg nem irányulnak egyes adatkezelési célok, így például bizonyos szerződéses következmények ellen. Az adatvédelmi jog célja ugyanis a személyes adatok védelméhez való jog biztosítása, nem pedig a szerződések tartalmára vonatkozó átfogó szabályozás. Ezért az olyan sötét minták, amelyeknek az a hatásuk, hogy az egyéneket szerződéskötésre késztetik anélkül, hogy a szükségesnél több adatot szereznének, alapvetően nem tartoznak az adatvédelmi jog hatálya alá.[72]

A 25. cikk (3) bekezdése szerint a Bizottság iránymutatást adhat ki az (1) bekezdés alkalmazásáról konkrét gyakorlatok esetében.[73] A (2) és a (3) bekezdés értelmezése azonban egymástól függ. Az egyik olvasat szerint a (3) bekezdés világít rá arra, hogy a Bizottság konkrét iránymutatása határozza meg, melyek a DSA alkalmazási körébe tartozó jogellenes megoldások, feltéve, hogy azok nem esnek egyébként sem a fogyasztóvédelmi, sem az adatvédelmi jog által tilalmazott kategóriákba, legyen szó akár átmeneti állapotról is.[74] Ennek felel meg Jürgen Kühling és Cornelius Sauberborn álláspontja is, mely szerint indokolatlan a részletes szabályozás és az általános tilalom a DSA körében. Véleményük szerint rugalmas szabályozásra van szükség, és a külön jogszabályi rendelkezések, így a GDPR is, megfelelő mértékű védelmet képesek garantálni, különösen az adatkezelésre vonatkozóan a sötét interfész kialakítások ellen.[75]

A másik lehetséges értelmezés szerint a (3) bekezdés arra mutat rá, hogy a DSA szabályrendszere ezekre az esetekre nem pusztán a jogi tilalmak felállításával reagál és azok megszegését szankcionálja, hanem az ilyen természetű technikai megoldásokat kiküszöbölő műszaki tar-

---

72 Mario Martini et al.: Dark Patterns: Phänomenologie und Antworten der Rechtsordnung. *Zeitschrift für Digitalisierung und Recht,* 2021/1., 58–59.

73 „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; és c) a szolgáltatás megszüntetésére irányuló eljárásnak az előfizetési eljárásnál nehezebbé tétele.”

74 Lásd szintén DMA (63) preambulumbekezdés: „Az üzleti felhasználók és végfelhasználók szabad választásának biztosítása érdekében a kapuőrök számára nem szabad megengedni, hogy szükségtelenül megnehezítsék vagy bonyolulttá tegyék az üzleti felhasználók és a végfelhasználók számára, hogy leiratkozzanak egy alapvető platformszolgáltatásról. A fiók megszüntetése vagy a leiratkozás nem lehet bonyolultabb, mint a fiók létrehozása vagy az ugyanazon szolgáltatásra való előfizetés.”

75 Kühling–Sauerborn i. m. (23. lj.) 234.

talmú szabványok bevezetésére utal,[76] élve a közvetlen technológiaszabályozás módszerével.[77] Ez esetben viszont ellentmondásként értékelhetjük, hogy az önkéntes szabványok kidolgozásáról és végrehajtásáról szóló 44. cikk kifejezetten nem hivatkozik a 25. cikkre. A 31. cikk „Beépített megfelelés a kialakítás által" címszó alatt az online interfész kialakításáról szintén rendelkezik, azonban a további jogszabályi előírások alapján a kereskedőket terhelő követelmények, így a szerződéskötés előtti tájékoztatás, a megfelelés és a termékbiztonságra vonatkozó tájékoztatás szempontjából az adatvédelmi szabályoknak megfelelő beépített megfelelés nem képezi e felsorolás részét, arra ezek szerint nem vonatkozik.

Továbbá, bár több dokumentum is rámutat a platformüzemeltetőket terhelő kockázatértékelés fontosságára, a DSA 34. cikke megfogalmazásából itt sem tűnik ki, hogy az online interfész visszaélésszerű kialakítása ilyen rendszerszintű kockázatokat jelenthetne, még ha a rendelkezésben a védendő értékek között a személyes adatok védelme és a fogyasztók magas szintű védelmét garantáló elv megjelenik is. Ezzel összefüggésben a kockázatcsökkentésről szóló 35. cikk szintén hiányos, bár utal arra, hogy az online óriásplatformot vagy nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak észszerű, arányos és hatékony kockázatcsökkentési intézkedéseket kell tenniük szolgáltatásaik kialakításának, jellemzőinek vagy működésének módosítása érdekében, beleértve online interfészeiket is.

A 37. cikk értelmében az online óriásplatformot vagy nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak – saját költségükre és legalább évente egyszer – független ellenőrzésen kell átesniük, amely felméri többek között azt is, hogy eleget tettek-e a rendelet III. szakaszában szereplő kötelezettségeknek (így a 25. cikkben foglaltaknak is, az online interfész megfelelő kialakítása körében). Elmarasztaló ellenőri vélemény esetén az üzemeltetők kötelesek a nekik címzett ajánlások végrehajtásáról intézkedni és azt egy hónapon belül igazolni.[78] Itt kell megjegyeznünk, hogy amíg a 25. cikk tiltása valamennyi platformra igaz, addig az érvényesülését biztosító további rendelkezések (33–48. cikk) már kizárólag az óriásplatformra és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatókra alkalmazandók. Így felmerül a kérdés, hogy vajon az online interfész kialakítása miatt valóban csak óriásplatformok esetében kell-e a jelen rendelkezéseknek érvényt szerezni. Ugyanígy a 40. cikk („Az adatokhoz való hozzáférés és az adatok vizsgálata") értelmében a szolgáltatók hozzáférést biztosítanak a letelepedési hely szerinti digitális szolgáltatási koordinátornak vagy a Bizottságnak – azok indokolt kérelmére és a kérelemben meghatározott észszerű határidőn belül – a rendeletnek való megfelelés nyomon követéséhez és értékeléséhez szükséges adatokhoz, és azok kérésére ismertetniük kell algoritmikus rendszereik, köztük ajánlórendszereik tervezését, logikáját, működését és tesztelését.

A jogszabály 6. fejezetében az európai és a nemzetközi szabványügyi szervezetek által meghatározott önkéntes szabványokkal kapcsolatban a 44. cikk tartalmaz utalást az interfészekre (és az

---

76 Martin Ebers: Standardizing AI: The Case of the European Commission's Proposal for an 'Artificial Intelligence Act'. In Larry DiMatteo – Cristina Poncibò – Michel Cannarsa (szerk.): *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*. Cambridge, Cambridge University Press, 2022, 321–344., https://doi.org/10.1017/9781009072168.030.

77 Ződi Zsolt: Kódokba zárt jog. Néhány gondolat az új AVMS irányelv kapcsán. *In Medias Res,* 2019/2., https://bit.ly/3Go0NWh, 169–186.

78 DSA 37. cikk (6) bekezdés.

alkalmazásprogram felületeire), viszont – ahogyan arra korábban kitértünk – itt sem csatolja vissza kifejezetten a 25. cikkben foglaltakat, hanem csak a 39. és a 40. cikkben előírt kötelezettségeknek való megfelelés elősegítése érdekében szól ezekről. Még távolabb kerülünk a piszkos technikák elleni fellépés konkrétumaitól a DSA 45. cikkében, amely különösen a jogellenes tartalomra és a rendszerszintű kockázatokra nézve támogatja az uniós szintű önkéntes magatartási kódexek kidolgozását. Ezeknek a rendelkezéseknek egyébként kellő nyomatékot ad a rendelet szankcióeszköztára, a felhasználót megillető kártérítési igénytől[79] az EU-s platformfelügyelet felállításán át a Bizottság által kirótt szankciókig (ideiglenes intézkedés, kötelezettségvállalás, pénzbírság).

3.3. Felaprózódott szabályozási tárgykör helyett az általános tilalom érvényre juttatása – a feltörekvő technológiák tükrében

A DMA és a DSA rendelkezéseit áttekintve megállapíthatjuk, hogy a meg nem engedett adatgyűjtéssel és -kezeléssel kapcsolatos legfontosabb tilalmakat e rendeletek megfogalmazzák. Különösen a DSA esetében igaz azonban, hogy az interfész visszaélésszerű kialakítása vonatkozásában a további alkalmazható rendelkezések nem vagy csak nagyon laza szállal kötődnek a 25. cikk rendelkezéseihez, ami leronthatja e normák (hatékony) alkalmazását. Az online manipulatív interfészmegoldások elleni fellépés a DSA és a DMA tükrében mindezek alapján még nem tűnik hiba- vagy hézagmentesnek. Itt megfogalmazható az a felvetés, hogy az adatvédelmi vagy a más ágazati körre lehatárolt, egymást nem átfedő szabályozás helyett a sötét, manipulatív technológiák mint tisztességtelen tervezési megoldások elleni fellépés öltsön holisztikus jelleget, azaz a DSA-ban biztosított, az online platformszolgáltatókat és az óriásplatform-szolgáltatókat terhelő gondossági kötelezettségek megkövetelése, az önkéntes vagy a kötelező szabványok, a közvetlen technológiaszabályozás, a kockázatelemzés és -kezelés, az önszabályozás lehetősége terjedjen ki valamennyi megtévesztő tervezési megoldásra.

Itt csak utalunk arra, hogy az európai fogyasztóvédelmi szervezet már két éve megfogalmazta az ezzel kapcsolatos aggályait, amikor a DSA, az adatkormányzási rendelet[80] és a mesterséges intelligenciáról szóló jogszabály[81] tervezetei kapcsán azt kívánta feltárni, hogy a fogyasztó digitális sérülékenységével és a sötét mintákkal szembeni fellépés az EU-n belül milyen jogszabályi keretrendszerben valósul meg: a jelenleg rendelkezésre álló fogyasztóvédelmi szabályrendszer területén, vagy inkább ezek az új rendelettervezetek magukhoz vonják e kérdések szabályozását mint a mesterségesintelligencia-rendszerek használatának és a platformgazdaság sajátos problémakörét.[82] A DMA és a DSA fent elemzett rendelkezéseinek tükrében úgy látjuk, továbbra is szükséges, hogy a megtévesztő interfésztervezési megoldásokra mind a fogyasztóvédelmi, mind az adatvédelmi jog konkrét szabályozási válaszokkal reagáljon. Az alábbiakban az adatvédelmi jog fejlesztésének lehetséges irányait vizsgáljuk meg.

---

79 DSA 54. cikk: „A szolgáltatás igénybe vevői jogosultak arra, hogy az uniós és nemzeti joggal összhangban kártérítést kérjenek a közvetítő szolgáltatóktól az e rendelet szerinti kötelezettségek közvetítő szolgáltatók általi megsértése miatt elszenvedett bármely kárért vagy veszteségért.”

80 Javaslat. Az Európai Parlament és a Tanács rendelete az európai adatkormányzásról (Adatkormányzási rendelet).

81 AI Act javaslat (15. lj.).

82 „Dark Patterns” and the EU Consumer Law Acquis (67. lj.).

4. Az adatvédelmi jog továbbfejlesztésére tett lépések

4.1. A GDPR rendelkezéseinek sötét mintákra szabott alkalmazása az EDPB iránymutatása tükrében

Az Európai Adatvédelmi Testület 3/2022 számú iránymutatásában[83] a közösségi médiaplatformokon alkalmazott személyes adatok megszerzését célzó megtévesztő tervezési megoldásokat *(deceptive design patterns)* vizsgálja, rendszerezi és fogalmaz meg azokkal kapcsolatos jó gyakorlatokat. Az iránymutatás az egyes technikai megoldásokat öt felhasználási helyzet köré csoportosítva elemzi: 1. a közösségimédia-felhasználói fiók létesítése; 2. a platform használata folyamán az adatkezeléssel összefüggésben a platform üzemeltetőjét terhelő tájékoztatási kötelezettség teljesítése az adatkezelésről, közös adatkezelésről, az észlelt incidensekről, valamint a felhasználó hozzájárulása és az egyes adatvédelmi beállítások kezelése; 3. az érintett személy jogainak érvényesítése; 4. a közösségimédia-platform funkciói hogyan támasztják alá az érintettek joggyakorlását; 5. a felhasználói fiók megszüntetése (felfüggesztése). Az EDPB az iránymutatás I. mellékletében[84] a megtévesztő megoldásokat megjelenési formájukra/fő működési elvükre tekintettel is kategorizálja, az alábbiak szerint:

A túlterhelés *(overloading)* a felhasználókat kérések, információk, opciók vagy lehetőségek sokasága alá temeti azért, hogy visszatartsa őket a továbblépéstől és rávegye őket bizonyos adatszolgáltatási gyakorlatok megtartására vagy elfogadására. Ide tartozó alkategóriák az újra és újra felugró ablakok, kérések *(continuous prompting),* az adatvédelmi labirintus (*privacy maze,* amely jelentősen megnehezíti, hogy a felhasználó a konkrét adatkezelési beállítást utólag ellenőrizhesse) és a túlságosan sok választási lehetőség felkínálása *(too many options)*.[85]

A következő fő kategóriát az átugrás *(skipping)* képezi: a felhasználói felület vagy a felhasználói útvonal olyan módon történő kialakítása, hogy a felhasználók elfelejtik az adatvédelmi kérdést vagy eleve nem is gondolnak rá. Ide tartozó alkategóriák a *deceptive snugness* és a *look over there*. Az előbbi lényege, hogy alapbeállításként nem az adatvédelmet támogató beállítás szerepel, az utóbbi célja pedig az, hogy az adatvédelmi kérdésekről a figyelmet más, akár teljesen eltérő tárgyúkérdésre terelje át.[86]

A sötét minták harmadik fő kategóriáját a fellelkesítés *(stirring)* képezi, amelynek célja a felhasználók választásának befolyásolása az érzelmeikre való hatással vagy vizuális ösztönzéssel. Az érzelmi befolyásolás *(emotional stirring)* kiaknázhat pozitív és negatív érzéseket egyaránt. A vizuális ösztönzők alkalmazásának célja pedig a felhasználónak a rá nézve kevésbé visszafogott adatvédelmi beállítások választására ösztönzése.[87]

A negyedik fő csoportba az akadályozó megoldások *(obstructing)* tartoznak, amelyek hátráltatják vagy akadályozzák a felhasználót abban, hogy az adatkezelésről információt szerezzen vagy az adatkezeléssel összefüggésben a szándékolt műveleteket végrehajtsa (például hozzájáru-

83 EDPB Guidelines 03/2022 (13. lj.).
84 Uo., 65–71.
85 Uo., 65.
86 Uo., 66.
87 Uo., 67.

lás visszavonása) linkzsákutcák alkalmazásával, a folyamat indokolatlan megnyújtásával vagy félrevezető műveletek segítségével.[88]

Az ötödik csoportba tartozó megoldások a bizonytalanságra építenek *(fickle),* mert a felület kialakítása instabil és következetlen, így megnehezíti a felhasználók számára, hogy megértsék az adatkezelés jellegét, hogy megfelelően döntsenek az adataikkal kapcsolatban és hogy megtalálják a különböző adatvédelmi beállítások helyét. Ide tartozó módszer az információ belső rendszerezettségének, alá-fölé rendeltségének hiánya *(lacking hierarchy),* az idegen szövegkörnyezetbe helyezés *(decontextualising),* az interfész nem konzisztens volta, valamint a nyelvi hiányosságok.[89]

Az utolsó csoportot azok a megtévesztő megoldások képezik, amelyeknél a szolgáltató elrejti az adatvédelemmel összefüggő információkat, az adatkezelésről való rendelkezés lehetőségét, vagy a felhasználókat bizonytalanságban hagyja arra nézve, hogy adataikat miként kezeli és azok felett hogyan gyakorolhatnak ellenőrzést *(left in the dark).* Mindez egymásnak ellentmondó információkkal, homályos megfogalmazással érhető el.[90]

A testület véleményében az egyes technikákhoz rendelten rögzítette, hogy a GDPR mely rendelkezésébe ütközhet az adott megoldás. Összességében megállapítható, hogy az adatkezelés alapelvei közül különös figyelmet érdemel a tisztességes eljárás és a transzparencia követelménye.[91] E generálklauzulák sérelme mellett az interfész megtévesztő kialakításának a tájékozott hozzájárulás feltételeinek hiánya,[92] az érintett jogainak csorbulása (átlátható tájékoztatás, adatok törléséhez való jog stb.),[93] a beépített, illetve az alapértelmezett adatvédelem követelményének[94] a megsértése a leggyakoribb következménye. Az iránymutatás jó gyakorlatok megfogalmazásával is támogatni kívánja a felhasználói interfészek kialakításának GDPR-konform megtervezését és az önkéntes jogkövetést.[95] A fent felsorolt egyes megoldásokra nézve a konkrét alkalmazás körülményeitől függetlenül általános tilalmat nem szab, mert a testület célja nem az volt, hogy adatvédelmi szempontból aggályos feketelistát alkosson.

Érdemes összevetni ezt az ajánlást a DSA 25. cikk (3) bekezdésével, amely szerint bizonyos konkrét felhasználási módozatokra nézve a Bizottság iránymutatást adhat ki: 1. egyes választási lehetőségek kiemelése a szolgáltatás igénybe vevőjének döntésre való felkérésekor; 2. a szolgáltatás igénybe vevőjének ismételt felkérése valamilyen választásra olyan kérdésben, amellyel kapcsolatban már döntést hozott, különösen a felhasználói élményt zavaró felugró ablak alkalmazásával, és 3. a szolgáltatás megszüntetésére irányuló eljárásnak az előfizetési eljárásnál nehezebbé tétele. Felmerül a kérdés, vélelmezhető-e, hogy e piszkos tervezői megoldások súlyosságuknál fogva minden további körülmény vizsgálata nélkül a GDPR rendelkezéseit is sértik. Alapvetően azonban itt is problémát jelent, hogy a DSA alkalmazása a közvetítő szolgáltatást nyújtókra korlátozódik, ilyen értelemben nem általános hatályú norma.

88 Uo., 68.
89 Uo., 69–70.
90 Uo., 70–71.
91 GDPR 5. cikk (1) bekezdés a) pont.
92 GDPR 4. cikk (5) bekezdés és 7. cikk.
93 GDPR 12–23. cikk.
94 GDPR 25. cikk.
95 EDPB Guidelines 03/2022 (13. lj.) II. melléklet, 73–74.

Mindamellett az adatvédelmi jogsértéssel szembeni fellépés eszköztárának ilyen természetű kibővítése közelebb hozhatná a Giovanni Sartor és kutatócsoportja által kidolgozott, alább összegzett reformelképzelés megvalósítását. További kérdésként merül fel, hogy az ún. második generációs sötét minták esetében a jövőben lehetséges lesz-e különválasztani az adat- és a fogyasztóvédelmi vagy akár a platformok szempontjából a felhasználóvédelmi kérdéseket. Az alább vizsgálandó DETOUR Act javaslatának előnye az, hogy meglátásunk szerint ilyen szabályozást vetít előre, de közben nem zárja ki az adatvédelmi szabályok alkalmazását sem.

4.2. Szabályozási reformelképzelések az üzleti célú adatszerzés sötét technikai megoldásai ellen

Sartor és kutatócsoportja az adatok megszerzésére vonatkozóan két szabályozási lehetőséget vázolt fel. Az egyik biztosíthatja azt, hogy a hozzájárulás a lehető legnagyobb mértékben tájékozott és tisztességesen megszerzett legyen. Ezzel szemben a másik elképzelés szerint a hozzájárulás eleve ne legyen érvényesnek tekinthető olyan adatkezelési tevékenységekre, amelyek az egyén vagy a társadalom számára hátrányosak. Véleményük szerint az első megoldás az alábbi intézkedésekkel érhető el:

– adatvédelem-párti alapértelmezések;
– az opciók és az interfészek szabványosítása;
– a hozzájáruláson alapuló adatkezelés körében az adatkezelési célok minél szigorúbb specifikációja és a célhoz kötöttség minél szigorúbb alkalmazása;
– szigorított tájékoztatási kötelezettségek, amelyek nemcsak az előnyökre, hanem a kockázatokra is kiterjednek;
– a hozzájárulások kezelésének előmozdítása a technológiák segítségével;
– az adatvédelmi gyakorlatok elemzéséhez és értékeléséhez, valamint az ezekre való reagáláshoz szükséges eszközök rendelkezésre bocsátása;
– az adatcsere és a szolgáltatások közötti igazságosság felülvizsgálata;
– a hozzájáruláson alapuló jogügyletek közös kezelésének támogatása.[96]

A második megközelítés körében a hozzájárulás érvénytelenségét eredményezné például a hirdetés politikai célja, az adatkezelés alapelveivel ellentétes tevékenységek, az alapvető szolgáltatások vagy bármely szolgáltatás ellentételezéseként való megkövetelése, vagy bármely eset, amelyben az adat egyfajta szolgáltatásként jelenik meg. Ez utóbbi járna a legszigorúbb következményekkel a techóriások által felépített, a szolgáltatás ingyenességét hangsúlyozó üzleti modellre nézve. A hozzájárulással való visszaélés veszélye ugyanis különösen ott súlyos, ahol a hozzájárulást „árucikké" teszik, azaz amikor a hozzájárulást olyan előnyök megszerzése érdekében adják meg, amelyek nem kapcsolódnak ahhoz a feldolgozáshoz, amelyhez a hozzájárulást kérték, ahogyan ez jellemzően a célzott reklámok esetében történik.[97]

[96] Sartor–Lagioia–Galli (5. lj.) 13.
[97] Uo.

4.3. A DETOUR Act és az American Data Privacy and Protection Act javaslatból tükröződő szabályozási koncepció

Bár az elő ízben 2019-ben, majd 2022-ben, aztán 2023-ban ismételten a Kongresszus elé benyújtott DETOUR Act javaslat alapvetően fogyasztóvédelmi indíttatású, az óriásplatformok vonatkozásában megfogalmazott egyes tilalmai érintik az üzleti célú adatszerzés kérdését. Továbbá a javaslat a platform üzemeltetője számára rendszeres közzétételi kötelezettséget ír elő a felhasználók tevékenységén vagy adatain alapuló viselkedési vagy pszichológiai kísérletről vagy kutatásról, azok általános céljáról, eredményeiről.

Itt kell említést tenni arról is, hogy az egyes haladó szövetségi állami adatvédelmi jogszabályokon kívül[98] 2022 folyamán a Kongresszus elé terjesztették az American Data Privacy and Protection Act javaslatát is a szövetségi szintű egységes adatvédelem érdekében. Ebből kiemelendő az a rendelkezés, amely tilalmazza a hozzájárulás megszerzését, ha azt hamis, fiktív, csalárd, tartalmában vagy előadásában félrevezető nyilatkozat felhasználásával vagy a felhasználói felület olyan kialakításával, módosításával vagy manipulálásával szerezték meg vagy kívánták megszerezni, amelynek célja vagy jelentős hatása az észszerűen eljáró személy autonómiájának, döntéshozatali képességének vagy az ilyen hozzájárulás vagy bármely érintett adat megadására vonatkozó döntésének elfedése, elferdítése vagy akadályozása.[99] Ugyanígy a javaslat tilalmazza az érintett személy jogainak gyakorlása vagy a hozzájárulás visszavonása körében alkalmazott hasonló megoldásokat.

5. Összegzés

A DSA 25. cikke átfogó jelleggel, a konkrét adatvédelmi és/vagy fogyasztóvédelmi jogsértés vizsgálatától függetlenül állítja fel a megtévesztő interfésztervezési megoldások alkalmazásával szembeni tilalmat, a szakmai gondosság követelményeit súlyosan sértő, a technológia tisztességtelen kiaknázását jelentő magatartással szemben fellépve. A DSA hatálya azonban kizárólag a digitális szolgáltatások közvetítőire terjed ki, így nem jelent védelmet a más üzemeltetők által alkalmazott ilyen mintákkal szemben. A jogszabály rendelkezései tükrében a megtévesztő interfész kialakításának nem feltétele a szándékosság vagy a felhasználó, a fogyasztó érdekeivel egyértelműen ellentétes kialakítás. A technikai megoldás manipulatív jellege viszont vizsgálandó, ami egyrészt fennáll, ha 1. a szándék valakinek a feltételezett vagy ismert érdeke ellen irányul; vagy 2. az igazság elferdítésével vagy elhallgatásával jár, vagy 3. az egyén szabad választási lehetőségét megszünteti vagy csökkenti. A DSA által biztosított fellépést azonban korlátozhatja az a tény, hogy bár a 25. cikke valamennyi platform esetében hatályos, a szabály érvényesülését

98 California Consumer Privacy Act (Cal. Civ. Code §1798.199.10), módosítja a California Consumer Privacy Act, The California Age-Appropriate Design Code Act (Cal. Civ. Code § 1798.99.28), a Colorado Privacy Act (Colo. Rev. Stat. § 6-1-1301), a Connecticut Data Privacy Act (Public Act No. 22-15). E jogszabályok, módosítások zömében 2023 folyamán léptek hatályba, és nem tekintik megadottnak a sötét minták által megszerzett adatkezelési hozzájárulást.

99 American Data Privacy and Protection Act (7. lj.), 2. szakasz 1/D pont.

biztosító további rendelkezések (33–48. cikk) már kizárólag az óriásplatformokra és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatókra alkalmazandók. Így felmerül a kérdés: vajon az online interfész kialakítása miatt valóban csak az óriásplatformok esetében kell e rendelkezéseknek érvényt szerezni?

A szabály alkalmazási körét tovább korlátozza a DSA 25. cikk (2) bekezdése rendelkezése szerint az a körülmény, hogy a GDPR és a fogyasztóval szembeni tisztességtelen kereskedelmi gyakorlatok tilalmáról szóló jogszabályok hatálya alá tartozó magatartásokra a DSA fenti rendelkezése nem alkalmazható. Más kérdés, hogy a (3) bekezdésre tekintettel a DSA megnyitja a lehetőséget önkéntes szabványok, esetleges önszabályozás útján a megtévesztő minták visszaszorítására, ami véleményünk szerint visszahathat az alkalmazott technikai megoldás jogellenessé minősítésére az adatvédelmi és a fogyasztóvédelmi jogi rendelkezések alkalmazása során is.

Ha összevetjük az Európai Adatvédelmi Testület 3/2022 számú iránymutatásában felsorolt megtévesztő mintákat a DSA 25. cikk (3) bekezdése alapján listázott tervezési megoldásokkal, akkor felmerül annak vélelme, hogy a piszkos megoldások súlyosságuknál fogva, minden további körülmény vizsgálata nélkül, a GDPR rendelkezéseit is sértik, vagyis az ilyen sötét minták manipulatívak és adatvédelmi szempontból jogsértők.

Irodalomjegyzék

„Dark Patterns" and the EU Consumer Law Acquis. Recommendations for better enforcement and reform. The European Consumer Organisation (BEUC), 2022, https://bit.ly/3sUqF8X.

Bösch, Christoph et al.: Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies Symposium,* 2016/4., 237–254. https://doi.org/10.1515/popets-2016-0038

Brignull, Harry: 90 Percent of Everything. Dark Patterns: Dirty Tricks Designers Use to Make People Do Stuff. *90 Percent of Everything,* 2010. július 8., https://bit.ly/3uGRspC.

De Streel, Alexandre et al.: *Making the Digital Markets Act More Resilient and Effective*. CERRE, 2021. május, 1–97. http://dx.doi.org/10.2139/ssrn.3853991

Ebers, Martin: Standardizing AI: The Case of the European Commission's Proposal for an 'Artificial Intelligence Act'. In DiMatteo, Larry – Poncibò, Cristina – Cannarsa, Michel (szerk.): *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*. Cambridge, Cambridge University Press, 2022, 321–344. https://doi.org/10.1017/9781009072168.030

Galli, Federico: AI and Consumer Manipulation: What is the Role of EU Fair Marketing Law? 4(2) *Católica Law Review* (2020) 35–64.https://doi.org/10.34632/catolicalawreview.2020.9320

Gellén Klára: Fogyasztók és vállalkozások az új üzleti modellek és a digitális technológiai környezet promóciós tendenciái tükrében. *Gazdaság és Jog,* 2019/7–8., 7–12., https://bit.ly/3GqpJMz.

Gunawan, Johanna et al.: A Comparative Study of Dark Patterns Across Mobile and Web Modalities. In *Proceedings of the ACM 2021 Conference on Computer-Supported*

Cooperative Work and Social Computing, Vol. 5, No. CSCW2, Article 377 (2021. október), https://bit.ly/3N2DAg2.

Helberger, Natali et al.: *EU Consumer Protection 2.0 Structural asymmetries in digital consumer markets.* Brussels, 2021. március, https://bit.ly/3uDGqBy.

Helberger, Natali et al.: Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability. 45(2) *Journal of Consumer Policy* (2022) 175–200. https://doi.org/10.1007/s10603-021-09500-5

Jarovsky, Luiza: *Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness.* 2022, https://bit.ly/3N0x1KP.

Kahneman, Daniel: *Gyors és lassú gondolkodás* (ford. Bányász Réka, Garai Attila). Budapest, HVG Könyvek, 2012.

Krauss, Veronika: Exploring Dark Patterns in XR. In *Proceedings of the 1st Workshop on Novel Challenges of Safety, Security and Privacy in Extended Reality,* CHI Extended Abstracts (CHIEA '22). ACM, 2022, https://bit.ly/3RdlPgi.

Kühling, Jürgen – Sauerborn, Cornelius: „Dark patterns” unter der DSGVO und dem DSA – Neue Herausforderung für die digitale Rechtsordnung — Klassifikation und datenschutzrechtliche Steuerungsvorgaben. 38(4) *Computer und Recht* (2022) 226–235. https://doi.org/10.9785/cr-2022-380409, 233

Luguri, Jamie – Strahilevitz, Lior J.: Shining a Light on Dark Patterns. 13(1) *Journal of Legal Analysis* (2012) 43–109.
https://doi.org/10.1093/jla/laaa006

Lupiáñez-Villanueva, Francisco et al.: *Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation. Final Report.* Publications Office of the European Union, 2022.
https://doi.org/10.2838/859030

Marosán György: A gazdasági döntés evolúciós elméletének néhány kérdése – a döntési helyzet meta- és utóértékelése mint a döntés alapeleme. Köz-Gazdaság, 2011/1., 107–121.

Martini, Mario et al.: Dark Patterns: Phänomenologie und Antworten der Rechtsordnung. *Zeitschrift für Digitalisierung und Recht,* 2021/1., 47–74.

Mathur, Arunesh – Mayer, Jonathan – Kshirsagar, Mihir: What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. *CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 2021. május, 1–18.
https://doi.org/10.1145/3411764.3445610

Online Choice Architecture: How Digital Design Can Harm Competition and Consumers. Discussion paper. Competition and Market Authority, 2022, https://bit.ly/412BIcY.

Owens, Kentrell et al.: Exploring Deceptive Design Patterns in Voice Interfaces. In *2022 European Symposium on Usable Security (EuroUSEC 2022),* September 29–30, 2022, Karlsruhe, Germany. ACM, New York, 2022.
https://doi.org/10.1145/3549015.3554213

Pázmándi Kinga: *A reklám a tisztességtelen verseny elleni jog és a modern reklámjog határán.* PhD-disszertáció, Miskolc, Miskolci Egyetem, 2005.

Pázmándi Kinga: Médiatartalmak forradalma és a „marketingjog” – újkori fogyasztóvédelem a digitális médiapiacon. *Gazdaság és Jog,* 2021/11–12., 2–6., https://bit.ly/3R3o58J.

Pusztahelyi Réka: Az „érzelmes MI" felhasználása az online marketing világában. In Török Bernát – Ződi Zsolt (szerk.): *A mesterséges intelligencia szabályozási kihívásai. Tanulmányok a mesterséges intelligencia és a jog határterületeiről.* Budapest, Ludovika, 2021, 439–464.

Pusztahelyi Réka – Buskó Tímea: A fogyasztói döntéshozatal (kifürkészhetetlen?) útjai a digitális térben a viselkedéstudományok és a pszichológia tükrében. *Publicationes Universitatis Miskolcinensis Sectio Juridica et Politica,* 2022/2., 329–353.

Pusztahelyi Réka – Czibrik Eszter: Online kereskedelmi gyakorlatok tisztességtelensége a Booking.com-döntés tükrében. *Miskolci Jogi Szemle,* 2022/1., 78–96. https://doi.org/10.32980/MJSz.2022.1.1939

Rössel, Markus: Digital Services Act – Eingehende Analyse und Überprüfung der regulatorischen Neuerungen aus dem Trilog und potentieller Lücken. 54(2) *Zeitschrift für das gesamte Medienrecht. Archiv für Presserecht* (2023) 93–106.

Sartor, Giovanni – Lagioia, Francesca – Galli, Federico: *Regulating Targeted and Behavioural Advertising in Digital Services. How to Ensure Users' Informed Consent.* 2021. szeptember, https://bit.ly/3sTrFdx.

Scherer, Matthew U.: Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. 29(2) *Harvard Journal of Law & Technology* (2016) 353–400.

Sunstein, Cass R.: Nudging: A Very Short Guide. 37(4) *Journal of Consumer Policy* (2014) 583–588.

Susser, Daniel – Roessler, Beate – Nissenbaum, Helen F.: Online Manipulation: Hidden Influences in a Digital World. 4(1) *Georgetown Law Technology Review* (2019) 1–45. http://dx.doi.org/10.2139/ssrn.3306006

Thaler, Richard H. – Sunstein, Cass R.: *Improving Decisions About Health, Wealth, and Happiness*. New Haven, Yale University Press, 2008.

Thaler, Richard H. – Sunstein, Cass R. – Balz, John P.: Choice Architecture. In Shafir, Eldar (szerk.): *The Behavioral Foundations of Public Policy.* Princeton, Princeton University Press, 2013, 428–439.

The 21st Century Customer: Who Is The Modern Consumer? *awardaroo.io,* 2023. február 7., https://bit.ly/3ST5z5u.

Wang, Xian et al.: The Dark Side of Augmented Reality: Exploring Manipulative Designs in AR. *International Journal of Human–Computer Interaction*, 2023. https://doi.org/10.1080/10447318.2023.2188799

Yeung, Karen: Hypernudge: Big Data as a Mode of Regulation by Design. 20(1) *Information, Communication & Society* (2017) 118–136.

Ződi Zsolt: Kódokba zárt jog. Néhány gondolat az új AVMS irányelv kapcsán. *In Medias Res,* 2019/2., 169–186., https://bit.ly/3Go0NWh.

Ződi Zsolt: Az Európai Unió digitális szolgáltatásokról és digitális piacokról szóló új rendelettervezetei. *Gazdaság és Jog,* 2021/1., 12–14., https://bit.ly/3T9kGrv.