SZABÁLYOZÓI CÉLKERESZTBEN A SÖTÉT MEGOLDÁSOK

SZERZŐ: DR. HORVÁTH ANNA ZSÓFIA LL.M (GÖTTINGEN), A CMS BUDAPEST KERESKEDELMI JOGI CSOPORTJÁNAK ÉS TMT CSOPORTJÁNAK ÜGYVÉDJELÖLTJE, ÉS A GEORG AUGUST UNIVERSITÄT GÖTTINGEN PHD HALLGATÓJA, KORÁBBAN AZ EURÓPAI ADATVÉDELMI BIZTOS HIVATALA TECHNOLÓGIAI ÉS ADATVÉDELMI OSZTÁLYÁNAK MUNKATÁRSA.

"A Google egyik csapata nem tudott dönteni két kék szín között, ezért 41 árnyalatot teszteltek az egyes kék színek közül, hogy kiderüljön, melyik teljesít jobban. Nemrégiben vitát folytattam arról, hogy a szegélynek 3, 4 vagy 5 pixel szélesnek kell-e lennie, és megkértek, hogy bizonyítsam be az érveimet "[1].

A megállapítás Douglas Bowmantól, a Google korábbi vizuális megjelenésért felelős tervezőjétől származik, és hűen tükrözi a tudatos tervezés szerepét az online platformok kialakításában. Jelen cikk célja annak bemutatása, hogy mi áll e tervszerűen kialakított design alkalmazása mögött, mekkora jelentősége van ennek a felhasználói döntések meghozatalában, és milyen eszközök állnak a jogalkotó rendelkezésére ennek szabályozására.

1. A sötét megoldások megjelenése

Az emberi gondolkodás folyamatainak megismerésével foglalkozó kognitív pszichológia képviselői viszonylag korán felismerték, hogy a hétköznapi döntéshozatal során az emberek ahelyett, hogy a döntéseik következményeit és azok valószínűségét részletesen mérlegelnék, jellemzően bizonyos beépített „döntéskönnyítő" mechanizmusokat alkalmaznak [2, 3]. Ezek a mechanizmusok kognitív torzításhoz, egyfajta nem tudatos logikai hibához vezetnek, amely lényege, hogy az egyén adott helyzet tényleges értékelése helyett bizonyos gondolkodási sémák alapján jut el egy döntésre [2]. Az egyik leggyakoribb kognitív torzítás a lehorgonyzási torzítás, mely szerint a döntés meghozatal során általában a témában kapott első információ a legmeghatározóbb, a később kapott információ kisebb súllyal esik latba [3], de ilyen például az ún. egyetlen szempontú döntéshozatal, amely szerint az egyén keres egy szempontot, amely alapján a két választási lehetőség megkülönböztethető, és e szempont alapján dönt (például: a zölddel jelölt opció jó, a piros rossz).

Számos kutatás született annak alátámasztására, hogy a megfelelő megjelenés, és a választási lehetőségek prezentálásának körülményei mérhető hatással vannak a felhasználók választásaira, ez pedig ajtót nyitott olyan, kezdetben offline, majd az internet elterjedésével megjelenő online stratégiáknak, amelyek kifejezetten az egyén döntésének fenti módokon történő befolyásolásán alapulnak, például marketing területen reklámokban, vagy pénzügyi befektetésekkel kapcsolatban [3]. Az Európai Bizottság 2022-ben nyilvánosságra hozott riportja több, 3-4 tagállamot lefedő reprezentatív kutatással támasztotta alá, hogy a digitális környezetben alkalmazott sötét megoldások alkalmasak a felhasználók döntéseinek befolyásolására [4].

2. A sötét megoldások fogalom megalkotása és elhatárolási kérdések

A felhasználókat, fogyasztókat érintő fenti gyakorlatot összefoglaló "dark pattern", később „deceptive pattern”, azaz sötét megoldások kifejezést Harry Brignull UX designer használta először 2010-ben, aki a sötét megoldásokat olyan internetes oldalakon és applikációkban alkalmazott trükkökként írta le, amelyek arra késztetik a felhasználót, hogy akkor is egy bizonyos választás, pl. egy termék megvásárlása, vagy szolgáltatásra való feliratkozás mellett döntsön, ha ez egyébként nem állt kifejezett szándékában.

Ugyan máig ez tekinthető a legelterjedtebb meghatározásnak, ezt követően mind a szakirodalomban [3, 5, 6], mind a jogalkotók részéről több absztrakt definíció született. Az Európai Unióban 2022. október 19-én elfogadott, a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról szóló 2022/2065 rendelet (Digital Services Act, "DSA") 67. preambulumbekezdése szerint a 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". A méltányos adathozzáférésre és adatfelhasználásra vonatkozó harmonizált szabályokról szóló adatmegosztási jogszabály („Data Act”) jelenleg jogalkotási fázisban lévő tervezetének meghatározása szerint a sötét megoldások „olyan webszerkesztési technikák, amelyek a fogyasztókat megtévesztő módon számukra hátrányos következményekkel járó, nem kívánt döntések felé terelik”. Az Európai Adatvédelmi Testület ("EDPB") a sötét megoldásokat adatvédelmi szempontból, és kizárólag a közösségi médiaplatformokon megvalósított "megtévesztő tervezési mintákként" definiálja,amelyek olyan, felhasználói felületeket és felhasználói utakat jelentenek,

amelyek „akaratlan és potenciálisan káros döntések meghozatalára sarkallják a felhasználókat, gyakran olyan döntésre, amely a felhasználók érdekeivel ellentétes, ellenben a közösségi médiaplatformok érdekeit szolgálja a felhasználók személyes adatainak kezelésével kapcsolatban” [7].

A fenti meghatározások két közös eleme, hogy a sötét mintázatok (i) a felhasználó számára tudatosan nem érzékelhető befolyásoló tényezők, és (ii) a felhasználókra nézve valamilyen negatív hatást váltanak ki. Attól függően, hogy ez a két jellemző hogyan valósul meg, a sötét megoldások lehetnek az elérhető információt és információáramlást befolyásoló, vagy a felhasználó döntési folyamatát befolyásoló sötétmegoldások. Előbbire tipikus példa a megtévesztő megjelenés vagy tartalom, ahol a dizájn szándékosan egy dologra irányítja a figyelmet, pl. harsányabb színekkel, az elfogadás, vásárlás gomb nagyobb, zöld, továbblépés vagy elutasítás nehezen kivehető, kisebb gomb. Cookie-hozzájárulásnál személyre szabható cookie beállítások megerősítésekor az ’összes elfogadása’ zöld színnel, a ’beállítások elfogadása’ szürke színnel szerepel. Ilyen továbbá a „kosárba csempészés”, ahol a vásárlási folyamat során a webhely egy további terméket ad hozzá (pl. pluszbiztosítás jegyfoglaláskor úgy kerül a kosárba, hogy a „Választ utasbiztosítást?” kérdésre a „nem” helyett a "biztosítás" az alapbeállítás), és a „zsákutca” megoldás, ahol a felhasználó számára feltétlenül szükséges információ nem áll rendelkezésre, pl. hozzáférési jog gyakorlása lehetőségre kattintás a felhasználó profiljához irányít. A felhasználó döntési folyamatát befolyásoló sötét megoldás például az szimmetrikus hozzáférés a felhasználó részéről, például nincs lehetőség valamely, pl. analitikai cookie elutasítására, a korlátozás, amikor bizonyos opciókat teljesen kizárnak a felhasználói felületről: pl. az ÁSZF-re lehet kattintani, de az adatvédelmi tájékoztatóra külön nem, a „pókháló”, amikor a felhasználó könnyen kerül egy helyzetbe, amiből később nehezen jut ki, például prémium feliratkozás, ingyenes néhány hónapos használat, ahol a leiratkozás, illetve az ingyenes próbaidőszak után a lemondás nagyon bonyolult, és a „sürgetés”, amikor a vásárló időnyomás alá kerül, például számláló jelzi az akció végét, vagy a még elérhető termékek számát [8]. A sötét megoldásoknak számos további kategorizálása ismert, például aszerint, hogy általános, bármilyen megjelenésbe ültethető, stratégiaként működő sötét megoldásról van-e szó (például kikényszerített felhasználói cselekedet, valaminek kényszerű elfogadása),vagy olyan, tartalomszenzitív sötét megoldásról,

amely csak bizonyos esetekben alkalmazható (például a rejtett árazás) [9].

3. Szabályozási háttér az Európai Unióban

A sötét megoldások szabályozásának központi eleme, hogy azok alkalmazása egyszerre több szabályozási rendszer által támasztott jogi követelményt is érint [8]. Ilyen, párhuzamosan alkalmazható szabályrendszer a fogyasztóvédelmi jog és az adatvédelmi jog, valamint általában a digitális platformok szabályozását megcélzó e-kereskedelmi szabályok.

3.1 Adatvédelmi szabályozás

A sötét mintázatok személyes adatok kezelésére kifejtett hatása jellemzően abból ered, hogy az érintettek számára rendelkezésre álló választási lehetőség, és a személyes adatok megosztásának tényleges szándéka eltérő [3]. Ezzel is magyarázható a "privacy paradox" jelenség, mely szerint ellentmondások vannak a megadott adatvédelmi preferenciák és a tényleges közzétételi magatartás között, azaz a felhasználók azt állítják, fontos számukra a magánélet védelme, közben egyidejűleg jelentős mennyiségű személyes adatot adnak meg magukról [10].

Adatvédelmi szempontból a 2016/679(EU) általános adatvédelmi rendelet ("GDPR") 5. cikk (1) bekezdésében meghatározott alapelvek az irányadók, amelyeket a GDPR további rendelkezései konkretizálnak. A GDPR 12. cikkében foglalt tájékoztatási kötelezettség megfelelő teljesítését, a GDPR 6. cikk (1) bekezdés a) pontjában meghatározott hozzájárulás jogalap esetén a GDPR 4. cikk 11. pontjában és 7. cikkében foglalt feltételek teljesülését. Kiemelendő e tekintetben a hozzájárulás tájékoztatott és önkéntes, azaz befolyástól mentes volta [7]. Kiemelten csorbítja az önkéntesség feltételének érvényesülését a sürgetés, amely az érintettet korlátozó nyomás alá helyezi [11]. Önmagában, a platformok kialakítását tekintve átfogó jelentőségű a GDPR 25. cikkében foglalt beépített adatvédelem elve, mert erre tekintettel alakítandók ki az érintett és az adatkezelő közötti erőviszonyok, a fogyasztó elvárásai és interakciói [7]. A beépített adatvédelem elve közvetlenül szembeállítható a sötét megoldások alkalmazásával, tekintettel arra, hogy előző célja az érintetti jogok hatékony érvényesülését biztosító adatkezelési rendszer kialakítása, ideértve pl. az adatminimalizáció és a transzparencia követelményeinek érvényesülését, míg utóbbi jellemzően a személyes adatok túlzott mértékű és átláthatatlan kezelésének eszköze. Ez alapján alapjaiban véve jogellenesnek tekinthetők a "design" részeként beépülő sötét megoldások, amennyiben azok lehetőséget nyújtanak az adatkezelőknek arra, hogy megkerüljék a beépített és alapértelmezett

adatvédelem elvét, és a fogyasztókat ösztönözzék az adatvédelemhez való jogaik figyelmen kívül hagyására, és a szükségesnél több személyes adat megadására [8, 12].

Megjegyzendő, hogy az EDPB kifejezetten szűk mozgásteret biztosít a közösségi média üzemeltetőinek azáltal, hogy a tájékoztatott hozzájárulás megadását bármilyen szempontból megnehezítő gyakorlatot megtévesztő mintaként jogellenesnek értékel, pl. túl sok kattintás szükséges az adatkezelési tájékoztató megismeréséhez, vagy ha egy adatkezelő adatkezelési tájékoztatója és elérhető adatfeldolgozási szerződései egymásra mutató linkeket tartalmaznak [7].

3.2. Fogyasztóvédelem

A fogyasztóvédelem célja a sötét megoldások vonatkozásában az elérhető információ különbségéből eredő fogyasztó és vállalkozás közötti eltérő erőviszonyok szabályozása, legyen az akár az elérhető információk aszimmetriája, akár a fogyasztó döntési folyamatának befolyásolása [8].Az észszerűen elvárható módon tájékozott átlagfogyasztó meg nem engedett befolyásolása kérdését az Európai Unió Bírósága több ízben közvetve a sötét megoldások értékelésére is alkalmas ügyben tárgyalta. A C-562/15 ügy szerint a kereskedelmi reklámra vonatkozóan általánosságban figyelembe kell venni a szubjektív érzékelést, hogy „a szokásosan tájékozott, észszerűen figyelmes és körültekintő, átlagos fogyasztó hogyan észleli a szóban forgó reklám tárgyát képező termékeket vagy szolgáltatásokat”. A C-54/17 ítélet pedig konkrétan a rejtett többletköltségeket és előzetes hozzájárulás nélkül nyújtott szolgáltatásokat tárgyalva jogellenesnek minősíti, ha egy távközlési szolgáltató úgy forgalmaz SIM-kártyát, hogy arra előre telepítettek és aktiváltak az internetes böngészéshez vagy az üzenetrögzítőhez hasonló bizonyos szolgáltatásokat, anélkül, hogy előzetesen megfelelően tájékoztatták volna a fogyasztót ezen előzetes telepítésről és aktiválásról, illetve e szolgáltatások költségeiről [8].

Az adatvezérelt termékekkel és szolgáltatásokkal kapcsolatban a Data Act fogyasztóvédelmi oldalról is közelítve mondja ki a 34. preambulumbekezdésében, hogy a digitális interfészeik tervezői nem hagyatkozhatnak sötét megoldásokra.

3.3. Platformszabályozás

A közvetítő szolgáltatásokat nyújtó szolgáltatókra vonatkozó DSA 25. cikke kifejezett kötelezettséget teremt online interfészek tervezésével és kialakításával kapcsolatban. A DSA szerint "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". Ez a rendelkezés tekinthető a GDPR 25. cikkében foglalt beépített adatvédelem elve kiterjesztő alkalmazásának, ugyanis a DSA 67. preambulumbekezdése kimondja, hogy a sötét mintázatok tilalmára vonatkozó rendelkezés alkalmazandó a GDPR hatálya alá nem tartozó gyakorlatokra. Ki kell emelni ugyanakkor, hogy a DSA 25. cikke nem minden közvetítő szolgáltatót érint, csak az online platformokat. A DSA 25. cikk (2) bekezdése emellett meghatározza a tiltott interfész-kialakítások kategóriáit is, melyek i) egyes választási lehetőségek kiemelése a szolgáltatás igénybe vevőjének döntésre való felkérésekor, ii) a szolgáltatás igénybe vevőjének ismételt felkérése valamely választásra olyan kérdésben, amellyel kapcsolatban már döntést hozott, különösen a felhasználói élményt zavaró felugró ablak alkalmazásával, és iii) a szolgáltatás megszüntetésére irányuló eljárásnak az előfizetési eljárásnál nehezebbé tétele. Bár ez a három minta széles körben elterjedt, ez a lista közel sem tekinthető kimerítőnek. . Az, hogy a DSA kifejezetten erre a három mintára összpontosít, azt sugallja, hogy a sötét megoldások tilalmának kezdeti fókusza a manipulatív gyakorlatok viszonylag szűk körére összpontosít majd [13].

A digitális jogalkotási csomag másik pillére, a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról szóló 2022/1925(EU) rendelet (Digital Market Act, "DMA") a kapuőrök, azaz a DMA 2. cikk 1 pontjában és 3. cikkében meghatározott alapvető platformszolgáltatásokat nyújtó vállalkozásokra tekintettel elvi éllel állapítja meg a 70. preambulumbekezdésben, hogy tilos a felhasználói felületet, vagy annak egy részét, funkcióit vagy működési módjait úgy kialakítani, hogy az a felhasználói autonómiát, döntéshozatalt vagy választást aláássa, vagy csorbítsa. Ezáltal a DMA általános kötelezettséget teremt a sötét megoldások elkerülésére, vagy beszüntetésére. A DMA 63. preambulumbekezdése nevesítve tartalmazza a fenti "pókháló" módszer tilalmát, azaz, "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". Míg a DMA szabályrendszere a nagy

platformokra kötelező erővel hat, a DMA egyik korlátja, hogy a fenti szabály hatálya a kisebb méretű platformokra nem terjed ki [13].

4. A magyar szabályozás

Uniós tagállamként a fent ismertetett jogszabályok Magyarországon is alkalmazandók. A magyar jogban a fentiek mellett a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról szóló 2008. évi XLVII. törvény (Fttv.) veendő figyelembe, amely 3. § (1) bekezdése általános elvként mondja ki a tisztességtelen kereskedelmi gyakorlat tilalmát.

Hatósági oldalon is léteznek kifejezetten a sötét megoldások tárgyában született döntések, függetlenül attól, hogy ezekben a sötét megoldás kifejezés nem szerepel. A Nemzeti Adatvédelmi és Információszabadság Hatóság NAIH-3195-11/2022 sz. határozatában a weboldalon elhelyezett cookiekkal kapcsolatos adatkezelést a GDPR 5. cikk (1) bekezdésébe ütközőnek találta, mert a cookiek elhelyezéséhez való hozzájárulás megadására szolgáló felugró ablakban az „OK, tovább” és egy „Adatkezelési tájékoztató” gomb szerepelt. Ez a megoldás a fent leírt az szimmetrikus hozzáférés esete, hiszen a felhasználó egyetlen tényleges lehetősége a hozzájárulás megadása. Többek között sötét megoldásnak is értékelhető kereskedelmi gyakorlat miatt marasztalta el a GVH 2,5 milliárd forintra a Booking.com vállalatot 2018-ban. A GVH álláspontja szerint agresszív és ezért tiltott kereskedelmi gyakorlat az oldalon a szálláshelyek melletti ajánlatoknál megjelenő sürgető, fogyasztót nyomás alá helyező üzenetek és felvillanó jelzések, pl. „ezen az áron már csak egy elérhető szoba maradt”.

5. Zárógondolatok

A gondosan kialakított megjelenés, és a megfelelő kontextusban bemutatott választási lehetőség alkalmas a felhasználók döntési autonómiájának befolyásolására. A sötét megoldások alkalmazására emiatt jelentős motiváció áll fenn a piaci szereplők oldaláról. A jogalkotó és a szabályozó hatóságok oldalán megjelenő tapasztalatok és tendenciák szerint ugyanakkor növekvő szabályozói hajlandóság áll fenn a fogyasztói autonómia erősítése, a felhasználók védelme, nem utolsó sorban a személyes adatok védelme érdekében. Megfigyelhető az adatvédelem, a fogyasztóvédelem és a platformszabályozás konvergálása, egyfajta „digitális jog”, mint olyan önálló jogterület kialakulása, amely az említett jogterületek által szabályozott, online térben is megjelenő magatartásokat fedi le, ideértve a sötét megoldásokat. A sötét megoldások alkalmazása ezért, bár rövidtávon kecsegtetőnek tűnhet, hosszú távon komoly kitettséget is okozhat az

azt alkalmazók számára, többek között azért is, mert könnyen észrevehetők. A sötét megoldások elhagyása az online platformok részéről sok esetben a működésük és megjelenésük teljes átértékelését teszi szükségessé. Kiemelt szerepet kap ennek során az „etikus design”, ahol a felhasználói felület kialakítása túlmutat a vizuális, tervezői elgondolásokon, és egyúttal a jogszabályi megfelelést szolgálja, amely végeredményben a fogyasztói bizalmat erősítve egyre inkább egyfajta márkaépítő hatással is bír.

Források

[1] Bowman, D. (2009). Goodbye, Google 1. rész. elérhető: https://stopdesign.com/archive/2009/03/20/goodbye-google.html, utolsó hozzáférés ideje: 2023. március 23.

[2] Tversky, A. és Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. Science, 185. évfolyam, 4157. szám, 1124-1131. oldal.

[3] Waldman, A. E. (2020). Cognitive biases, dark patterns, and the ‘privacy paradox’. elérhető: doi, https://doi.org/10.1016/j.copsyc.2019.08.025, utolsó hozzáférés ideje: 2023. március 23.

[4] Európai Bizottság (2022). Viselkedési tanulmány a digitális környezetben alkalmazott tisztességtelen kereskedelmi gyakorlatokról: sötét megoldások és manipulatív mintázatok. elérhető: https://data.europa.eu/doi/10.2838/859030, utolsó hozzáférés ideje: 2023. március23

[5] Narayanan, A. és mtsai (2020). Dark Patterns - Past, Present, and Future - The evolution of tricky user interfaces. ACM Queue, 18. évfolyam, 2. szám.

[6] Bösch, Ch. és mtsai. (2016). Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. Proceedings on Privacy Enhancing Technologies, 4. szám, 237-254. oldal.

[7] Európai Adatvédelmi Testület (EDPB), (2023). Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, elérhető: https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf, utolsó hozzáférés ideje: 2023. március 23.

[8] Domokos, M. és Horváth, A. (2021). Dark patterns - napvilágra kerülő sötét megoldások. elérhető: https://www.jogiforum.hu/blog-ip-it-vedjegy-domain-internet-jogi-blog-11/2021/09/02/dark-patterns-napvilagra-kerulo-sotet-megoldasok/, utolsó hozzáférés: 2023. március 23.

[9] Gray, C.M. és mtsai (2023). Towards a Preliminary Ontology of Dark Patterns Knowledge. elérhető: doi, https://doi.org/10.1145/3544549.3585676, utolsó hozzáférés: 2023. március 23.

[10] Norberg, P. és mtsai (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, elérhető: doi, https://doi.org/10.1111/j.1745-6606.2006.00070.x, utolsó hozzáférés ideje: 2023. március 23.

[11] Information Commissioner's Office (2019). Consultation: Age Appropriate Design code. elérhető: https://ico.org.uk/media/about-the-ico/consultations/aadc/2616602/act-the-app-association.pdf, utolsó hozzáférés: 2023. március 23.

[12] Európai Adatvédelmi Biztos Hivatala (EDPS), (2019). Legal Design Roundtable, elérhető: https://edps.europa.eu/sites/default/files/publication/19-04-27_dark_patterns_en.pdf, utolsó hozzáférés: 2023. március 23.

[13] King, J, és MacKinnon, E. (2022). Do the DSA and DMA Have What It Takes to Take on Dark Patterns? elérhető: https://techpolicy.press/do-the-dsa-and-dma-have-what-it-takes-to-take-on-dark-patterns/, utolsó hozzáférés: 2023. március 23.