Az online platformokon alkalmazott sötét megoldások

2023. június 12., frissítve 2023. július 4.

Szerzők:
Dr. Petrányi Dóra, Dr. Domokos Márton, Dr. Horváth Anna Zsófia, Dr. Huszár Daniella

Tartalomjegyzék

1. Problémafelvetés és a sötét megoldások meghatározása ... 3
1.1 A sötét megoldások elterjedése az online térben ... 3
1.2 Sötét megoldások fogalma ... 4
1.2.1 Kategorizációs rendszerek a sötét megoldások típusai alapján ... 4
1.2.2 Fogalomalkotási kísérletek ... 6
2. A viselkedési közgazdaságtan és a kognitív pszichológia viselkedés-befolyásolással kapcsolatos eredményei ... 9
3. A sötét megoldások szabályozásának jogi háttere ... 11
3.1 Az EU szabályozási keretrendszere ... 13
3.1.1 Az alkalmazott megoldások adatvédelmi szempontú megítélése ... 13
3.1.2 A sötét megoldások fogyasztóvédelmi szempontú megítélése: a fogyasztó választási szabadsága, lehetősége a tájékozott döntés meghozatalára ... 15
3.1.3 Az alkalmazott megoldások megítélése online platformszabályozás vonatkozásában ... 18
3.2 Magyar szabályozási háttér ... 21
3.2.1 Az alkalmazott megoldások adatvédelmi szempontú megítélése ... 21
3.2.2 Az alkalmazott megoldások fogyasztóvédelmi szempontú megítélése ... 21
3.2.3 Az alkalmazott megoldások platformszabályozási szempontú megítélése ... 21
4. Jogalkalmazási gyakorlat ... 22
4.1 Magyar szabályozási gyakorlat ... 23
4.1.1 NAIH döntések ... 23
4.1.2 A GVH tevékenysége és döntései ... 28
4.2 Európai Uniós szabályozási gyakorlat ... 32
4.2.1 Európai Uniós szervek ... 32
4.2.2 Tagállami szabályozási irányok ... 37
5. Javaslatok a sötét megoldások szabályozására ... 38
5.1 Jogszabályi keretrendszer ... 38
5.2 Jogon kívüli eszközök ... 40
Irodalomjegyzék ... 42
1. melléklet: Rövidítések jegyzéke ... 46
2. melléklet: Sötét megoldások kategorizációs rendszerei, taxonómiák ... 49
3. melléklet: EGT-tagállamok szabályozó hatósági gyakorlat, statisztika ... 55

1. Problémafelvetés és a sötét megoldások meghatározása

Az utóbbi években tapasztalható digitalizációs hullám eredményeként a felhasználók számára a digitális környezetben szinte teljes egészében elérhetővé váltak ugyanazok a mindennapos tevékenységek és szolgáltatások, amelyek korábban kizárólag, vagy döntően offline történtek. Ebben az online térben egyre több olyan módszer és eszköz áll rendelkezésre, amelyek célja, hogy a felhasználókat olyan tranzakciós döntések meghozatalára sarkallják, amelyek ellentétesek lehetnek az érdekeikkel, vagy amelyeket egyébként nem kívánnának megtenni (Európai Bizottság, 2022).

1.1 A sötét megoldások elterjedése az online térben

A korábbi, felhasználók és vásárlók minél szélesebb körének elérését és bevonását célzó marketingstratégiákkal ellentétben ezek az online módszerek és eszközök sokkal kifinomultabbak, és hatékonyabban képesek megszólítani, illetve a kívánt eredmény felé terelni a felhasználókat (Calo, 2014). Ennek oka egyrészt, hogy az offline tranzakciókkal ellentétben a fogyasztók és a vállalkozások közötti online tranzakciók jellemzően interaktív módon és eszközön, például számítógépen vagy mobiltelefonon keresztül zajlanak, amely révén a vállalkozás saját maga által kialakított vagy megválasztott felhasználói felületen („user experience”, „UX” design), és lépéseken keresztül vezetheti végig a felhasználót, másrészt, hogy a vállalkozás a felhasználó által megtett lépések követése és megfigyelése során folyamatos visszajelzést kap a felhasználó viselkedéséről, preferenciáiról (OECD, 2022). Ezt kihasználva az online vállalkozások ismétlődően végezhetnek véletlenszerű kísérleteket (ún. A/B teszteket), amelyek során a weboldalaik változatait két vagy több véletlenszerűen kiválasztott felhasználói csoportnak mutatják be, hogy folyamatosan finomíthassák a weboldalak és alkalmazások kialakítását annak alapján, hogy melyik kialakítás és megjelenés maximalizálja a felhasználókból kiváltani kívánt eredményeket (Narayanan és mtsai., 2020). Az A/B tesztelés webdesignban betöltött kiemelt jelentőségét mutatja például, hogy a Google egy felhasználói felülete tervezésekor a kék szín 41 árnyalatát tesztelte, hogy kiderüljön, melyik teljesít jobban (Bowman, 2009). Ezzel együtt egyre inkább elterjedtek az adatvezérelt, ún. „hiper-nudging” kereskedelmi gyakorlatok is a fogyasztók figyelmének felkeltésére és befolyásolására, azaz az olyan technikák, amelyek kifejezetten személyreszabott „ösztönzőkkel” terelik a felhasználókat a kívánt cselekvés irányába (Yeung, 2016).

Az Európai Bizottság 2023. január 30-án publikálta a 23 uniós tagállam, Norvégia és Izland fogyasztóvédelmi hatóságait tömörítő CPC hálózat részvételével végzett webáruház-átvilágítás eredményeit. A koordinált vizsgálat Európa-szerte 399 webáruházra terjedt ki, a ruházati áruházaktól az elektronikai cikkekig, három ismert manipulatív gyakorlatra összpontosítva: a hamis visszaszámlálásokra, a többletvásárlásra késztető felhasználói felületekre és az információkat elrejtő gyakorlatokra (GVH, 2023, Európai Bizottság, 2023). Az eredmények szerint 148 weboldal alkalmazott legalább egy sötét megoldást. 42 weboldal hamis visszaszámlálót használt bizonyos termékek megvásárlására vonatkozó határidőkkel, 54 weboldal bizonyos, többletvásárlásra késztető választási lehetőségek felé terelte a fogyasztókat - az előfizetésektől a drágább termékekig vagy szállítási lehetőségekig, 70 weboldal pedig fontos információkat rejtett el, vagy tett kevésbé láthatóvá

a fogyasztók számára (Európai Bizottság, 2023). A jelenség globálisan is hasonló mértékben figyelhető meg, egy 2019-ben 64 ország (köztük Magyarország) fogyasztóvédelmi hatóságait tömörítő ICPEN nemzetközi hálózat által lefolytatott koordinált akció 1760 weboldal és applikáció átvizsgálását követően az átvizsgált weboldalak és applikációk 24 %-nál (429 db) azonosított felhasználói viselkedést ösztönző manipulációt (OECD, 2021).

1.2 Sötét megoldások fogalma

A sötét megoldások megjelenésének kezdeti szakaszában mind az akadémiai kutatások, mind a szakpolitikai elemzések izoláltan, a sötét megoldások egy-egy megjelenését vizsgálták, azokat egyesével és önállóan nevezték el, majd a nevesített sötét megoldásokat igyekeztek rendszerbe foglalni különböző taxonómiák alapján.

1.2.1 Kategorizációs rendszerek a sötét megoldások típusai alapján

A „sötét megoldások" fogalmat először Harry Brignull UX designer használta[1], mint olyan rosszindulatú felhasználói felületek, amelyek például arra késztetik a felhasználót, hogy akkor is vásároljon meg egy terméket vagy iratkozzon fel valamilyen szolgáltatásra, ha ez nem állt kifejezett szándékában. Brignull kezdeti leíró definíciója mögött nem állt szisztematikus rendszerezés, hanem ad hoc, weboldalakon rögzített példák, úgy, mint a „csalás és átverés" („bait and switch"), azaz látszólag kedvező árú termékek reklámozása, azzal a szándékkal, hogy a vásárláskor gyengébb vagy drágább árukkal helyettesítsék őket, vagy a „sürgetés", („urge"), azaz a vásárló gyors döntéshozatali helyzetbe kényszerítése, például egy számlálóval (vö. Mathur és mtsai, 2021).

A sötét megoldások első rendszerbe foglalását Conti és Sobiesk (2010) végezték, akik értelmezésében a sötét megoldás olyan felhasználói felület, amely szándékosan megsérti a bevett felhasználóbarát tervezési gyakorlatot, és a kellemes felhasználói élménnyel ellentétben manipulálja és kihasználja a felhasználót. Az általuk azonosított sötét megoldások részben átfedésben voltak a Brignull által nevesített gyakorlati példákkal, másrészt azokat olyan új kategóriákba rendezték, amelyek jobban képesek voltak lefedni a különböző technikákat. Conti és Sobiesk első kategorizációs kísérletét követően számos további csoportosítás született, amelyek a korábban azonosított manipulatív technikákra és taxonómiákra építve, azokat újra feldolgozva részben új kategóriákat hoztak létre (Gray és mtsai., 2018), vagy meglévő kategóriák összevonásával gyűjtőkategóriákba rendszerezték a korábban azonosított sötét megoldásokat (Bösch és mtsai., 2016, Mathur és mtsai, 2019, Luguri és Strahilevitz, 2021). Mathur és mtsai. (2019) összesen 11.000 webáruház 53.000 termékeladási weboldalát megvizsgálva 1818 egyedi manipulatív technikát azonosítottak, amelyet 15 sötét megoldásként összesen 7 kategóriába soroltak. Az egyes hivatkozott taxonómiák részletes bemutatását a 2. melléklet tartalmazza.

Új szempontrendszert alkalmazott a fenti korai taxonómiákhoz képest Leiser (2022), aki a manipulatív technikákat az UCPD kontextusában tárgyalta, felismerve, hogy az UCPD szabályozása

1 https://www.deceptive.design/, a weboldal eredeti indulásakor 2010-ben www.darkpatterns.org

nem csak a fogyasztó és vállalkozás közötti kereskedelmi ügylet során és azt követően alkalmazott kereskedelmi gyakorlatokra vonatkozik, hanem a kereskedelmi ügylet tényleges megkötését vagy létrejöttét (pl. vásárlás, feliratkozás szolgáltatásra, regisztráció) megelőzően is, azaz, amikor legtöbb manipulatív felhasználói felület megjelenik. Az UCPD 5-9. cikkei egy három lépésből álló teszt alapján határozzák meg a i) tisztességtelen, ii) különösen tisztességtelen és iii) tiltott kereskedelmi gyakorlatokat, amelyek legtöbb esetben megfeleltethetők korábban azonosított manipulatív technikákkal. Például, a korábban említett „csalás és átverés" az UCPD 6. cikke szerinti megtévesztő tevékenységnek, míg a „csótánymotel" („roach motel") elnevezésű sötét megoldás, amely ellehetetleníti a felhasználó számára egy szolgáltatás lemondását vagy leiratkozást, tipikusan az UCPD 8. cikke szerinti agresszív kereskedelmi gyakorlatnak minősül.

Szintén már kiforrott jogszabályi keretrendszerre alapozta taxonómiáját Jarovsky (2022), aki a korábbi, felhasználó befolyásmentes és informált döntéshozatali lehetőségét és képességét központba helyező rendszerek helyett egy, a kontinentális jogrendszerekben rögzített általános polgári jogi intézményre, a jogügyletek érvénytelenségére épülő rendszert hozott létre. Elmélete szerint a manipulatív technikák egyben a jogügyletek érvénytelenségét eredményező érvénytelenségi okként is felfoghatók. A magyar jogrendszerben ennek megfelelően a manipulatív felhasználói felületek a Ptk. 6:90. § szerinti tévedés, Ptk. 6:91. § szerinti megtévesztés, Ptk. 6:92. § szerinti titkos fenntartás, vagy Ptk. 6:100. § szerinti fogyasztói jogot csorbító feltétel érvénytelenségi okot valósíthatják meg. A kontinentális jogrendszert alkalmazó EU-tagállamok polgári jogi szabályozása közötti terminológiai akadályok áthidalása érdekében Jarovsky a sötét megoldásokat négy általános kategóriába rendezte aszerint, hogy mely érvényteleségi oknak felelnek meg, ezek a „nyomás alá helyezés", („pressure"), „akadályozás" („hinder"), „félrevezetés" („mislead"), és „megtévesztés" („misrepresent") esetei (Jarovsky, 2022).

Legújabb kutatások a manipulatív felhasználói felületek első és második generációját különböztetik meg. Az ún. első-generációs sötét megoldások a fent hivatkozott taxonómiákban azonosított manipulatív megjelenési felületek, amelyek a felhasználókat közvetlenül célozzák, és ezáltal viszonylag könnyen felismerhetők. A második generációs sötét megoldások az első generációs sötét megoldások technikáira épülnek, de azoknál kifinomultabbak, sokszor a felhasználó elől teljesen rejtve, a weboldal fejlesztői és üzemeltetői oldalán jelentkeznek (Kitkowska és mtsai., 2022). A második generációs sötét megoldások jellemzően a böngészési előzmények és online magatartás széles körű megfigyelése által gyűjtött felhasználói adatokra alapuló megoldások, mint például a böngészési előzmények és a közösségi médián belüli interakciók felhasználása a manipulatív megoldások testre szabásához, kifejezetten az egyéni sebezhetőségek vagy preferenciák kihasználására, vagy olyan algoritmus-alapú rendszerek, amelyek finoman, gyakran kifejezett hozzájárulás vagy tájékoztatás nélkül bizonyos viselkedésmódok vagy eredmények felé terelik a felhasználókat (BEUC, 2022). Ennek egyik példája a különböző regisztrációhoz kötött foglalási rendszerek, amelyek megjegyzik a korábbi kereséseket, foglalásokat, nem választott lehetőségeket, majd a következő ajánlatok megjelenítésekor ezeket az adatokat is figyelembe veszik – így a felhasználók nem lehetnek biztosak abban, hogy ugyanazt az információt látják-e egy ajánlatnál, mint a többi felhasználó. Ezek sokkal nehezebben felismerhetőek, így károsabbak lehetnek, mivel a

felhasználók online viselkedése alapján gyűjtött adatok széles körű elemzése alapján egyfajta „személyre szabott csapdát” állítanak, és a felhasználók átmeneti sebezhetőségét (pl. kíváncsiság, sietség) célozzák meg (Kitkowska és mtsai., 2022).

1.2.2 Fogalomalkotási kísérletek

A sötét megoldások egyes esetei azonosításának lényege, hogy megragadja a jelenség egyedi megjelenését, azonosítsa az egyes megjelenések közös jellemzőit, és ez alapján absztrahálja azt egy konkrét felhasználási esettől függetlenül (Európai Bizottság, 2022). A sötét megoldások absztrakt definícióinak meghatározása ugyanis elengedhetetlen a hatékony szabályozáshoz, mivel a sötét megoldások folyamatosan fejlődnek, korábbi sötét megoldások válnak szofisztikáltabbá és újak jelennek meg. A taxonómiák nehezen tudják megragadni e manipulatív tervezési gyakorlatok árnyalt és folyamatosan változó természetét, az absztrakt definíciók viszont a sötét megoldások széles körét felölelő, rugalmas keretet biztosítanak.

A sötét megoldások legelső definíciója a korábban említettek szerint Harry Brignulltól származik:

> “*a sötét megoldások olyan rosszindulatú felhasználói felületek, amelyek például arra késztetik a felhasználót, hogy akkor is vásároljon meg egy terméket vagy iratkozzon fel valamilyen szolgáltatásra, ha ez nem állt kifejezett szándékában*.”

A szakirodalomban több hasonló meghatározás is született:

> „*A felhasználói felület sötét megoldása a felhasználókat nem szándékolt és nem kívánt műveletek elvégzésére készteti, egy félrevezető felület kialakításán alapul. Általánosabban szólva, egy sötét megoldás egy a felhasználók kihasználására és megtévesztésére bevett megoldást ír le egy általános formában*.” (Bösch és mtsai., 2016)
>
> “*Olyan esetek, amikor a tervezők az emberi viselkedésről (pl. pszichológia) és a végfelhasználók kívánságairól szerzett ismereteiket felhasználva olyan megtévesztő funkciókat valósítanak meg, amelyek nem a felhasználó érdekeit szolgálják*.” (Gray és mtsai., 2018).
>
> „*Olyan felhasználói felületek, amelyek tervezői tudatosan összezavarják a felhasználókat, megnehezítik a felhasználók számára, hogy kifejezzék tényleges preferenciáikat, vagy manipulálják a felhasználókat, hogy bizonyos műveleteket hajtsanak végre*” (Luguri és Strahilevitz, 2021).

A sötét megoldások meghatározására a szakirodalommal párhuzamosan, azokra építve a szabályozói oldalról is születtek definíciók, mind nemzetközi ajánlásokban, szakpolitikai dokumentumokban, mind szabályozó hatósági ajánlásokban és iránymutatásokban, például:

> *„A sötét kereskedelmi megoldások olyan üzleti gyakorlatok, amelyek a digitális választási architektúra elemeit alkalmazzák, különösen az online felhasználói felületeken, és amelyek aláássák vagy károsítják a fogyasztói autonómiát, döntéshozatalt vagy választást. Ezek gyakran megtévesztik, kényszerítik vagy manipulálják a fogyasztókat, és valószínűleg különböző módon közvetlen vagy*

közvetett fogyasztói hátrányt okoznak, bár sok esetben nehéz vagy lehetetlen mérni az ilyen hátrányt." (OECD, 2022).

„Olyan online felület vagy annak egy része, amely szerkezetén, funkcióján vagy működési módján keresztül felforgatja vagy korlátozza a szolgáltatás igénybevevőinek autonómiáját, döntéshozatali képességét vagy választási lehetőségeit." (BEUC, 2022).

„A felhasználói felület kialakításának olyan jellemzői, amelyek célja, hogy rávegyék a felhasználókat olyan dolgok megtételére, amelyeket nem feltétlenül akarnak, de amelyek a szóban forgó vállalkozás számára előnyösek" (NCC, 2018)

"Megtévesztő tervezési minták, 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." (EDPB, 2022).

A sötét megoldások absztrakt meghatározására való kísérletek a jelenség jogszabályba való beépítésének szükségszerű előfutáraiként jelentkeztek. Ez az integráció teremtett szilárd alapot a digitális térben a fogyasztók védelmét szolgáló, valamint az átlátható felhasználói élményt elősegítő jogszabályok megalkotásához a jogalkotók számára:

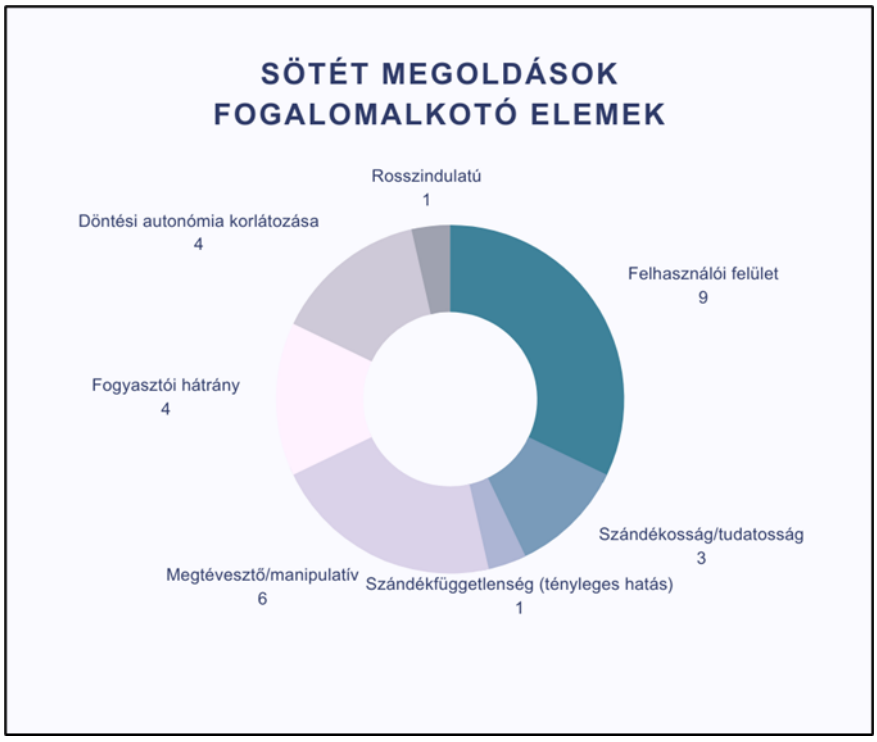
"Az online platformok online interfészein megjelenő sötét megoldások olyan gyakorlatok, amelyek akár szándékosan, akár ténylegesen jelentősen torzítják vagy korlátozzák a szolgáltatás igénybe vevőinek azon képességét, hogy önálló és megalapozott döntéseket hozzanak. Ezek a gyakorlatok felhasználhatók arra, hogy a szolgáltatás igénybe vevőit meggyőzzék arról, hogy nem kívánt magatartást tanúsítsanak, vagy olyan nem kívánt döntéseket hozzanak, amelyek negatív következményekkel járnak rájuk nézve." (DSA, 67. preambulumbekezdés).

„A kapuőr nem ronthatja le azon alapvető platformszolgáltatások feltételeit vagy minőségét, amelyeket olyan üzleti felhasználók vagy végfelhasználók részére nyújt, […] 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 egy részének felépítése, kialakítása, funkciója vagy működési módja révén." (DMA, 13. cikk (6) bek.).

"*A sötét megoldások olyan webszerkesztési technikák, amelyek a fogyasztókat megtévesztő módon számukra hátrányos következményekkel járó, nem kívánt döntések felé terelik. Ezek a manipulatív technikák felhasználhatók arra, hogy a felhasználókat – különösen a kiszolgáltatott fogyasztókat – meggyőzzék arról,*

hogy nem kívánt magatartást tanúsítsanak, és félrevezessék őket azáltal, hogy adatközlési műveletekkel kapcsolatos döntések felé terelik őket, vagy indokolatlanul torzítják a szolgáltatás felhasználóinak döntéshozatalát oly módon, hogy az aláássa és gyengíti autonómiájukat, döntéshozatalukat és választásukat. Az uniós joggal összhangban lévő általános és jogszerű üzleti gyakorlatok önmagukban nem tekinthetők sötét megoldásoknak." (Data Act, 34. preambulumbekezdés)

A 1. ábra gyakoriság szerint szemlélteti a fenti 11 meghatározásban megjelenő fogalmi elemeket, aszerint, hogy hány fenti definícióban fordulnak elő. Látható, hogy míg alapvetően konszenzus van abban, hogy a sötét megoldások manipulatív felhasználói felületek, addig a többi fogalmi elem estén lényegesen kisebb az egyetértés.



1. ábra: A sötét megoldások leggyakoribb fogalomalkotó elemei

Az 1. ábrán feltüntetett fogalmi elemek az egyes definíciók közelítése érdekében az alábbi négy építőelemben foglalhatók össze:

- **Szándékosság**: a legtöbb definíció szerint a sötét megoldás használata tudatos döntés eredménye, és használatával az alkalmazó fél célja kifejezetten az, hogy a felhasználót valamilyen irányba befolyásolja. Kivételt jelent ez alól a DSA definíciója, amely úgy fogalmaz, a sötét megoldás az, ami „*akár szándékosan, akár ténylegesen*” torzítja a felhasználó választási szabadságát és döntéshozatalát. Ez azért lényeges körülmény, mert a tényleges hatás beemelésével egy gyakorlat a DSA alatt az azt alkalmazó fél szubjektív tudatállapotától függetlenül, a befolyásolási képesség objektív feltétele alapján tekinthető sötét megoldásnak.

- **Felhasználó számára hátrány okozása**: A sötét megoldások jellemzően olyan, az alkalmazó félnek előnyös és kedvező megoldások, amelyek a felhasználói oldalon valamilyen hátrányként jelennek meg. Ez a hátrány jelentkezhet az informált döntéshozatali lehetőség csorbulásában, információs önrendelkezési jog sérelmében, vagy akár közvetlen anyagi kár formájában (például az észrevétlenül hozzáadott többletköltségek kifizetése „csempészés" eredményeként). A hátrány megállapítása bizonyos esetekben viszont nagyon nehéz, vagy akár az egyén szintjén nem is lehetséges. Ilyen például a streaming platformokon elérhető ún. „autoplay" funkció, azaz videók vagy filmek automatikus lejátszása / betöltése, amint az előző véget ér (Bongard-Blanchy és mtsai, 2021). Ez önmagában nem jelent hátrányt a felhasználó számára, hiszen rövid távon a felhasználó akár hasznosnak is tekintheti, hosszú távon viszont kimutathatóan szerepet játszik a „streaming-függőség", vagy ún. „digitális függőség kialakulásában (Flayelle és mtsai, 2023).
- **Megtévesztő és leplezett jelleg**: a sötét megoldásokat az eddigi definíciók a megtévesztő jelleget jellemzően leplezetten működő, félrevezető technikaként értelmezik, ahol a felhasználók sokszor nincsenek tisztában azzal, hogy a felhasználói felület önmagában befolyásolja őket. Ezt a szűk értelmezést követve ugyanakkor egyes sötét megoldások, bár a többi fogalmi elemet egyébként teljesítik, a szabályozási körön kívül esnek. Ilyen például az ún. „megszégyenítés" („Confirm Shaming"), azaz együttműködés bűntudatkeltés alapján, ahol csak úgy lehet nemet mondani egy ajánlatra, hogy a felhasználó ettől rosszul érzi magát, például „*Akarsz adományozni a tengerek tisztítására?*" kérdésre adott két opció az „igen" és a „nem, nem érdekelnek a tiszta tengerek" (Domokos és Horváth, 2022). Az ilyen kérdések jellemzően nem leplezett módon, hanem kifejezetten szembetűnően jelennek meg.
- **Felhasználói felület kialakításának része**: a sötét megoldások minden definícióban egyöntetűen a felhasználói felület kialakításában megjelenő manipulatív technológiák. Ez az elhatárolási szempont szolgálja a sötét megoldások és az egyéb marketingeszközök, például a süti („cookie") alapú technológiák vagy a közösségi médiaoldalak forgalmának elemzésére épülő reklámkampányok elhatárolását.

A fenti részletektől eltekintve a meghatározások központi eleme összhangban áll egymással, mivel mindegyik abból indul ki, hogy a sötét megoldások módosítják a fogyasztó elé tárt digitális választási architektúrát. Ez vagy a fogyasztó rendelkezésére álló választási lehetőségek módosításával (a rendelkezésre álló választási lehetőségek egyenlőtlen súlyozásával, olyan választási lehetőségek kizárásával, amelyeknek rendelkezésre kellene állniuk, vagy az egyes fogyasztókkal szemben eltérő bánásmóddal), vagy a fogyasztóhoz érkező információáramlás manipulálásával (hamis információk nyújtásával vagy a releváns információk elfedésével vagy késleltetésével) történik (Mathur és mtsai., 2021).

2. A viselkedési közgazdaságtan és a kognitív pszichológia viselkedés-befolyásolással kapcsolatos eredményei

Az emberi gondolkodás folyamatait vizsgáló kognitív pszichológia és a környezet döntésekre gyakorolt hatását vizsgáló viselkedési közgazdaságtan eredményei mind abba az irányba mutatnak,

hogy a gondosan kialakított megjelenés, és a megfelelő kontextusban bemutatott választási lehetőség alkalmas a felhasználók döntési autonómiájának befolyásolására (Horváth, 2023).

A sötét megoldások alkalmazása azért annyira hatékony és népszerű, mert az online felületek kialakítása a "meggyőző számítástechnika" („*persuasive computing*”) elvének alkalmazásával alakítja ki a felhasználók számára elérhető ún. affordanciákat (Európai Bizottság, 2022). Az affordanciák kifejezést James J. Gibson (1979) alkotta meg a környezet egyénfüggő érzékelésének leírására az ún. ökológiai pszichológia elmélet keretében, amely szerint az egyén és a környezete között „egymást feltételező” kapcsolat van (Szokolszky és Kádár, 1999). Az affordanciák a környezet és a tárgyak olyan jellemzői, amelyek alapján az egyén megállapítja, hogy azok hogyan és mire használhatók. Gibson elmélete szerint a környezet tárgyai nem önmagukban értelmezhetőek, hanem mindig az érzékelő személyétől, készségeitől, tapasztalataitól, és az érzékelt használattól függően. Például, egy ajtókilincs formája és elhelyezkedése alapján sugallja azt, hogy az ajtót húzni vagy tolni kell ahhoz, hogy kinyíljon. Az affordancia-koncepció széles körben alkalmazható a technológiában, így az UX tervezésben is, mert az affordanciák megértése lehetővé teszi olyan intuitívabb és felhasználóbarát eszközök létrehozását, amelyek jobban illeszkednek az egyének természetes érzékeléséhez és cselekvéséhez. Igaz ez ugyanakkor fordítva is, hiszen az érzékelési folyamatok megismerésével könnyebb olyan felhasználói felületek kialakítása is, amelyek kihasználják ezen érzékelési folyamatok sérülékenységeit.

Az észlelési folyamatokat illetően széles körű egyetértés van a pszichológiai kutatások terén abban, hogy az észlelési és gondolkodási folyamatok hátterében két különböző kognitív rendszer áll (Kahneman, 2011). Jelen elemzés keretében ezek közül az a rendszer releváns, amelyik elsősorban öntudatlanul, automatikusan és kevés erőfeszítéssel működik (Bösch és mtsai, 2016). Tipikus példa ezen rendszer működésére az adatkezelési tájékoztatók, általános szerződési feltételek átolvasás nélküli, azonnali elfogadása. Ennek a gondolkodási rendszernek a működése összefügg az észlelés egyik legmeghatározóbb és ezért kihasználható tulajdonságával, ami a figyelem korlátossága. A figyelem korlátozott kapacitásának elmélete szerint az emberi figyelem erőforrásai végesek, azaz, az egyén nem képes az összes rendelkezésére álló információra egyszerre koncentrálni. Ez a korlátosság befolyásolja döntéseket és észlelést, mivel az egyén kénytelen nem tudatosan „válogatni” a figyelembe vett és a figyelmen kívül hagyott információk között. Az információk közötti ezen automatikus, nem tudatos és ezért jellemzően nem befolyásolható szelektálást ún. döntéskönnyítő mechanizmusok, döntési heurisztikák segítik (Waldman, 2020). Ezek a mechanizmusok kognitív torzításokhoz vezetnek, ahol az egyén a helyzet tényleges értékelése helyett gondolkodási sémákra támaszkodva dönt (Tvertsky és Kahneman, 1974). Ilyen kognitív torzítás például a lehorgonyzási hatás („anchoring bias”), mely szerint a döntés meghozatalában a tárgyban kapott első információ esik legnagyobb súllyal a latba, a később kapott információt az egyén kisebb jelentőségűnek értékeli. További kognitív torzítás az „egytényezős” 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 (Horváth, 2023), vagy a megerősítési torzítás („confirmation bias”), mely szerint az egyének azokat információkat részesítik előnyben, amelyek igazolják saját előfeltevéseiket.

A kognitív pszichológia kognitív torzításokkal foglalkozó elméletei és kutatási eredményei alapján általánosan elfogadott és igazolt tény, hogy az egyén döntései nem racionálisak, legalábbis nem

abban a közgazdaságtani értelemben, mely szerint a döntések mindig egy tudatosan előre meghatározott cél felé mutatnak (Sibony, 2019).

Az Európai Bizottság (2022) két átfogó kutatást folytatott le a fogyasztók sötét megoldásokkal kapcsolatos tudatosságának és tapasztalatainak felmérése érdekében.

Az első kísérletben felugró ablakokat jelenítettek meg a résztvevőknek, a vizsgált csoportban személyre szabott „*Szia, (név)*" üdvözléssel, a kontrollcsoportban csak „*Szia*" felirattal. Az adatok megerősítették, hogy a vizsgált csoport esetében a résztvevők általában nem tudták figyelmen kívül hagyni a felugró ablakot, valamint, hogy a figyelmük szélesebb körben oszlott meg a weboldalon, szemben a kontrollcsoporttal, amelynek figyelme főként a felugró ablakon belül összpontosult, ami azt jelzi, hogy a vizsgált csoport tagjainak figyelme a teljes felület egészére kiterjedt, míg a kontrollcsoport figyelmét lekötötte a felugró ablak bezárása. A kísérlet eredményei tehát a perszonalizált hirdetési felugró ablak sötét megoldás figyelemfelkeltő jellegét mutatják, a hirdetések személyre szabása (azaz a névre szóló üdvözlés) kierőszakolt cselekvéssel, azaz a felugró ablak bezárásával kombinálva hatással van arra, hogy miként navigálnak egy weboldalon és hogyan lépnek kapcsolatba a weboldalon megjelenített tartalmakkal (Európai Bizottság, 2022).

A második kutatásban szintén felugró ablakot mutattak a résztvevőknek, a vizsgált csoportban egy megszégyenítő („Confirm shaming") üzenetet tartalmazó, a kontrollcsoportban egy igen/nem kérdéssel próbálták rávenni őket kedvezmény elfogadására. Az eredmények azt sugallják, hogy a megszégyenítés hatással van a felhasználók figyelmére, mivel befolyásolja azokat a felületeket, amelyekre a résztvevők figyelmet fordítanak. Érdekes viszont, hogy az érzelmi reakciókat jelző érzelmi indexet és a pulzusszámot nem befolyásolta a „Confirm shaming" sötét megoldása, ami egyfajta immunitást jelezhet a gyakorlattal szemben. Mivel egyre több weboldal alkalmaz érzelmeket kiváltó üzeneteket, valószínűsíthető, hogy a felhasználók egyre inkább hozzászoknak ezekhez a gyakorlatokhoz, ami magyarázatot ad az érzelmi reakció hiányára (Európai Bizottság, 2022).

Egy, a sötét megoldások felhasználók általi érzékelésével kapcsolatos, 406 résztvevővel lefolytatott empirikus kutatás kimutatta továbbá, hogy a felhasználók általában képesek azonosítani a sötét megoldásokat, ellenben alábecsülik az azok által okozott hátrány mértékét, míg a saját rezilienciájukat túlbecsülik, azaz inkább feltételezik magukról azt, hogy az átlagosnál jobban „átlátnak" a sötét megoldásokon, és nem hagyják magukat befolyásolni (Bongard-Blanchy és mtsai, 2021). Ugyanez a kutatás kimutatta azt, is, hogy a magasabb iskolázottságú, egyetemi vagy magasabb végzettséggel rendelkező, és a 40 év alatti korosztályba tartozó személyek valószínűbben ismerik fel a sötét megoldásokat, ami a demográfiai és szocioökonómiai tényezők szerepét bizonyítja.

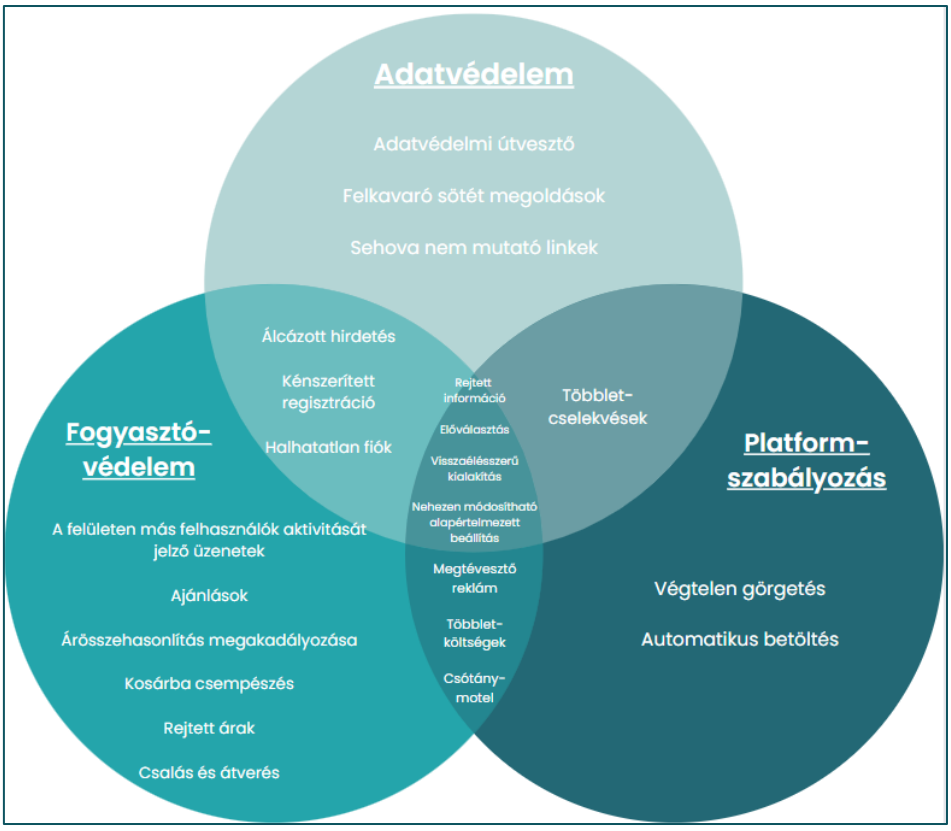
Összességében a kognitív pszichológia és a viselkedési közgazdaságtan fent bemutatott eredményei és elméletei egyértelműen azt mutatják, hogy a sötét megoldások hogyan használják ki az egyéni észlelés és gondolkodás korlátait és manipulálják a döntéshozatali folyamatokat, ami arra vezethet, hogy a felhasználók olyan cselekedeteket végeznek, amelyek nem igazodnak az egyébként racionális preferenciáikhoz vagy érdekeikhez.

3. A sötét megoldások szabályozásának jogi háttere

A sötét megoldások jogi megítélése nem azonosítható pusztán egy homogén rendszerben, hiszen annak fogalma és szabályozási igénye is a jog rendszerén kívülről érkezett. Ennek megfelelően nem

meglepő, hogy a sötét megoldások alkalmazásának szankcionálása sem köthető kifejezetten csak egy jogterülethez, hiszen az adatvédelem, a fogyasztóvédelem, illetve a platformszabályozás rendelkezéseibe is ütközhet egy-egy gyakorlat. (Domokos és Horváth, 2021) Az így kialakult szabályozási pluralizmus mentén felmerülhet ugyanakkor olyan helyzet is, amikor a területek nem válnak el élesen egymástól, így az alkalmazott sötét megoldás adott esetben mind adatvédelmi, mind fogyasztóvédelmi, mind platformszabályozási szempontból jogsértő lehet (ld. 2. ábra). E helyzet feloldását jelentheti a DSA 25. cikk (2) bekezdésében szereplő hatáskör elhatárolás, mely szerint a DSA nem alkalmazandó a fogyasztóvédelmi és az adatvédelmi jog hatálya alá eső sötét megoldásokra – az ezzel kapcsolatos részletes elemzés az alábbi 3.1.3.4 pontban került kifejtésre.

Az, hogy mely jogterület rendelkezései érvényesülnek elsődlegesen, főként abban áll, hogy a szabályozás milyen alapon vonatkozik a sötét megoldásra. Az adatvédelem esetében az adatgyűjtés és az azt követő adatkezelés jogszerűsége tekintetében merülhet fel sötét megoldás alkalmazása, amely esetben a sötét megoldást alkalmazó vállalkozás adatkezelőként, a felhasználó pedig érintettként kerül azonosításra. Fogyasztóvédelmi szempontból a tisztességtelen kereskedelmi gyakorlatok keretében figyelhetőek meg a sötét megoldások, ahol a felhasználó fogyasztóként szerepel B2C viszonyban a sötét megoldást alkalmazó vállalkozással szemben. A klasszikus jogterületeken túl, a platformszabályozási rezsim is reagál a sötét megoldások alkalmazására, kifejezett sui generis tilalmat megállapítva az online platformok üzemeltetői számára.



2. ábra: Sötét megoldások az irányadó jogterületek tükrében[2]

3.1 Az EU szabályozási keretrendszere

Az Európai Bizottság 2020-2025 évekre vonatkozó fogyasztóügyi stratégiája kiemelt területként határozza meg a digitális átalakulás és a fogyasztói jogok hatékony érvényesítését. Ennek keretében a Bizottság különösen az olyan online kereskedelmi gyakorlatok ellen kíván fellépni, amelyek figyelmen kívül hagyják a fogyasztók tájékozott döntéshez való jogát, visszaélnek viselkedésbeli elfogultságaikkal vagy torzítják döntéshozatali folyamataikat. A sötét megoldások alkalmazásának elterjedése egyértelművé tette a Bizottság számára annak szükségességét, hogy értékelje a meglévő jogszabályok hatékonyságát, valamint, hogy olyan további szabályok megalkotására törekedjen, amelyek a szabályozási környezetbe illeszkedve pótolják a hiányosságokat. (Európai Bizottság, 2020).

3.1.1 Az alkalmazott megoldások adatvédelmi szempontú megítélése

A sötét megoldások egy része a felhasználó számára elérhető információt és információ áramlást befolyásolja, korlátozva ezzel a felhasználók információs önrendelkezési jogát. E tekintetben uniós szinten a GDPR és az ePrivacy Irányelv rendelkezései irányadóak.

3.1.1.1 Általános Adatvédelmi Rendelet (GDPR)

A GDPR tartalmazza a személyes adatok kezelésével összefüggő elveket, valamint az adatok szabad áramlására vonatkozó szabályokat, biztosítva ezzel a természetes személyek alapvető jogait és szabadságait. Ebből kifolyólag a GDPR alkalmazandó minden olyan kereskedelmi gyakorlatra is, amely személyes adatok kezelésével jár, egészen az adatkezelés megkezdését megelőző állapottól az adatok törléséig.

- **Jogszerűség, tisztességesség és átláthatóság (5. cikk (1) bek. a) pont):** Azok a sötét megoldások, amelyek a felhasználók megtévesztésére vagy manipulálásra épülnek, ellehetetlenítik az adatkezelés átláthatóságát, így a felhasználók képtelenné válnak arra, hogy az adatkezelés jogaikra gyakorolt hatásának következményeit megismerjék és annak megfelelő tájékozott döntést hozzanak. Tipikusan ilyen sötét megoldás többek között az adatvédelmi útvesztő („privacy maze”), ahol a felhasználó elveszik az oldalak közötti navigálásban, vagy a felkavaró sötét megoldások („stirring dark patterns”) alkalmazása, amely a felhasználó érzelmi állapotát erősen pozitív vagy negatív kijelentésekkel

[2] A gyakorlatban alkalmazott sötét megoldások tekintetében jól látható, hogy egy-egy megoldás esetről-esetre vizsgálandó, hiszen nem minden gyakorlat minősül minden esetben feltétlenül sötét megoldásnak, illetve a körülményektől függően tartozhat egyik, vagy másik jogterület szabályai alá. Fontos látni ugyanakkor, hogy a jelenleg ismert sötét megoldások nagy része főként adatvédelmi, vagy fogyasztóvédelmi rendelkezések tekintetében szankcionált, a platformszabályozásra vonatkozó előírások többnyire szubszidiárius jelleggel jelennek meg azon kevés esetben, ahol a sötét megoldás nem tartozik egyik terület alá sem. Jelenleg a „végtelen görgetés” és az „automatikus betöltés” esetei tartozhatnak ide, ugyanakkor ezekben az esetekben is szükséges a körülmények gondos mérlegelése, ugyanis amennyiben a végtelen görgetés nem egy közösségi médiaplatformon kerül alkalmazásra, hanem egy weboldalon nehezíti meg az általában az oldal alján található impresszum, és így az adatkezelési tájékoztató elérését, úgy már a sötét megoldás alkalmazása adatvédelmi szempont szerint kerül megítélésre. Az automatikus betöltés megítélése és annak sötét megoldásként történő azonosítása újdonságának köszönhetően még vitatott, ezzel kapcsolatos további információt lásd. 9. oldalon.

befolyásolja, ezzel késztetve őt olyan cselekvésre, amely aláássa adatvédelmi érdekeit (lsd. 1.2.2 Fogalomalkotási kísérletek, „*megtévesztés és leplezett jelleg*” példája).

- **Célhoz kötöttség és adattakarékosság (5. cikk (1) bek. b) és c) pontok):** Azok a sötét megoldások, amelyek a szükségesnél több személyes adat megadására ösztönzik a felhasználót azáltal, hogy tömeges és ismétlődő kérésekkel, ún. többletcselekvéssekkel („forced action”) terhelik őket a hozzájárulásuk vagy az adatok új adatkezelési célhoz történő megadása érdekében, sértik a GDPR rendelkezéseit.
- **Hozzájárulás (4. cikk 11. pont, 6., 7. cikk):** A jogszerű adatkezeléshez megkövetelt érvényes felhasználói hozzájárulás tekintetében a GDPR hangsúlyozza, hogy a hozzájárulásnak szabadon megadottnak, konkrétnak, tájékozottnak és egyértelműnek kell lennie. Az ezt a követelményt sértő leggyakrabban alkalmazott sötét megoldások az előre bepipált jelölőnégyzetek („Pre-ticked checkboxes”) vagy más hasonló, a hozzájárulást feltételező alapértelmezett beállítások.
- **A tájékoztatáshoz való jog (12-14. cikk):** A GDPR biztosítja a felhasználók számára a személyes adataik gyűjtéséről és kezeléséről szóló tájékoztatáshoz való jogot. A vállalkozásoknak világos, tömör és könnyen hozzáférhető tájékoztatást kell nyújtaniuk elsősorban az adatkezelés céljairól, jogalapjáról, az adatok címzettjeiről és a felhasználók jogairól. Az olyan sötét megoldások, amelyek elfedik vagy elrejtik ezeket az információkat, aláássák a felhasználók tájékoztatáshoz való jogát. A gyakorlatban ilyen megoldás lehet, amikor a vállalkozások a felhasználó számára ténylegesen nem elérhető, sehova nem mutató linkeket nyújtanak (“dead end trails”); vagy amikor a felhasználót félrevezetik a megadott adatkezelési információk és a tényleges adatkezelési műveletek közötti ellentmondások.
- **Tiltakozáshoz való jog (21. cikk)** Bár a sötét megoldások nem kapcsolódnak kifejezetten a 21. cikkhez, alkalmazásuk mégis akadályozhatja vagy megnehezítheti a tiltakozáshoz való jog gyakorlását a manipulatív tervezési technikákon keresztül, amelyek befolyásolhatják a felhasználói viselkedést. A sötét megoldások például megnehezíthetik a tiltakozási mechanizmus megtalálását az adatvédelmi beállításokon belül, vagy szándékosan összezavarhatják a felhasználókat bonyolult nyelvezet használatával.
- **Beépített és alapértelmezett adatvédelem (25. cikk):** Az itt szabályozott beépített és alapértelmezett adatvédelem követelménye alapján a személyes adatok kezelésén alapuló alkalmazások, szolgáltatások, valamint termékek esetében nem csak a felhasználás, de már a tervezés és a fejlesztés során is arra kell törekednie az előállítónak, hogy biztosítsák az adatvédelmi jogokat és a követelményeknek való megfelelést. Az alapértelmezett beállítás semmiképpen sem foglalhatja magába olyan személyes adatok gyűjtését, amelyek nem szükségesek a konkrét adatkezelési cél eléréséhez, egyes sötét megoldások alkalmazása viszont mégis arra ösztönzi a felhasználókat, hogy hagyják figyelmen kívül az adatvédelemhez való jogaikat, például a korábban említett előre bepipált jelölőnégyzetek („pre-ticked checkboxes”), rejtett információk („hidden information”), vagy kényszerített regisztráció („forced registration”), megszegve ezzel a GDPR 25. cikke által támasztott elvárásokat. (EDPB, 2019) E cikk vonatkozásában a tisztességesség elve („*fairness by*

design”) (Rachadel, 2022) is nagy hangsúlyt kap, miszerint az adatkezeléssel kapcsolatos információkat és lehetőségeket objektív és semleges módon kell megadni, elkerülve a megtévesztő vagy manipulatív nyelvezetet vagy kialakítást. (EDPB, 2022)

3.1.1.2 Az elektronikus hírközlési adatvédelmi irányelv (ePrivacy Irányelv)

Az ePrivacy Irányelv célja a felhasználók magánéletének védelme a digitális térben az elektronikus hírközlés és elektronikus kommunikációs eszközök használata során.

- **Hozzájárulás a sütik elhelyezéséhez (5. cikk (3) bek.):** Az ePrivacy Irányelv sötét megoldások által leggyakrabban megsértett rendelkezése, a sütik elhelyezéséhez szükséges hozzájárulások megszerzése körében azonosítható. A weboldalak üzemeltetőinek ugyanis be kell szerezniük a felhasználók hozzájárulását, mielőtt sütiket vagy hasonló nyomkövető technológiákat helyeznének el az eszközeiken, vagy azokhoz hozzáférnének, kivéve, ha a (i) süti célja az olyan műszaki tárolás vagy műszaki hozzáférés, amelynek kizárólagos célja az elektronikus hírközlő hálózaton keresztül történő közléstovábbítás vagy annak megkönnyítése, vagy (ii) a süti az előfizető vagy felhasználó által kifejezetten kért, információs társadalommal összefüggő szolgáltatás nyújtásához feltétlenül szükséges. Ennek megfelelően, az olyan sötét megoldások, amelyek manipulálják vagy becsapják a felhasználókat a hozzájárulásuk megadása érdekében, mint például az „összes elfogadása” gomb hangsúlyosabb színnel történő kiemelése a süti beállításoknál, ellentétesek az ePrivacy Irányelv követelményeivel.
- **Nem kívánt tájékoztatás (13. cikk):** Az olyan sötét megoldások, amelyek megtévesztik a felhasználókat, annak érdekében, hogy a korábban megadott elérhetőségi adataikat más célokból is felhasználják vagy feliratkozzanak nem kívánt kommunikációra, a nem kívánt tájékoztatás tilalmába ütköznek.

3.1.2 A sötét megoldások fogyasztóvédelmi szempontú megítélése: a fogyasztó választási szabadsága, lehetősége a tájékozott döntés meghozatalára

Fogyasztóvédelmi szempontból a sötét megoldások kihívást jelentenek a fogyasztók választási szabadságának biztosítására nézve, amely aláássa a szabad és autonóm döntéshozatal elvét. Az alkalmazott megoldások átláthatóságának hiánya megnehezíti a fogyasztók számára, hogy teljes mértékben megértsék döntéseik következményeit, így akadályozva őket abban, hogy valóban tájékozott döntéseket hozzanak. Az alkalmazandó rendelkezések az alábbiakban bemutatottak szerint irányelvi szinten szabályozottak.

3.1.2.1 A tisztességtelen kereskedelmi gyakorlatokról szóló irányelv (UCPD)

Az UCPD a fogyasztók termékekkel kapcsolatos ügyleti döntéseit közvetlenül befolyásoló kereskedelmi gyakorlatokkal foglalkozik. Bár az UCPD kifejezetten nem nevesíti a sötét megoldásokat, az irányelvben foglalt elvi alapú rendelkezések és tilalmak, mint a tisztességtelen gyakorlatokra, a megtévesztő kereskedelmi gyakorlatokra és az agresszív kereskedelmi gyakorlatokra vonatkozó rendelkezések, közvetve mégis szabályozzák a sötét megoldások alkalmazását (Európai Bizottság, 2021a).

- **A "kereskedelmi gyakorlat" fogalma (2. cikk d) pont):** Az UCPD egyik legfontosabb rendelkezése a "kereskedelmi gyakorlat" fogalmának definiálása, amely magában foglal

minden olyan kifejtett tevékenységet, mulasztást, magatartási formát vagy megjelenítési módot, illetve kereskedelmi kommunikációt, beleértve a reklámot és a marketingkommunikációt is, amely közvetlenül kapcsolódik egy termék fogyasztó részére történő eladásösztönzéséhez, értékesítéséhez vagy szolgáltatásához. Ennek megfelelően azok a sötét megoldások, amelyek a termékek népszerűsítése vagy értékesítése során alkalmazott megtévesztő vagy félrevezető állításokat, mulasztásokat vagy manipulatív cselekményeket tartalmaznak, a „kereskedelmi gyakorlat" fogalmának körébe tartozhatnak.

- **A tisztességtelen kereskedelmi gyakorlatok általános tilalma (5. cikk):** Az UCPD a tisztességtelen gyakorlatokat úgy határozza meg, mint olyan megtévesztő, agresszív vagy a szakmai gondosság követelményeivel egyébként ellentétes gyakorlatokat, amelyek alkalmasak a fogyasztók gazdasági magatartásának lényeges torzítására. E rendelkezés értelmében a legtöbb sötét megoldás tisztességtelen gyakorlatnak minősülhet, amely manipulálja vagy megtéveszti a fogyasztókat, annak érdekében, hogy olyan döntést hozzanak, amelyet egyébként nem hoztak volna meg.
- **Megtévesztő tevékenységek (6. cikk):** A megtévesztő gyakorlatok hamis információkat tartalmaznak, illetve alkalmasak arra, hogy félrevezessék a felhasználót, annak érdekében, hogy olyan ügyleti döntésre jussanak, amelyet egyébként nem hoztak volna meg. Ide tartozhatnak különösen az olyan sötét megoldások, amelyek megtévesztő kialakítással, félrevezető információkkal vagy manipulatív technikákkal próbálják megtéveszteni a fogyasztókat, mint a félrevezető akció („misleading action"), vagy félrevezető hirdetés ("misleading advertising").
- **Megtévesztő mulasztások (7. cikk):** Az UCPD ezen rendelkezése tiltja, hogy a ténybeli körülmények alapján – figyelembe véve annak valamennyi jellemzőjét és feltételét, valamint kommunikációs eszközeinek korlátait is –, az átlagfogyasztó tájékozott ügyleti döntéséhez szükséges jelentős információkat hagyjon ki a kereskedő, ezáltal ténylegesen vagy valószínűsíthetően ahhoz vezetve az átlagfogyasztót, hogy olyan ügyleti döntést hozzon, amelyet egyébként nem hozott volna. A 7. cikk szerinti megtévesztő kereskedelmi gyakorlatnak tekinthetők például a megtévesztő kialakítást, rejtett költségeket („hidden costs"), hamis állításokat („misleading statements from consumers") vagy egyéb félrevezető technikákat alkalmazó sötét megoldások.
- **Agresszív kereskedelmi gyakorlatok (8-9. cikk):** Az UCPD 8. cikke az agresszív kereskedelmi gyakorlatokkal foglalkozik, és megtiltja a kereskedőknek, hogy olyan gyakorlatot folytassanak, amely magában foglalja a zaklatást, a kényszerítést, beleértve a fizikai erőszakot is és a nem megengedett befolyást, amely jelentősen korlátozza vagy valószínűleg jelentősen korlátozza az átlagfogyasztó választási szabadságát vagy magatartását. Bár a sötét megoldások nem feltétlenül járnak agresszióval, az alkalmazott manipulatív vagy kényszerítő technikák potenciálisan az agresszív kereskedelmi gyakorlatok körébe tartozhatnak, akárcsak a csótányhotel („roach motel") vagy a rejtett feliratkozás („hidden subscription").

Az UCPD I. melléklete tartalmazza a minden körülmények között tisztességtelennek minősülő kereskedelmi gyakorlatok ún. fekete listáját, amely az Fttv. mellékleteként került átültetésre a magyar

jogba. Ugyan a melléklet sem említi kifejezetten a sötét megoldásokat, bizonyos, a sötét megoldásokkal kapcsolatos gyakorlatok, mint például a valótlan vagy megtévesztő állítások (I. melléklet 1-5. pont); a fogyasztó azonnali döntéshozatalra kényszerítése (I. melléklet 7. pont); vagy az átverés (I. melléklet 31. pont) tilalma közvetetten szabályozottak.

3.1.2.2 A fogyasztói jogokról szóló irányelv (CRD)

A CRD irányelv a távollevők között és az üzlethelyiségen kívül kötött szerződésekkel, valamint az ezektől eltérő szerződésekkel kapcsolatban nyújtandó tájékoztatásra vonatkozó szabályokat állapít meg. Az UCPD-hez hasonlóan a CRD sem tartalmaz kifejezett utalást a sötét megoldásokra, közvetve mégis alkalmazandóak rendelkezései a sötét megoldások által vezérelt gyakorlatokra, mint például a félrevezető felhasználói felületre vagy a zavaros web-, alkalmazáskialakításra, amennyiben azok CRD-ben meghatározott követelmények megkerülését jelentik (Európai Bizottság, 2021b)

- **Tájékoztatási követelmények (6. cikk):** A CRD részletes követelményeket határoz meg arra vonatkozóan, hogy a vállalkozásoknak milyen tájékoztatást kell nyújtaniuk a felhasználók számára vásárlás előtt. Ez magában foglalja a termék vagy szolgáltatás fő jellemzőire, a teljes árra, az esetleges további költségekre és a szerződés feltételeire vonatkozó világos és átlátható tájékoztatást. E tájékoztatási követelmények célja a megtévesztő gyakorlatok megelőzése, valamint annak biztosítása, hogy a fogyasztók pontos és átlátható információkkal rendelkezzenek, mielőtt döntést hoznának. A sötét megoldások tekintetében ide tartozik többek között a rejtett költségek („hidden costs”), vagy a halhatatlan fiók („immortal account”) alkalmazása.
- **A távollevők között kötött szerződések formai követelményei (8. cikk):** Tiltottak a felhasználók számára hátrányos rendelkezéseket tartalmazó szerződési feltételek, amelyeket nem egyedileg tárgyaltak meg és jelentős egyensúlyhiányt teremtenek a felek jogai és kötelezettségei között. Bár e cikk nem kifejezetten a sötét megoldásokat adresszálja, célját tekintve alkalmazható az azok elleni fellépésre is. Az egyik leggyakoribb sötét megoldás ebben a körben a rejtett előfizetés („hidden subscription”) vagy kényszerű folytonosság („forced continuity”) alkalmazása.
- **Többletösszegek fizetése (22. cikk):** A CRD 22. cikke alapján amennyiben a vállalkozás a fő szerződéses kötelezettsége teljesítéséért járó ellenértéken felül további pénzbeli követeléssel él, a felhasználót mindaddig nem köti a szerződés, illetve az ajánlat, amíg ennek megfizetéséhez kifejezetten hozzá nem járult. Ez a rendelkezés az egyik legelterjedtebb sötét megoldást, a rejtett költségek („hidden costs”) gyakorlatát tiltja.

3.1.2.3 A tisztességtelen szerződési feltételekről szóló irányelv (UCTD)

Az UCTD irányelv védi a felhasználókat a vállalkozások által alkalmazott tisztességtelen általános szerződési feltételekkel szemben. Az irányelv az áruk és szolgáltatások vásárlására vonatkozó szerződésekre vonatkozik, így a fogyasztási cikkek online vásárlására is.

- **Egyedileg meg nem tárgyalt szerződési feltételek (3. cikk):** Az UCTD 3. cikkét sértik a sötét megoldásokon keresztül beépített olyan szerződési feltételek, amelyek

tisztességtelenül hátrányos helyzetbe hozzák a felhasználókat, vagy jelentős egyensúlyhiányt okoznak.

- **Világos és érthető feltételek (5. cikk):** A bonyolult nyelvezetet, apró betűs részeket vagy rejtett záradékokat használó megoldások az UCTD 5. cikkében foglalt rendelkezésekbe ütközhetnek, hiszen nem biztosítják az elvárt átláthatóságot és egyértelműséget, így a szándékos vagy nyilvánvaló kétértelműség is („trick questions").

3.1.3 Az alkalmazott megoldások megítélése online platformszabályozás vonatkozásában

Az adatvédelem és a fogyasztóvédelem mellett az online platformok szabályozásának területe is tartalmaz releváns rendelkezéseket a sötét megoldások vonatkozásában. **3.1.3.1 Az elektronikus kereskedelemről szóló irányelv (Eker Irányelv)**

A Eker Irányelv elsősorban az online szolgáltatások jogi kereteinek létrehozására és az információs társadalom szolgáltatásainak az Európai Unión belüli szabad mozgásának előmozdítására összpontosít. Az Eker Irányelv a tisztességtelen gyakorlatok szempontjából a rejtett hirdetésekkel („hidden advertising") és a rejtett információkkal („hidden information") kapcsolatban bír relevanciával.

- **Adatszolgáltatás (6. cikk):** Az Eker Irányelv 6. cikke szerint annak a kereskedelmi tájékoztatásnak, amely az információs társadalommal összefüggő valamely szolgáltatás részét képezi, vagy maga annak minősül, világosan azonosíthatónak kell lennie.
- **Tájékoztatási kötelezettség (10. cikk):** Ezen túlmenően az 10. cikk alapján a szolgáltatók kötelesek a szerződéskötés előtti tájékoztatást világos, érthető és egyértelmű módon elérhetővé tenni a felhasználók számára.

3.1.3.2 Az online közvetítői szolgáltatások üzleti felhasználói számára a méltányosság és az átláthatóság előmozdításáról szóló rendelet (P2B Rendelet)

A P2B rendelet elsősorban az online közvetítő szolgáltatások, online keresőmotorok és az üzleti felhasználók közötti kapcsolatokat szabályozza, főként átláthatósági és kiszámíthatósági követelményeket támasztva.

- **Rangsorolás (5. cikk):** A P2B Rendelet 5. cikke rendelkezik úgy, hogy meg kell határozni az áruk és szolgáltatások rangsorolásának meghatározására szolgáló főbb paramétereket, ami nemcsak az üzleti felhasználók, hanem a fogyasztók számára is fontos, különösen a személyre szabott rangsorolással összefüggésben. Ez a rendelkezés biztosítja, hogy a platformok ne használhassák a sötét megoldásokat arra, hogy tisztességtelenül vagy önkényesen, alapos indoklás nélkül korlátozzák a szolgáltatásaikhoz való hozzáférést.

3.1.3.3 Audiovizuális médiaszolgáltatásokról szóló irányelv (AVMSD)

Az AVMSD az audiovizuális médiaszolgáltatások szabályozási kereteit határozza meg, amelynek hatálya kiterjed a videómegosztó szolgáltatásokra is.

- **Audiovizuális kereskedelmi közlemény (9. cikk):** Ennek megfelelően a videómegosztó platformoknak meg kell felelniük az AVMSD 9. cikk (1) bekezdésében meghatározott követelményeknek a saját maguk által forgalmazott, értékesített vagy szervezett kereskedelmi közlemények tekintetében, és megfelelő intézkedéseket kell tenniük a

megfelelés biztosítására a nem saját maguk által forgalmazott, értékesített vagy szervezett kereskedelmi közlemények tekintetében. Az AVMSD a videómegosztó platformokon megjelenő audiovizuális kereskedelmi közleményekre vonatkozó közzétételi követelményeket is tartalmaz, és előírja, hogy a kereskedelmi közleményeknek, mint olyannak, könnyen felismerhetőknek kell lenniük; továbbá tiltja a burkolt audiovizuális kereskedelmi közleményt. Az AVMSD rendelkezései alapján az audiovizuális kereskedelmi közlemények nem alkalmazhatnak tudatosan nem észlelhető (ún. szubliminális) technikákat sem. Ezek a rendelkezések a videómegosztó szolgáltatásokon és a közösségi médiában megjelenő álcázott hirdetések („disguised advertisements"), valamint a célzott reklámok („personalized advertisements") közzététele szempontjából relevánsak.

3.1.3.4 Digitális szolgáltatásokról szóló jogszabály (DSA)

A DSA célja a közvetítő szolgáltatásokra alkalmazandó szabályok harmonizálása, a belső piacon, biztonságos, kiszámítható és megbízható online környezetet teremtve. A DSA célozza a jogellenes tartalmak, valamint a dezinformáció online terjesztésének visszaszorítását, és ezáltal azok társadalmi kockázatának csökkentését.

- **Sötét megoldások definíciója ((67) és (68) preambulumbekezdések):** A korábban ismertetett jogszabályokkal ellentétben a DSA (67) preambulumbekezdése már kifejezetten említi a sötét megoldásokat, amelynek keretében a DSA megtiltja az online platformot üzemeltető szolgáltatók számára a felhasználók megtévesztését vagy ösztönzését („nudging"), továbbá a felhasználók autonómiájának, döntéshozatalának vagy választásának torzítását, akadályozását. A DSA (68) preambulumbekezdése tovább árnyalja a (67) preambulumbekezdés szerinti definíciót, így nyújtva átfogó képet a DSA megközelítéséről. A DSA (67) preambulumbekezdés elismeri, hogy az uniós jognak megfelelő jogszerű gyakorlatok, mint a hirdetések, önmagukban nem tekintendők sötét megoldásnak, viszont a DSA (68) preambulumbekezdésével együtt olvasva válik csak egyértelművé, hogy a DSA pontosan milyen átláthatósági követelményeket támaszt az online hirdetésekkel szemben azok jogszerűségének biztosítása érdekében.

- **Online interfész tervezése és kialakítása (25. cikk):** A DSA 25. cikke a preambulum bekezdésekben foglaltakkal összefüggésben kifejezett kötelezettséget teremt az online interfészek tervezésével és kialakításával kapcsolatban. Ennek megfelelően az online platformot üzemeltető szolgáltatók interfészeik tervezése, kialakítása, valamint üzemeltetése során kötelesek szem előtt tartani, hogy azok ne tévesszék meg, vagy manipulálják a szolgáltatásaikat igénybe vevőket, illetve más módon se torzítják vagy gyengítsék a szolgáltatásaikat igénybe vevők szabad és tájékozott döntéshozatalra való képességét. Ez a rendelkezés párhuzamot mutat az adatvédelem területén megalkotott „privacy by design", azaz beépített adatvédelem elvével, amely a GDPR 25. cikkében kifejezett kötelezettségként jelentkezik. A DSA 25. cikkében foglalt tilalom egyfajta „*fairness by design*"-ként értelmezhető, amely arra kötelezi az online platformot üzemeltető szolgáltatókat, hogy a DSA 25. cikk (1) bekezdésben foglalt szempontokat már az online interfészek kialakításának megtervezésekor figyelembe vegyék. A DSA 25 cikk (1) bekezdésében foglalt tilalom a DSA 25. cikk (2) bekezdés értelmében egy szubszidiárius szabály, amely azokban az esetekben és azon sötét megoldásokra alkalmazható, amelyek

nem tartoznak sem a fogyasztóvédelmi jogi, sem az adatvédelmi jogi szabályozás alá. A gyakorlatban megjelenő sötét megoldások közül ilyen lehet például a feltételezhetően digitális függőséget okozó megoldások közül a végtelen görgetés („infinite scroll”), amely elrejti az alternatív választási lehetőségeket, vagy az alapértelmezett automatikus lejátszás/betöltés („autoplay”) funkció, amely lényegében az előválasztás egy formájaként is értelmezhető lenne – az automatikus lejátszás egyelőre még került azonosításra átfogó sötét megoldásokat tárgyaló taxonómiákban. Kérdéses ugyanakkor, hogy a DSA milyen elhatárolás alapján sorolja az egyes sötét megoldásokat az egyes jogágak/jogszabályok alá. Az egyik legnagyobb kihívás annak elkerülése, hogy a GDPR kiskapuként működjön bármely online platformot üzemeltető szolgáltató számára egy használt sötét megoldás további használatára. Erre példa lehet a DSA 25. cikk (1) és (3) pontban felsorolt felhasználó döntéshozatala befolyásolásának tilalma. Ebben az esetben az online platformot üzemeltető szolgáltató a GDPR 12-14. cikkeiben foglalt átláthatósági követelmény szerint egyértelművé teszi a felhasználó számára, hogy a döntése mit jelent, ugyanakkor ezt az információt megadhatja sötét megoldás formájában. A DSA szerint ez a 25. cikk (1) pontja szerinti tiltott cselekménynek minősül, a GDPR alapján azonban nem az.[3]

Továbbá a DSA 25. cikk (3) bekezdése a Bizottságra hagyja egyes sötét megoldások nevesítését, ami ahhoz vezethet, hogy a szabályozás – legalábbis kezdetben – a sötét megoldások szűk, a Bizottság által kifejezetten nevesített körére fog korlátozódni, ahelyett, hogy i) taxatív listát nyújtana sötét megoldásokról, vagy ii) általános definíció alkalmazásával teret engedne *az a maiore ad minus* következtetésen alapuló absztrakciós szabályozásnak.

3.1.3.5 Digitális piacokról szóló jogszabály (DMA)

A DMA célja olyan rendelkezések meghatározása, amelyek hozzájárulnak a belső piac megfelelő működéséhez, biztosítva a versengő jelleget és a tisztességességet a digitális ágazat piacai, így különösen a kapuőrök által nyújtott alapvető platformszolgáltatások üzleti felhasználói és végfelhasználói számára.

- **Kapuőrök kötelezettsége ((63) és (70) preambulumbekezdések, 13. Cikk (6) bekezdése):** A DMA a kapuőrök vonatkozásában tiltja meg a (70) preambulumbekezdésében a felhasználói felület, vagy annak egy része, funkciója, vagy működési módja olyan kialakítását, amely a felhasználói autonómiát, döntéshozatalt vagy választást aláássa, vagy csorbítja. Ezáltal a DMA sui generis kötelezettséget teremt a DSA-hoz hasonlóan a sötét megoldások elkerülésére vagy beszüntetésére, különösen a 13. cikk (6) bekezdésével. A DMA (63) preambulumbekezdésében külön nevesítésre kerül a "pókháló" módszer tilalma is, így a kapuőrök nem nehezíthetik meg szükségtelenül vagy tehetik bonyolulttá az üzleti felhasználók és a végfelhasználók leiratkozását. Ehhez

[3] Ugyanennek fordított esete a DSA 25. cikk (2) bekezdése szerint eleve nem fordulhat elő, tekintettel arra, hogy amennyiben egy sötét megoldás alkalmazása a GDPR alatt jogellenes, arra a DSA ab ovo nem alkalmazható.

hasonlóan a fiók megszüntetése vagy a leiratkozás sem lehet bonyolultabb, mint a fiók létrehozása vagy a szolgáltatásra való előfizetés.

3.2 Magyar szabályozási háttér

3.2.1 Az alkalmazott megoldások adatvédelmi szempontú megítélése

A magyar szabályozás tekintetében is az előző pontban ismertetett jogterületeken átívelő szabályozás az irányadó tagállami voltából adódóan. Ennek megfelelően az adatvédelmi szabályozást tekintve Magyarországon is a GDPR és az ePrivacy Irányelv rendelkezéseit kell irányadónak tekinteni. Érdemes ugyanakkor megemlíteni az Eht.-t is, ami tárgyát tekintve ugyan nem kifejezetten a platformszabályozás területére tartozik, azonban a 162. § rendelkezése irányadó abban az esetben, amennyiben marketing célú megkeresésekhez online felhasználói felületen keresztül szerzik meg - sötét megoldás alkalmazásával - a felhasználó hozzájárulását. Az elektronikus hirdetések vonatkozásában az Ekertv. 14. § (1) – (2), (5) bekezdései tartalmaznak releváns előírásokat, amely szabályokat a Grt. 6. §-a egészít ki a közvetlen üzletszerzési célú megkeresések tekintetében az előzetes, egyértelmű, és kifejezett hozzájárulás követelményével.

3.2.2 Az alkalmazott megoldások fogyasztóvédelmi szempontú megítélése

A fogyasztóvédelmi rendelkezések tekintetében szintén elmondható, hogy kifejezetten egyik jogszabály sem nevesíti a sötét megoldásokat, ugyanakkor az EU szabályozási keretrendszerhez hasonlóan, a sötét megoldások az általános fogyasztóvédelmi rendelkezések követelményeibe ütközhetnek.

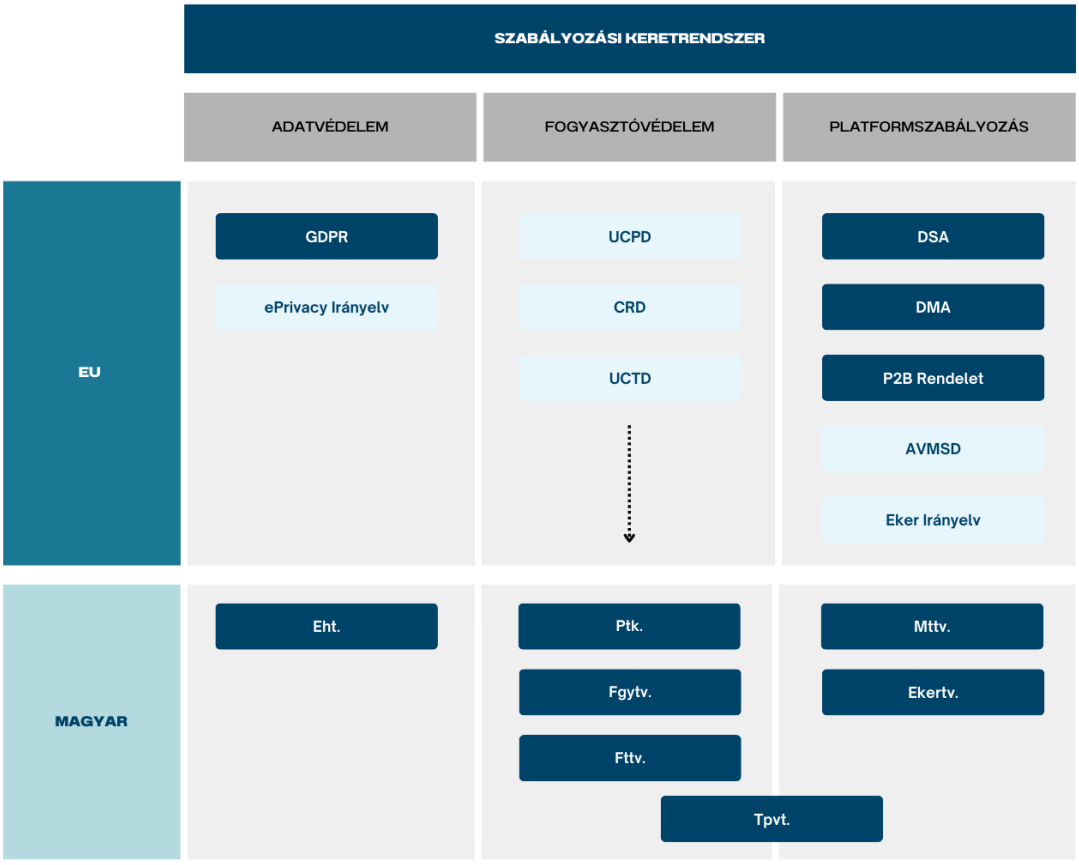
Alkalmazandó szabályokat találhatunk nemzeti szinten a Ptk., mint háttérjogszabály 6:104 §-ban, amely tételesen felsorolja a fogyasztói szerződés esetén tisztességtelennek minősülő kikötéseket, amelyek irányadóak a sötét megoldások alkalmazása esetén is, amennyiben azok kifejezetten az általános szerződési feltételekben jelennek meg.

A Ptk. rendelkezései mellett az EU-s irányelveket nemzeti jogba átültető magyar fogyasztóvédelmi jogszabályok bírnak relevanciával, mint az Fttv., és az Fgytv. Az Fttv. 3. § (1) bek. általános elvként mondja ki a tisztességtelen kereskedelmi gyakorlat tilalmát. Az Fttv. 3. § (2) bek. szerint ilyen az a gyakorlat, amely rontja a fogyasztó lehetőségeit az elegendő információn alapuló tájékozott döntéshozatalra, vagy a fogyasztót olyan magatartás megtételére készteti vagy késztetheti, amelyet egyébként nem tett volna meg – utóbbit az Fttv. „megtévesztő mulasztás”-ként nevesíti. Ilyen értelmében a 3. § (3). bek. szerint tisztességtelen különösen a megtévesztő (6. § és 7. §) és az agresszív (8. §) kereskedelmi gyakorlat. Az Fttv. melléklete tartalmazza az UCPD szerinti feketelista átültetését. Az Fgytv. 2008 júniusában került módosításra annak érdekében, hogy az UCPD rendelkezéseit átültesse. Az implementálás keretében átalakításra került az Fgytv. fogalmi rendszere (Fgytv. 1-2. §), így egységesítésre került többek között a „fogyasztó”, a „vállalkozás/kereskedő”, a „termék/áru/szolgáltatás”, valamint a „kereskedelmi kommunikáció/reklám/hirdetés” fogalomköre. Az átültetés keretében az Fgytv. néhány anyagi jogi szabálya hatályon kívül helyezésre került (Fgytv. 9. §, "fogyasztók tájékoztatása” című IV. fejezet), mivel az azokban megfogalmazott követelmények az irányelv anyagi jogi jellegű átültetését tartalmazó Fttv.-ben nyertek szabályozást.

3.2.3 Az alkalmazott megoldások platformszabályozási szempontú megítélése

Platformszabályozás tekintetében elsősorban az európai uniós szintű jogszabályok bírnak relevanciával, azonban mégis megtalálható a magyar szabályozásban is néhány irányadó rendelkezés. Az AVMSD Irányelv átültetését Magyarország több jogszabály módosításával valósított meg, ezek közül főként az Mttv. és az Ekertv. emelendőek ki, ugyanis a videómegosztóplatform-szolgáltatással összefüggő irányelvi rendelkezések az Ekertv.-be, míg videomegosztóplatform-szolgáltatás és a videomegosztóplatform-szolgáltató fogalmak meghatározására vonatkozó szabályok az Mttv.-be kerültek átültetésre. A DMA hatálybalépésére tekintettel módosításra került a Tpvt. is, amely új jogkörrel ruházta fel a GVH-t, így a Tpvt. 80/S § (2) bekezdésben foglaltak alapján a GVH versenyfelügyeleti eljárást indíthat annak megállapítása érdekében, hogy álláspontja szerint a jelentős piaci hatású digitális platformszolgáltatók (ún. kapuőrök) megfelelnek-e DMA-ban foglalt kötelezettségeiknek.

Az alábbi 3. ábra tartalmazza a jelen 3. fejezetben kifejtett szabályozási keretrendszer szemléltetését.



3. ábra: A sötét megoldások jogi szabályozásának uniós és magyar keretrendszere

4. Jogalkalmazási gyakorlat

4.1 Magyar szabályozási gyakorlat

A magyar jogalkalmazási gyakorlatban is léteznek kifejezetten a sötét megoldások tárgyában hozott döntések, függetlenül attól, hogy ezekben a sötét megoldás kifejezés, mint olyan, nem szerepel. Lehetséges magyarázat erre, hogy a magyar jogalkotásban a DSA alkalmazandóságát megelőzően a sötét megoldások definíció, mint olyan nem létezett, és a szabályozó hatóságokon belül sincs általánosan bevett magyar szóhasználat, így pl. a „sötét megoldások" mellett a „sötét mintázatok" is használatos (ezt a kérdést a DSA a „sötét megoldások" bevezetése által, *de lege ferenda* rendezi). A kérdéskör vizsgálatakor főként a NAIH és a GVH döntései tekinthetők relevánsnak.[4]

4.1.1 NAIH döntések

A NAIH a sötét megoldások alkalmazását a GDPR 57. és 58. cikkeiben meghatározott feladat- és hatáskörei alapján és az Infotv. VI. fejezetében szabályozott eljárások során adatvédelmi megfelelés szempontjából vizsgálja. Ennek megfelelően a NAIH által vizsgált esetek kizárólag olyan sötét megoldásokat tárgyalnak, amelyek egyben a személyes adatok GDPR rendelkezéseivel ellentétes kezelését valósítja meg.

Adatkezelő: **szálláshely szolgáltató társaság, pontos név ismeretlen[5]**	**Azonosítható sötét megoldás:** csempészés, félrevezetés, többletcselekvés, „csótánymotel" (nehéz lemondás)	**Jogsértéssel érintett jogszabályhely**: GDPR 5. cikk (1) bek., 6. cikk (1) bek., 7. cikk (1) bek., 12. cikk (1) bek., 17. cikk (1) bek.
Az adatkezelő szállásfoglalásokat lehetővé tevő weboldala üzemeltetése során közvetlen üzletszerzési célú elektronikus hírlevelek („elektronikus direktmarketing", „**EDM**") küldéséhez kapcsolódóan félrevezető információkat adott meg adatkezelési tájékoztatójában, mivel azt állította, hogy a weboldalon szálláshelyet foglaló felhasználók e-mail címének EDM küldése céljából való kezelése jogalapja a GDPR 6. cikke (1) bek. a) pontja szerinti hozzájárulás, miközben az adatkezelési tájékoztatóban az adatkezelő jogos érdeke szerepelt. Ez a rejtett információ alkalmas a felhasználók összezavarására, hogy valójában melyik jogalap irányadó, ami sérti a GDPR 12. cikk (1) bekezdését. Továbbá, azon a webes felületen, ahol a felhasználók leadhatták a foglalást, annak ellenére, hogy az adatkezelési tájékoztató a hozzájárulás jogalapot jelölte a marketing célú adatkezeléshez, az adatkezelő nem helyezett el jelölőnégyzetet az EDM célú adatkezeléshez, holott ez önálló adatkezelési cél, és a hozzájárulást célonként külön jelölőnégyzet bejelölésével kell beszerezni. Végül, az adatkezelő nem biztosított lehetőséget a hírlevél-leiratkozásra az egyes hírlevelekben, ahogy ez elvárható lett volna, ami által		

[4] Jelen elemzésnek nem célja a NAIH és a GVH teljes idevágó esetjogának részletes feldolgozása, sokkal inkább a jelentősebb ügyek részletes tárgyalása, és azok alapján általános jogalkalmazási irányvonalak, esetleges tendenciák meghatározása.

[5] NAIH, NAIH-1091-10/2022.(NAIH-6936/2021) sz. határozat, 2022. július 11.

megnehezítette a hírlevél-leiratkozást, majd a felhasználók részére azt követően is küldött hírlevelet, hogy ők e-mail címük törlését kérték az adatkezelő adatbázisából. A NAIH 500.000 Ft bírságot szabott ki az adatkezelőre.		
Adatkezelő: **hírügynökség, pontos név ismeretlen[6]**	**Azonosítható sötét megoldás:** többletcselekvés, csempészés, félrevezetés	**Jogsértéssel érintett jogszabályhely**: GDPR 6. cikk (1) bek., 7. cikk (2)-(4). bek., 12. cikk (1) bek.
Az adatkezelő weboldalán a szolgáltatására történő online regisztráció esetén minden előfizetőt automatikusan az EDM-re is feliratkoztatott. A weboldalon egy jelölőnégyzet szolgált a szolgáltatás ÁSZF-ének elfogadására (amely az előfizetés feltétele) és az EDM-re történő feliratkozásra, így a regisztráció idején nem volt lehetőség csak a szolgáltatásra regisztrálni, az EDM-re történő feliratkozás nélkül. Az adatkezelő az adatkezelési tájékoztatóban sem jelölte meg, hogy lenne olyan lehetőség, hogy a szolgáltatásra történő regisztráció mellett az EDM-re nem iratkozik fel a felhasználó. A NAIH 2.000.000 Ft bírságot szabott ki az adatkezelőre.		
Adatkezelő: **TV2 Média Csoport Zrt.[7]**	**Azonosítható sötét megoldás:** többletcselekvés, adatvédelmi labirintus	**Jogsértéssel érintett jogszabályhely**: GDPR 5. cikk (1) a)-b) pontok 6. cikk (1) bek., 12. cikk (1) bek, 13. cikk (1) bek.
A NAIH az adatkezelő sütik („cookie-k") elhelyezésének gyakorlatát vizsgálta a www.tenyek.hu és a www.tv2play.hu weboldalakon. A sütik a weboldalon elhelyezhető kisméretű szöveges fájlok, amelyek a weboldalt meglátogató felhasználók egyes személyes adatait rögzítik különböző célokra (weboldal megjelenítése, teljesítményoptimalizálás, statisztikák készítése, reklámtartalmak megjelenítése). Ezek elhelyezéséhez főszabály szerint az ePrivacy Irányelv 5. cikk (3) bek. szerint a felhasználó hozzájárulása szükséges, egyes esetekben pedig elhelyezésük a weboldalt üzemeltető adatkezelő GDPR 6. cikk (1) bek. f) pont szerinti jogos érdekén alapul. A jogszerű sütielhelyezésnek mindkét esetben előfeltétele a felhasználó megfelelő tájékoztatása egy ún. cookie banneren, azaz a webes felületen megjelenő jól látható, elkülönített részen, és további részletes tájékoztatása az adatkezelési tájékoztatóban, valamint biztosítani kell a sütik elutasításának lehetőségét. A NAIH szerint a TV2 indokolatlanul akadályozta a felhasználókat a sütik elutasításában azáltal, hogy a www.tenyek.hu weboldalra érkezéskor felugró ablak jelent meg, amelyen két gomb szerepelt: az „*OK, tovább*" gombbal lehet a beállításokat látatlanul elfogadni, míg a másik, „*adatkezelési tájékoztató*" nevű gomb átirányította a felhasználót a „tv2play.hu" weboldalra. Utóbbi gombra kattintással újabb felugró ablak jelent meg a sütik kezelésére, amelyen alul az ismételten		

[6] NAIH, NAIH-7058/2022 sz. határozat, 2022. november 15.
[7] NAIH, NAIH-3195-11/2022 sz. határozat, 2022. szeptember 26.

megjelenő „*ok, tovább*” gomb mellett egy „*további lehetőségek*” gomb volt. A „*további lehetőségek*”-re kattintás esetén egy felugró ablak jelent meg „*összes elutasítása*” és „*összes elfogadása*” opciókkal, alattuk a felugró ablak körülbelül egy nyolcad részén egy görgetősávban olvasható a sütikről szóló adatkezelési tájékoztató, amelyből egyszerre átlagosan 2-4 sor volt látható. Legalul a „*partnerek*” a „*jogos érdek*” és a „*mentés és kilépés*” gombok voltak megtalálhatóak. Ennek ellenére az adatkezelési tájékoztató szerint a TV2 kizárólag a felhasználó hozzájárulása alapján helyezett el sütiket. Az az elvárás, hogy a felhasználó a „*partnerek*” fül alatt linkelt 754 partner adatkezelési tájékoztatóját elolvassa és ezeknél egyenként vonja vissza a hozzájárulást, a NAIH szerint nem átlátható és tisztességes feltétel. A NAIH a teljes cookie-elhelyezés folyamatára tekintettel megállapította, hogy "*rendkívül hosszú tájékoztató szöveg a képernyő indokolatlanul kicsi területén, egyszerre néhány soronként olvashatóan volt elérhető. [...] nem nevezhető sem tömörnek, sem világosnak. A „mindent elfogadás” az első szinten érdeminek nevezhető tájékoztatás nélkül lehetséges, a „mindent elutasítás” csak a második szinten érhető el. A TV2 által használt „jogos érdek” kifejezés egyértelműen megfeleltethető az általános adatvédelmi rendelet szerinti fogalomnak, így azt vagy teljesen tévesen használta az TV2 – és emiatt volt félrevezető a tájékoztatás –, vagy megfelelően használta, de minden tájékoztatás […] nélkül. Mindkét esetben tisztességtelen és átláthatatlan érdemben azonos célok feltüntetése a hozzájárulás és a jogos érdek felületen is, mivel azt a benyomást kelti az érintettekben, hogy a hozzájárulás meg nem adása mellett is lehetségesek ugyanazon adatkezelések […]. Ha a „jogos érdek” felületen elhelyezett célok szerinti adatkezelések hozzájárulás hiányában nem történnek meg, akkor emiatt félrevezető a tájékoztatás és a felület, ha megtörténnek, akkor amiatt*.” A NAIH ezen határozata az eddigi egyetlen sütikkel kapcsolatos adatkezelést szankcionáló hazai határozat, amely a sütik elhelyezésekor tapasztalt számos sötét megoldást tárgyal, mint a sütik elutasításának indokolatlan akadályozása a több egymást követő felugró ablakkal és átirányítással, észszerűtlen többletcselekmények megkövetelése a felhasználóktól a több, mint 700 partner egyenkénti elutasításakor, valamint a félrevezető tájékoztatás az adatkezelés GDPR 6. cikk (1) bek. a) pont szerinti hozzájárulás és f) pont szerinti jogos érdek vonatkozásában. A NAIH a TV2-re 10.000.000 Ft bírságot szabott ki.

Adatkezelő: **webáruház üzemeltető, pontos név ismeretlen[8]**	**Azonosítható sötét megoldás:** kényszerített hozzájárulás, hiányzó választási lehetőség	**Jogsértéssel érintett jogszabályhely**: GDPR 6. cikk (1) bek. a) pont, 7. cikk 2. bek.,12. cikk (4) bek.
A webáruházat üzemeltető adatkezelő a webáruházba való regisztrációkor egyetlen jelölőnégyzetet biztosított az általános szerződési feltételei és az adatkezelési tájékoztatója elfogadására, amely mellett „*Az ÁSZF elfogadásával Ön kijelenti, hogy az adatvédelmi tájékoztatót megismerte, elfogadta, és azon adatkezelési célokhoz, melynél az Érintett*		

[8] NAIH, NAIH-406-21/2022. sz. határozat, 2022. december 10.

hozzájárulása a jogalap, Ön a hozzájárulását adja az adatkezeléshez. Az adatkezelési célok a weboldal használatával, hírlevél küldéssel, weboldalról való rendeléssel, szolgáltatás igénybevételével, személyes vásárlással kapcsolatosak." szöveg szerepelt. A GDPR 6. cikk (1) bek. a) pont szerinti hozzájárulás megadása ugyanakkor adatvédelmi jogi kategória, nem válhat az ÁSZF részévé akként, hogy annak elfogadása egyben automatikusan adatkezeléshez való hozzájárulást is jelent. A GDPR 7. cikk (2) bek. értelmében, ha a felhasználó hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell megadni. Tehát a hozzájárulást az ÁSZF-től különállóan kell beszerezni, külön-külön adatkezelési célonként. Az adatkezelő által alkalmazott sötét megoldás ez esetben a választási lehetőség hiánya, azaz a felhasználó lehetőségeinek leszűkítése azáltal, hogy nem biztosított a webes felületen még egy jelölőnégyzetet.

Adatkezelő:	**Azonosítható sötét megoldás:**	**Jogsértéssel érintett jogszabályhely**:
Magyar Éremkibocsátó Kft.[9]	kényszerített hozzájárulás, hiányzó választási lehetőség	GDPR 5. cikk (1) bek. a) pont, 6. cikk (1) bek. a) pont, 12. cikk

A vizsgált ügyben az online webáruházat üzemeltető adatkezelő úgy alakította ki online felületét, hogy a webáruházban "vendégfelhasználóként" előzetes regisztrációval nem rendelkező felhasználók a vásárlás során megadott személyes adatokkal tudtuk és szándékuk nélkül egy felhasználói fiókot regisztráltak, amely tényéről a webáruházat üzemeltető adatkezelő utólagosan nyújtott tájékoztatást.

A NAIH az előzetes tájékoztatás nélkül, automatikusan létrehozott felhasználói fiók vonatkozásában megállapította, hogy a jogellenesen szerzett személyes adatok kezelése a későbbiekben sem lesz önmagában utólagos tájékoztatással és ráutaló magatartással jogszerű, ha a tájékoztatást nem követi aktív, kifejezetten csak a hozzájárulás megadását célzó cselekmény. Azaz, jogellenes adatkezelést valósít meg az az adatkezelő, aki a felhasználók előzetes tájékoztatása hiányában automatikusan hoz létre felhasználói fiókot, amennyiben utólag nem tájékoztatja a felhasználókat, és kéri hozzájárulásukat a felhasználói fiók megtartásához. A NAIH 30.000.000 Ft bírságot szabott ki az adatkezelőre.

Adatkezelő:	**Azonosítható sötét megoldás:**	**Jogsértéssel érintett jogszabályhely**:
Magyar Telekom Nyrt.[10]	csótánymotel, leiratkozás ellehetetlenítése	GDPR 5. cikk (1) bek. a) pont, 6. cikk (1) bek. a) pont, 12. cikk

A NAIH által érintetti kérelem alapján vizsgált ügyben a kérelmező érintett, aki nem az adatkezelő ügyfele, kéretlen e-mailt kapott e-mail fiókjába, mivel egy harmadik fél (a Telekom egy ügyfele)

[9] NAIH, NAIH-2501-10/2022. sz. határozat, 2022. szeptember 12.
10 NAIH-924-10/2021. sz. határozat, 2021. június 18.

tévesen adta meg e-mail címét kapcsolattartási címként. Az érintett ezt három alkalommal is jelezte a Telekom ügyfélszolgálatán, ahol adatai törlését kérte, azonban válaszul csak bejelentkezést igénylő hírlevél leiratkozási, automatikusan generált sablonüzeneteket kapott. Mivel nem volt ügyfél, nem tudott továbblépni, belépni a fiókjában és e-mail címe törlését kérni.

A NAIH határozatának sötét megoldások szabályozása szempontból releváns részei az érintett GDPR 17. cikk (1) bekezdése szerinti törlési jogának megsértésével kapcsolatos megállapítások. A NAIH kimondta, hogy sablonüzenetek ismételt küldése nem megfelelő módja az érintetti kérelmek kezelésének. Az ilyen sablonüzenetek nem tekinthetők az érintetti kérelem érdemi megválaszolásának, a nem ügyfél érintett által igénybe nem vehető leiratkozási hivatkozásra többször, változatlanul ismételt sablonszöveggel történő utalás pedig nem minősül a GDPR 12. cikk (3) és (4) bekezdések szerinti teljesítésnek, vagy megfelelően indokolt elutasító válasznak. A GDPR 17. cikk (1) bekezdés d) pontja alapján az adatkezelő köteles lett volna a Kérelmező kérelmére a kapcsolati adatot haladéktalanul törölni.

A NAIH (egyéb jogsértésekre tekintettel is) 10.000.000 Ft bírságot szabott ki az adatkezelőre.

Ugyan jelen elemzés nem nyújt taxatív ismertetést minden, az elemzés tekintetében relevánsnak ítélhető NAIH döntésről, a fenti döntések alapján önmagában levonhatóak az alábbi szabályozási tendenciák:

- A NAIH a sötét megoldásokat annyiban és olyan szempontból vizsgálja, amennyiben azok a hatályos adatvédelmi szabályrendszer, azaz elsősorban a GDPR hatálya alá esnek. Ez egyben azt is jelenti, hogy a NAIH a sötét megoldásokat tárgyaló döntéseiben a sötét megoldásokat minden esetben kizárólag adatvédelmi jogba ütközés szempontjából vizsgálta és tartotta jogellenesnek.
- A sötét megoldások alkalmazásához jellemzően a következő adatvédelmi jogsértések társulnak: GDPR 5. cikk (1) bek. a) pont szerinti tisztességes, jogszerű és átlátható adatkezelés elve, és ehhez kapcsolódóan a GDPR 12.-13. cikkei szerint a felhasználók megfelelő tájékoztatása, valamint a GDPR 6. cikk (1) bek. a) pontja és 7. cikke szerinti, felhasználó hozzájárulásával kapcsolatos jogsértés, akár a hozzájárulás lehetőségének hiánya, akár a hozzájárulás feltételhez kötése vagy visszavonása, végül a GDPR 17. cikke szerint a személyes adatok törléséhez való jog.
- Fontos látni ugyanakkor, hogy ugyanazon adatkezeléssel kapcsolatban megállapítható a GDPR sérelme a sötét megoldás alkalmazásához kapcsolódóan, valamint a sötét megoldástól függetlenül is. Más szavakkal, egy adatkezelés több szempontból is lehet jogszerűtlen, és a sötét megoldás alkalmazása miatti jogszerűtlenség mellett egyéb GDPR rendelkezés, pl. érintetti jogok, adatbiztonsági intézkedések sérelme is megállapítható, amelyek a sötét megoldás alkalmazásától függetlenek. Ennek a bírságkiszabás szempontjából lehet jelentősége, például, ha maga az adatkezelés jogszerűtlen volt azért, mert a hozzájárulás bejelölt jelölőnégyzet miatt nem volt önkéntes, majd ezt követően az adatkezelő egyéb, ettől független kötelezettségét, pl. a GDPR 32. cikke szerinti adatbiztonsági intézkedések alkalmazását elmulasztja, e két jogsértés párhuzamosan szankcionálható.

- A NAIH honlapján és éves beszámolóiban nyilvánosságra hozott határozatai között tendenciaszinten megállapítható a digitális marketingtevékenységekhez kapcsolódó sötét megoldásokra irányuló hatósági vizsgálatok relatív magasabb előfordulása egyéb felhasználási területtel szemben (pl. közösségi média platform üzemeltetése keretében túlzó mértékű személyes adatok gyűjtése felhasználói fiók létrehozásakor). A vizsgált marketingtevékenységek jellemzően a hírlevél-feliratkozásokhoz, sütik és online követő („tracking") rendszerek alkalmazásához fűződnek. A NAIH digitális marketingtevékenységre irányuló fokozott figyelme összhangban van az európai szabályozói hatósági trendekkel – az utóbbi években jelentős növekedés tapasztalható a digitális marketing, ezen belül is az online platformok (különösen a DSA alatti online óriásplatformok („very large online platform") által végzett marketingtevékenységgel vagy az általuk kínált marketingeszközökkel (pl. közösségi médiaoldalak forgalmának elemzésére épülő reklámkampányok, sütik) kapcsolatos hatósági ügyek számában.

4.1.2 A GVH tevékenysége és döntései

A GVH a célzottan a sötét megoldások alkalmazásának ellenőrzését tekintve a legaktívabb magyar szabályozó hatóság. A sötét megoldások magyar piacon való elterjedtségének felmérése céljából a GVH saját kezdeményezésre végzett szektorspecifikus gyorselemzést („sweep") az egyes légitársaságok jegyértékesítési felületeiről, amely során a platformok többségén pszichés manipulációt alkalmazó technikákat azonosított (GVH, 2022). A GVH részt vett továbbá a fenti 1.1. pontban ismertetett, az Európai Bizottság és a CPC ernyője alatt 2022 folyamán lefolytatott 399 webáruház online jelenlétét vizsgáló koordinált vizsgálati akcióban (GVH, 2023).

A főként piaci helyzetfelmérés célját szolgáló gyorselemzések és ellenőrzések mellett a GVH számos ügyben vizsgált sötét megoldásnak tekinthető kereskedelmi gyakorlatokat. Ezekben a „sötét megoldás" kifejezés nem szerepel, ugyanakkor a fenti 1.2. pontban ismertetett taxonómiák és fogalommeghatározások, valamint az egyes döntésekben vizsgált jogszabályok alapján a döntések egyaránt a sötét megoldások alkalmazásának hatósági ellenőrzéséhez kapcsolódnak.

Eljárás alá vont fél:	**Azonosítható sötét megoldás:**	**Jogsértéssel érintett jogszabályhely**:
ContextLogic B.V. és ContextLogic Inc. (együttesen ContextLogic)[11]	rejtett árazás, ún. „csepegtető árazás", visszaszámláló, sürgetés	Fttv. 3. § (1) bek., 9. § (1) bek., melléklet 7. pont
Az eljárás alá vont fél a www.wish.com weboldalon és Wish mobil applikációban elérhető Wish online piactéren az elérhető termékre kattintást követően „azonnali ajánlat" lehetőséget jelenített meg. A GVH kifogásolta, hogy az „azonnali ajánlat" részeként látható volt a „Vásárlás" gomb felett egy 4 perces visszaszámláló óra, valamint az „*Azonnali ajánlat: tedd be a kosárba most, hogy olcsóbban megvehesd!*" állítás. Ezen visszaszámláló óra lejártát követően az idézett egy mondatos állítás változatlanul továbbra is látható volt. A fizetési aloldalon megjelent egy 55 perces		

[11] GVH, VJ/22-114/2021. sz. határozat, 2023. február 16.

visszaszámláló óra a következő állítással együtt: „*Az ár hamarosan lejár! Menjen a pénztárhoz a számláló lejárta előtt, hogy megszerezze ezt az árat*.” Továbbá, a termékek árazásánál a Wish online piactér egyes termékek mellett „ingyenes”, 0 Ft-nak megfelelő árat adott meg, majd a vásárlási folyamat során adta hozzá („csepegtette”) a szállítási költséget. A versenyfelügyeleti eljárást lezáró kötelezettségvállalással a ContextLogic vállalta a visszaszámláló eltávolítását a weboldalról, és a felhasználót sürgető üzenetek mellőzését.

Eljárás alá vont fél: be2 S.á.r.l.[12]	**Azonosítható sötét megoldás:** megtévesztő információ, rejtett információ, „Privacy Zuckering”, azaz ösztönzés egyre több személyes adat megadására többletcselekvés, zavarás	**Jogsértéssel érintett jogszabályhely**: Fttv. 3. § (1) bek., 6. § (1) bek.

Az eljárás alá vont be2 a www.be2.hu weboldalon, valamint 2017. december 18-tól kezdődően a www.academicsingles.hu weboldalon elérhető online társkereső szolgáltatással kapcsolatban tisztességtelen kereskedelmi gyakorlatot valósított meg azáltal, hogy a weboldalon való regisztrációt, mint a szolgáltatás igénybevételének kötelező előfeltételét, ingyenesnek hirdette, míg a regisztrációt követően a tényleges szolgáltatás igénybevétele már díjköteles volt (prémium előfizetés). Továbbá, a felhasználói fiók létrehozását követően felugró ablak jelent meg a felhasználónak „*Szánjon időt a profiljára! Tegye feltűnőbbé!*”, és „*Legyen korrekt! Ha szeretne képeket megtekinteni, először önnek is fel kell töltenie egyet > Feltöltés most*” szövegekkel. A be2 indokolatlanul megnehezítette a profiltörlés folyamatát is, amely során terelgetés („nudging”) technikát alkalmazott a profil fenntartására bíztató üzenetekkel, pl.: „*A mi tanácsunk: Ne deaktiválja a profilját.*” A „deaktiválás” linkről elérhető aloldalon ismét választania kellett a felhasználónak: a hangsúlyosan, zöld színnel kiemelt „*Nem*” és a szürke alapon szürke színnel látható „*Profilom deaktiválása*” opció között.

A GVH a fenti jogsértésekért a be2-t 1.600.000.000 Ft bírság megfizetésére kötelezte. A GVH határozatát felülvizsgálati eljárásban mind az elsőfokon eljáró Fővárosi Törvényszék[13], mind a Kúria helyben hagyta[14]. A Fővárosi Törvényszék ítéletében a GVH határozata jogszerűségének tárgyalása mellett kitért az online térben átlagosan tájékoztatott fogyasztó koncepció értelmezésére, és megállapította, hogy „*az ingyenes regisztráció ígéretével találkozó, észszerűen tájékozott, adott helyzetben körültekintően eljáró fogyasztó alappal következtetett arra, hogy regisztrációval a funkcióját betöltő szintig a szolgáltatást ingyenesen tudja majd igénybe venni […]. A fogyasztótól nem várható el, hogy részletesen kutakodjon a fő üzenetként eljuttatni*

[12] GVH, VJ/19-120/2018. sz. határozat, 2020. július 30.
[13] Fővárosi Törvényszék, 103.K.706.642/2020/36. sz. ítélet, 2021. november 19.
[14] Kúria, Kfv.VI.37.026/2022/8. sz. ítélet, 2022. május 26.

szándékozott információ olyan elemei után, melyek az információból nem következnek, azzal ellentétesek vagy attól eltérnek”.[15]

Eljárás alá vont fél: Booking.com B.V.[16]	**Azonosítható sötét megoldás:** pszichés nyomásgyakorlás, sürgetés	**Jogsértéssel érintett jogszabályhely**: Fttv. 3. § (1) bek., 8. § (1) bek.

Az eljárás alá vont Booking.com vállalat az Fttv. 8. § (1) bek. szerinti agresszív és ezért tiltott kereskedelmi gyakorlatot alkalmazott azáltal, hogy a www.booking.com weboldalon a szálláshelyek melletti ajánlatoknál sürgető, a felhasználót pszichés nyomás alá helyező üzeneteket és felvillanó jelzéseket helyezett el, amelyek az elérhető ajánlatokat jelezték, pl. „*rajtad kívül még négyen nézik most ezt a szállást*”, „*Ezen az áron már csak egy elérhető szoba maradt*”, vagy „*Az árak emelkedhetnek! Biztosítsa foglalását még ma!*”.

A GVH ezért a gyakorlatért 2,5 milliárd forint bírságot szabott ki a Booking.com-ra. A GVH határozatában szintén tárgyalta az átlagosan tájékozott fogyasztó koncepcióját, és azzal kapcsolatban kiemelte, „*a magasabb képzettség nem jelenti az adott piacra jellemző szakismeretek meglétét, így magasabb tudatossági szintet*”, illetve, hogy adott esetben kérdéses, hogy az internet „*készségszintű*” ismerete relevánsnak tekinthető-e, figyelemmel arra, hogy „*pszichés nyomásgyakorlást megvalósító kereskedelmi gyakorlatok kapcsán a tudatosságnak egyébként is kisebb jelentősége van, hiszen ezen gyakorlatok a későbbiekben kifejtettek miatt a tudat alatti szinten (is) hatnak. Ugyanezen okból az sem releváns, ha a fogyasztók a Booking.com honlapját vagy más hasonló oldalakat rendszeresen használnak, mivel tudat alatti befolyásolás ellen kevéssé lehet jártasságot szerezni*.”[17]

Eljárás alá vont fél: PayPal (Europe) S.á.r.l. et Cie, S.C.A. (együttesen PayPayl EU)[18]	**Azonosítható sötét megoldás:** rejtett többletköltségek, rejtett információ	**Jogsértéssel érintett jogszabályhely**: Fttv. 3. § (1) bek., 7. § (1) bek.

A PayPal EU fizetési tranzakciók lebonyolításához és szolgáltatásához nyújt szolgáltatást a PayPal platformon keresztül. A PayPal platformon keresztül külföldi devizában online fizetést teljesítő felhasználók számára a PayPal EU végzi el a pénznemváltást alapértelmezés szerint saját átváltási árfolyamán, de a felhasználók választhatják a saját kártyakibocsátó bankjuk által alkalmazott, banki árfolyamon végzett átváltást is. Mivel az egyes PayPal partnerek által alkalmazott váltási árfolyamok eltérők, így a felhasználó ez irányú döntése eltérő végösszegű vételárhoz vezet, amiről a PayPal nem nyújtott megfelelő és időszerű tájékoztatást a felhasználóknak. A PayPal EU által az online fizetési felületen elhelyezett „*Átváltási lehetőségek megtekintése*” hiperhivatkozást a GVH ugyanis nem találta megfelelő tájékoztatásnak, Ehelyett az

[15] Kúria, Kfv.VI.37.026/2022/8. sz. ítélet, 2022. május 26. [25]-[26]. bek.
[16] GVH, VJ/17-110/2018. sz. határozat, 2020. április 28.
[17] GVH, VJ/17-110/2018. sz. határozat, 2020. április 28. 396-397. bek.
[18] GVH, VJ/18-120/2017. sz. határozat, 2019. május 29.

eljárást lezáró kötelezettségvállalás keretében az eljáró versenyhatóság kötelezte a PayPal EU-t a fizetési felület megjelenítésének módosítására, és az „*Átváltási lehetőségek megtekintése”* opció helyett egy „*Vagy Kártya kibocsátója árfolyamának kiválasztása*” hiperhivatkozás elhelyezésére. Így, ha a felhasználó a kártyakibocsátójának árfolyamát választja, úgy egy olyan mondat kerül megjelenítésre, amely megerősíti a felhasználó számára azt, hogy a kártyakibocsátó árfolyamát választotta a fizetéshez és felhívja a felhasználót, hogy ellenőrizze a banki értesítőjén a feltételeket és költségeket („*Fizetéshez kártyakibocsátója árfolyamát használja. Ellenőrizze banki értesítőjén a feltételeket és költségeket*.”). A felhasználó számára egy dinamikus hiperhivatkozáson keresztül azt a lehetőséget is biztosítania kell az új fizetési folyamatnak, hogy amennyiben úgy kívánja, visszatérhet a PayPal EU árfolyamra.		
Eljárás alá vont fél: Airbnb Ireland[19]	**Azonosítható sötét megoldás:** rejtett árazás, „csepegtető árazás”, megtévesztő árazás, rejtett információ	**Jogsértéssel érintett jogszabályhely**: Fttv. 3. § (1) bek., 7. § (1) bek.
A szálláshely-kereső platformot üzemeltető Airbnb Ireland a www.airbnb.hu weboldal és az Airbnb mobilalkalmazás üzemeltetése során a felhasználók elől elhallgatta, vagy homályosan és nem megfelelő időben tüntette fel a szálláshelyekkel kapcsolatos költségeket. Az Airbnb a felhasználó keresési paraméterei megadása után az ún. „listázó oldalon” megjeleníti a szálláshelyeket és a szállásárat, a további költségeket (pl. takarítás díja, szolgáltatási költség) csak később, a szálláshelyre kattintással elérhető ún. „szállás oldal” mutatja. Továbbá, az Airbnb webes és mobilapplikáció felületein ugyanazon keresési paraméterek mellett ugyanazon szálláshely különböző áron volt elérhető. A versenyfelügyeleti eljárás az Airbnb Ireland kötelezettségvállalásával zárult, amelyben az Airbnb vállalata a megtévesztő árazás és az információ rejtett megjelenítése gyakorlatának felülvizsgálatát és megszüntetését.		
Eljárás alá vont fél: Kultúrpark Zrt.[20]	**Azonosítható sötét megoldás:** rejtett árazás, „csepegtető árazás”, megtévesztő árazás, rejtett információ	**Jogsértéssel érintett jogszabályhely**: Fttv. 3. § (1) bek., 7. § (1) bek.
A GVH a Kultúrpark Zrt. által a Budapest Parkban megrendezésre kerülő koncertekre, egyéb rendezvényekre történő jegyek online értékesítése során megtévesztő kereskedelmi gyakorlatot folytatott azáltal, hogy 2019. január 1. és 2020. május 22. között a www.budapestpark.hu weboldalán, 2019. január 1. és 2021. február 11. között a Budapest Park Facebook oldalán és a jegyárat megjelenítő Facebook, Google és Instagram hirdetésein nem tüntette fel a jegyek végső árát befolyásoló összes költséget, valamint a jegyekért fizetendő végső árról csak a vásárlás későbbi fázisában, a jegyek kiválasztását követően tájékoztatta a fogyasztókat. A fogyasztók a		

[19] GVH, VJ/89-90/2016. sz. határozat, 2018. június 11.
[20] GVH, VJ/17/2020 sz. határozat, 2021. április 29.

vásárlási folyamat végén szembesültek azzal, hogy a jegyek kiválasztása és jóváhagyása után a korábban vételárként feltüntetett összegnél magasabb végösszeg szerepelt, mivel a jegyvásárlási folyamat során minden jegy vonatkozásában külön-külön kezelési költség került felszámításra. A versenyfelügyeleti eljárás eredményeként a GVH az eljárás alá vont Kultúrpark Zrt.-t figyelmeztetésben részesítette, bírság kiszabására nem került sor.

A GVH jelen elemzésben bemutatott döntései alapján kirajzolódik egyfajta „konzervatív" jogalkalmazási és szabályozási tendencia:

- A GVH által vizsgált, sötét megoldásoknak minősülő kereskedelmi gyakorlatok jellemzően nem kizárólag az online térben előforduló, a digitalizáció következményeként megjelenő tisztességtelen vagy tilalmazott kereskedelmi gyakorlatok, hanem olyan kereskedelmi gyakorlatok, amelyre vonatkozóan „offline" körülmények között már kiterjedt szabályozói gyakorlat áll fenn. Példának okáért, a leggyakrabban vizsgált, sötét megoldásnak minősülő kereskedelmi gyakorlat az árkommunikáció (rejtett árak, félrevezető árak, csepegtető árazás). Ez a gyakorlat az online térre, az online platformokra nézve nem specifikus.
- A GVH eddigi döntéseiben nem lépett ki ebből a „hagyományos" Fttv. hatálya alá tartozó kereskedelmi gyakorlatnak minősülő sötét megoldásokat szabályozó szerepéből. Ennek egyik magyarázata lehet a GVH jogszabályban meghatározott hatásköre, az Fttv. 10. § (3) bek. értelmében a GVH ugyanis tisztességtelen kereskedelmi gyakorlat tilalmának megsértése miatt és csak akkor járhat el, ha a kereskedelmi gyakorlat a gazdasági verseny érdemi befolyásolására alkalmas. Ez a kettős feltétel magában foglalja azt, hogy a sötét megoldás csak akkor tartozik a GVH hatáskörébe, ha kereskedelmi gyakorlatnak minősül. Ez pedig nem minden esetben egyértelmű, mint például az online platformok vizuális kialakítása esetében.

4.2 Európai Uniós szabályozási gyakorlat

A sötét megoldásokra irányuló európai uniós jogalkalmazás vizsgálata a magyar szabályozás tükrében kiemelten releváns. Ennek oka egyrészt, hogy a szupranacionális jellegű, az EUMSZ 267. és 344. cikkei értelmében az uniós jog értelmezésére monopoljoggal rendelkező EUB döntései a magyar hatóságokra és bíróságokra nézve kötelező erővel bírnak. Továbbá, tekintettel arra, hogy a sötét megoldásokat szabályozó releváns jogterületek a fenti 3. fejezetben bemutatottak szerint jellemzően magas szinten harmonizált jogterületek, az egyes uniós szintű szervezetek egységes jogértelmezése szintén orientálja a magyar hatóságokat is. Így például az adatvédelem területén a GDPR VII. fejezetében meghatározott Együttműködés és egységesség szabályai szerint az EDPB egyes határozatai kötik a tagállami adatvédelmi hatóságokat. Végül, az egyes tagállami szintű jogalkalmazás relevanciája is a jogharmonizációs törekvésekre vezethető vissza, amennyiben az egyes tagállami szabályozási irányvonalak konvergálnak, vagy épp ellenkezőleg, annak ismerete érdekében, hogy melyek a legfőbb eltérések az egyes tagállami jogalkalmazások között.

4.2.1 Európai Uniós szervek

4.2.1.1. Európai Unió Bírósága

Az EUB több előzetes döntéshozatali eljárásban foglalt állást a sötét megoldásokra vonatkoztatható jogértelmezéssel. Az EUB ezen ügyekben hozott döntéseire jellemző, hogy az előzetes

döntéshozatali eljárásban előterjesztett kérdések nem a digitális térben megjelenő sötét megoldásokat tárgyalják, hanem a fogyasztó megtévesztésével kapcsolatban általános és az észszerűen elvárható mértékben tájékozott fogyasztó archetípusának több irányú értelmezését biztosítják. Ezek a döntések ezért közvetetten relevánsak a sötét megoldásokkal kapcsolatban, annyiban, hogy az EUB által megállapított kritériumok analóg módon alkalmazhatók a sötét megoldások megtévesztő jellegének megállapítására. Tekintettel a fenti 1. ábrán bemutatott jellemző fogalomalkotó elemekre, az EUB fogyasztóvédelmi jogszabályok értelmezése során kimunkált gyakorlata a sötét megoldások jogsértő voltának megállapításában is releváns. Így például a DSA 25. cikk (1) bekezdése szerint az online platformot üzemeltető szolgáltatók nem alakíthatnak ki a szolgáltatásukat igénybe vevőket megtévesztő vagy manipulatív online interfészeket. A DSA nem tartalmaz iránymutatást arra nézve, hogy mit és milyen feltételek alapján tekint megtévesztőnek és manipulatívnak. Az EUB fogyasztóvédelmi jogot értelmező döntéseinek platformszabályozás körében nyert relevanciája alátámasztására lényeges megjegyezni, hogy a DSA fogalomrendszerében a „*szolgáltatás igénybe vevője*" alatt a DSA (2) preambulumbekezdése szerint a fogyasztó is értendő, továbbá, a DSA (3) preambulumbekezdése szerint a közvetítő szolgáltatók kellően gondos magatartása biztosítja a „*fogyasztóvédelem magas szintjének elérését*". Önmagában a tény, hogy a DSA a (10) preambulumbekezdése, a 2. cikk (3) bekezdése és a 25. cikk (2) bekezdése szerint nem érinti a fogyasztóvédelemre vonatkozó uniós jogot, nem zárja ki a fogyasztóvédelmi jog keretében megalkotott uniós *acquis* alkalmazhatóságát.

Ügy száma: **C-562/15**	Az előzetes döntéshozatali eljárásban értelmezett jogszabályhely: Az Európai Parlament és a Tanács megtévesztő és összehasonlító reklámról szóló 2006/114/EK irányelve (2006. december 12.) 4. cikk a) - c) pont UCPD 7. cikk (1)-(3) bek.
Az EUB egy francia élelmiszer-kiskereskedelmi hálózat által alkalmazott összehasonlító árazást megjelenítő televíziós reklámkampányt vizsgált, ahol a reklámozó hálózat a saját üzleteit és termékeit kedvezőbb, olcsóbb árszínvonalúnak állította be a versenytársakéhoz képest. A reklám azért volt megtévesztő, mert a reklámozó a saját és a versenytársak termékeit más paraméterek alapján választotta ki (saját alacsonyabb árkategóriába tartozó termékeit hasonlította a versenytárs magasabb árkategóriába tartozó termékeihez, holott a versenytársnál az olcsóbb termék is elérhető volt). Az EUB álláspontja szerint a kereskedelmi reklámra vonatkozóan általánosságban figyelembe kell venni, hogy „*a szokásosan tájékozott, észszerűen figyelmes és körültekintő, átlagos fogyasztó hogyan észleli a szóban forgó reklám tárgyát képező termékeket vagy szolgáltatásokat*"[21]. Ebben a tekintetben vizsgálandó az is, hogy az adott reklám alkalmas-e *„a fogyasztó gazdasági magatartásának befolyásolására azzal, hogy a fogyasztót arra vezeti, hogy abban a téves feltevésben hozzon döntést, hogy az érintett termékeknek a versenytárs*	

[21] EUB, C-562/15 (2017. február 8.), 31. bek.

cégek üzletei helyett a reklámozó cég bármely üzletében való megvásárlásával részesülni fog a reklámban hirdetett árkülönbség előnyében”.

Ugyan az ügyben az EUB televíziós, és nem online kereskedelmi gyakorlatot vizsgált, az átlagfogyasztó befolyásolására való képesség értelmezése megfelelően interpretálható a megtévesztő jellegű online sötét megoldásokra, pl. információ elrejtése, megtévesztő árak, bizonytalan forrásból származó ajánlások.

Ügy száma:	Az előzetes döntéshozatali eljárásban értelmezett jogszabályhely:
C-54/17	UCPD I. melléklet, 29. pont

Az EUB egy, az olasz versenyhatóság által a Wind és a Vodafone mobil távközlési szolgáltatókra kiszabott bírság jogszerűségét vizsgálta. A Wind és a Vodafone olyan SIM kártyákat forgalmaztak, amelyeken előre telepítettek és aktiváltak bizonyos szolgáltatásokat – például az internetes böngészés és az üzenetrögzítő szolgáltatását –, amelyek költségei a felhasználót terhelték, anélkül, hogy a felhasználót előzetesen tájékoztatták volna ezen szolgáltatásokról és azok visszterhes jellegéről. Az EUB az UCPD I. mellékletének 29. pontjában foglalt „nem kívánt értékesítés” fogalmának értelmezése alapján kimondta ezen kereskedelmi gyakorlat jogszerűtlenségét, és megerősítette azt a korábbi esetjogában kimunkált elvet, hogy az UCPD 8. cikke az „*agresszív kereskedelmi gyakorlat fogalmát különösen azzal határozza meg, hogy e gyakorlat ténylegesen vagy valószínűsíthetően jelentősen korlátozza az átlagfogyasztónak a termékkel kapcsolatos választási szabadságát vagy magatartását. Ebből következik, hogy a szolgáltatás iránti kérelemnek a fogyasztó szabad választásában kell megnyilvánulnia. Ez különösen azt feltételezi, hogy a kereskedő által a fogyasztónak nyújtott tájékoztatás egyértelmű és megfelelő legyen*.”[22]

Ezzel az ítélettel az EUB hozzájárult a vállalkozásokat terhelő megfelelő tájékoztatási kötelezettség uniós jogba való beágyazásához, ami szintén egy mind „offline”, mind digitális környezetben értelmezhető jogelv.

Ügy száma:	Az előzetes döntéshozatali eljárásban értelmezett jogszabályhely:
C- 61/19	GDPR 4. cikk (11) és 6. cikk (1) bek. a) pont

A fenti ügyektől eltérően jelen ügyben az EUB sötét megoldásnak minősülő személyes adat-kezelés jogszerűségét vizsgálta. Az alapügyben a román adatvédelmi hatóság jogellenesnek találta az Orange Romania mobil távközlési szolgáltató adatkezelését, mert az a felhasználóktól a papíralapú előfizetői szerződések megkötését megelőzően elkérte személyi igazolványaik másolatát, és ehhez a felhasználó hozzájárulását egy, a szerződésen előre bejelölt jelölőnégyzetben szerezte meg. Amennyiben a felhasználó nem kívánt hozzájárulni a személyi igazolvány másolatának megadásához, nem tudta a jelölőnégyzetből az ’X’ jelölést eltávolítani,

[22] EUB, C-54/17 (2018. szeptember 13.), 45. bek.

hanem egy erre a célra biztosított „megtagadó nyilatkozat” nevű formanyomtatványt kellett kitöltenie.

Az EUB a román adatvédelmi hatóság érveléseit követve kimondta, hogy sérül a hozzájárulás önkéntességének GDPR 4. cikk 11. pontja szerint támasztott követelménye, amennyiben az adatkezelő a hozzájárulás megadására szolgáló jelölőnégyzetet előre bejelöli; továbbá, a konkrét ügy vonatkozásában azt, hogy önkéntesség és a felhasználó szabad döntése hiányában nem jogszerű a hozzájárulás akkor, ha az adatkezelő által teremtett körülmények megtévesztik a felhasználót, mert elhitetik vele, hogy hozzájárulás nélkül nem tud igénybe venni egy szolgáltatást.

Az EUB ezen megállapítása analógia alapján alkalmazható minden olyan sötét megoldásra, amely akár leplezetten, a felhasználó nem tudatos befolyásolása alapján, akár kifejezetten szembetűnően megtéveszti a felhasználót, és ezáltal „kicsalja” tőle a hozzájárulást.

4.2.1.2 Európai Adatvédelmi Testület és Európai Adatvédelmi Biztos

Az EDPB az EU tagállamainak adatvédelmi hatóságait összefogó testületként több véleményben és irányelvben fogalmaz meg iránymutatásokat mind a GDPR hatálya alá tartozó adatkezelők (azaz, ebben a kontextusban a sötét megoldásokat alkalmazó vállalkozások), mind a tagállami adatvédelmi felügyeleti hatóságok számára.

Az EDPB 03/2022 iránymutatásában a sötét megoldásokat adatvédelmi szempontból, és kizárólag a közösségi médiaplatformokon megvalósított „*megtévesztő tervezési mintákként*” vizsgálja (EDPB, 2022). AZ EDPB egyedi nézőpontból, a közösség média felhasználói fiók életciklusai alapján három „fázis”, a felhasználói fiók létrehozása, használata és törlése szerint tekint át összesen hat kategóriába tartozó 16 azonosított sötét megoldást az alábbiak szerint:

Túlterhelés („overloading”)	**Átugrás** („skipping”)	**Megkavarás** („stirring”)	**Akadályozás** („obstructing”)	**Zavarás** („fickle”)	**Sötétben hagyás** („left in the dark”)
Folytonos noszogatás, pl. adatszolgáltatásra ösztönző folyamatos felugró ablakok, üzenetek küldése (“Continuous prompting”)	**Megtévesztő ismeretség,** amely adatok megadására sarkall közvetlen ismerősöknek. (“Deceptive Snugness”)	**Érzelmi befolyásolás,** pl. megszégyenítéssel – megfeleltethető a „Confirm Shaming néven azonosított sötét megoldással (“Emotional steering”)	**Zsákutca**, önmagába mutató linkek elhelyezése, ahol a felhasználó pl. négy kattintással visszaér oda, ahonnan indult (“Dead end”)	**Hiányzó hierarchia** (“Lacking hierarchy”)	**Ellentmondásos információ** (“Conflicting information”)
Adatvédelmi útvesztő, a fontos funkciók	**Figyelemelterelés** oda nem illő szöveggel vagy	**Vizuális stílus vagy technika használata**,	**Várakoztatás,** azaz amikor adott választás	**Az adatvédelmi információ vártalan helyre**	**Homályos megfogalmazás**

vagy jogok gyakorlását szükségtelenül megnehezíti egy számtalan rétegből álló, összetett adatvédelmi szabályzat (“privacy maze”)	ábrázolással (“Look over there”)	amely a felhasználókat a kevésbé szigorú és ezáltal invazívabb lehetőségek felé tereli. (“Hidden in plain sight”)	rögzítése indokolatlanul sok ideig tart, például sütibeállítások elfogadása egyből lehetséges, elutasítás esetén a továbblépés 10-20 másodpercbe telik. (“Longer than necessary”)	**helyezése**, ahol a felhasználó kontextus hiányában nem számít rá, pl. impresszum “jogi” füle alatt (“De-contextualising”)	(“Ambiguous wording or information”)
Túl sok lehetőség (“Too Many Options”)			**Félrevezetés** (“Misleading action”)	**Követhetetlen felület** (“Inconsistent Interface”)	
				Nyelvi akadályok, például a tájékoztatás nem érhető el a felhasználó anyanyelvén (“Language Discontinuity”)	

Az azonosított sötét megoldásokat az EDPB tovább kategorizálja a felhasználók viselkedésére gyakorolt hatásuk szerint. A *tartalom-alapú* sötét megoldások a tényleges tartalomban jelentkeznek, megfogalmazásban, információtartalomban, míg a *felület-alapú* sötét megoldások felhasználói felület kialakítására, vizuális megjelenésre, a felhasználói felületen való navigálásra, és az ott végezhető interakciók módjára vonatkoznak. Ez a felosztás sok hasonlóságot mutat Mathur és mtsai (2021) fenti 1.2.2 pontban említett, a fogyasztó rendelkezésére álló választási lehetőségeket módosító vagy a fogyasztóhoz érkező információáramlás manipuláló sötét megoldások felosztására.

Hangsúlyozandó, hogy az EDPB szűk mozgásteret biztosít a közösségi média platformok üzemeltetőinek, mivel sötét megoldásként jogsértőnek tekint mindazon gyakorlatot, amelyek bármilyen tekintetben megnehezítik a személyes adatok kezeléséhez szükséges hozzájárulás megadását, pl. ha túl sok kattintás szükséges az adatvédelmi tájékoztató megtekintéséhez, vagy ha

a közösségi média üzemeltető adatvédelmi tájékoztatója és az adatfeldolgozási megállapodások „*egymásra mutató linkeket*” tartalmaznak (Horváth, 2023).

Talán elszalasztott lehetőség azonban, hogy az EDPB csak a közösségi médiaplatformok felületeinek kialakítására ad ajánlásokat, az adatvédelmi szempontból megtévesztő sötét megoldások használata ugyanis nem korlátozódik bizonyos ágazatokra vagy iparágakra. Például, az online marketingcégek, a keresőmotorok, az e-kereskedelmi weboldalak vagy a felhőalapú tárhelyszolgáltatók mind használhatnak sötét megoldásokat a felhasználói viselkedés befolyásolására, személyes adatok gyűjtésére és a felhasználói interakciók nyomon követésére, gyakran a felhasználók egyértelmű hozzájárulása és tájékoztatása nélkül. Az adatvezérelt technológiákat (mesterséges intelligenciát, gépi tanulást vagy nagy adatelemző platformokat) fejlesztő és működtető vállalatok szintén gyűjthetnek, kezelhetnek és elemezhetnek személyes adatokat megfelelő átláthatóság, tisztességesség vagy felhasználói ellenőrzés nélkül, ami felvetheti az elfogultság, a megkülönböztetés az előre nem látható következmények kockázatát. Feltételezhető, hogy az EU-ban külön szabályozási eszközök hiányában az adatkezelők minden iparágban végső soron erre a 03/2022 iránymutatásra támaszkodnak majd, amikor a virtuális megjelenésük és jelenlétük adatvédelmi megfelelőségét értékelik. Ennek eredményeképpen az iránymutatás célközönsége valójában szélesebb lehet a tényleges címzetti körnél (Domokos, 2023).

Az EDPS, mint az EU-s szervek adatvédelmi felügyeleti hatósága megközelítése a sötét megoldásokra nézve az átláthatóság szerepét hangsúlyozza, ami a beépített és alapértelmezett adatvédelem szerves részét képezi, és célja a szándékos megtévesztés kizárása. A transzparencia ellentételezi azt, hogy ezek a gyakorlatok aláássák mind az adat-, mind a fogyasztóvédelmet, mivel arra ösztönzik (vagy kényszerítik) a felhasználókat, hogy elfogadják a túlzott mértékű személyes adatok gyűjtését, vagy hogy elhamarkodottan hozzanak vásárlási döntéseket (EDPS, 2019).

4.2.2 Tagállami szabályozási irányok

A magyar szabályozói gyakorlathoz hasonlóan az EU és EGT tagállamokban is megfigyelhető, ahogy a sötét megoldások szabályozására vonatkozó intézményi kompetenciák követik az uniós szabályozás fent bemutatott tagozódását. Ennek megfelelően az egyes uniós tagállamokban egyfelől a tagállami adatvédelmi felügyeleti hatóságok, másfelől a versenyhatóságok és fogyasztóvédelmi hatóságok párhuzamosan fennálló hatáskörökkel rendelkeznek a sötét megoldások szabályozására, attól függően, hogy azok adatkezelésnek, vagy tisztességtelen és ezért tiltott kereskedelmi gyakorlatnak minősülnek.

Emellett ugyanakkor tagállamonként eltérés mutatkozik abban, hogy melyik hatóság kezeli kiemelt prioritásként a sötét megoldások vizsgálatát és az azzal kapcsolatos társadalmi figyelemfelhívást. Míg Franciaországban (CNIL, 2020), Olaszországban (Garante, 2023) és Spanyolországban (AEPD, 2022) az adatvédelmi felügyeleti hatóságok, addig a Holland Királyságban a tagállami versenyhatóság (ACM, 2023), Ausztriában (Arbeiterkammer Österreich, 2023) és Norvégiában (NCC, 2018) pedig a tagállami fogyasztóvédelmi hatóságok adtak ki részletes iránymutatást és tájékoztató anyagot a sötét megoldásokra vonatkozóan. Egy további példa Németország, ahol már megjelenik a sötét megoldások kifejezett szektorspecifikus tilalma is, a német Fizetési Szolgáltatók Szövetségi Felügyelete ugyanis önálló iránymutatásban tiltotta meg a felhasználók döntését vizuális elemekkel befolyásoló sötét megoldások (az egyes gombok lényegesen kisebb kontraszttal való

kialakítása, a többihez képest szürkék vagy átlátszóak) alkalmazását befektetési szolgáltatásokat nyújtó vállalkozások számára kereskedési alkalmazásokban vagy kereskedési portálokon (BaFin, 2022).

Változó intenzitással, de a legtöbb uniós tagállamban létezik már precedens a sötét megoldásokat tárgyaló hatósági eljárásokra. Jelenleg az eljárások döntő többsége a cookie bannerekkel kapcsolatban megjelenő sötét megoldásokat vizsgálja, úgy, mint szuggesztív, félrevezető vizuális megjelenés, előre bejelölt jelölőnégyzetek hozzájárulás esetén, apró betűvel, vagy nehezen észrevehető helyen elrejtett tájékoztatás. Az EGT-tagállamok hatáskörrel rendelkező hatóságai által folyamatban lévő és 2023 márciusáig lezárt sötét megoldásokat tárgyaló ügyekről készült statisztikát a 3. melléklet tartalmazza.

5. Javaslatok a sötét megoldások szabályozására

A sötét megoldások jelentette problémakör lehetséges megoldásainak feltérképezése során célszerű a jogi és a jogon kívüli eszközök egymással párhuzamos, egymást kiegészítő alkalmazása. A jogi eszközök, a jogszabályokon keresztül történő szabályozás fontos, mert törvényes keret teremt az etikus üzleti gyakorlatok előmozdításához és a felhasználók adatvédelmi, fogyasztóvédelmi jogainak erősítéséhez. A jogi eszközök lehetővé teszik továbbá a hatóságoknak a sötét megoldásokkal visszaélő vállalkozások előre meghatározott szempontok szerinti ellenőrzését, ami megfékezi az ilyen gyakorlatok elterjedését és visszatartó erejű lehet a jövőbeni esetekben.

Ugyanakkor a jogon kívüli eszközök is fontos szerepet játszanak a megoldások kezelésében. Például az oktatás és a tudatosság növelése a fogyasztók között lehetővé teszi, hogy jobban felismerjék és elkerüljék ezeket a manipulatív tervezési technikákat. A felhasználók tájékoztatása és oktatása arra ösztönzi az embereket, hogy kritikusan vizsgálják meg a vállalatok és termékek interakcióit, és szükség esetén megkeressék az alternatívákat. Emellett a technológiai megoldások, például böngészőkben vagy alkalmazásokban elérhető sötét megoldás felismerő eszközök is hozzájárulhatnak a felhasználók védelméhez és az átlátható online környezet kialakításához.

5.1 Jogszabályi keretrendszer

- **Jogterületek és hatáskörök elhatárolása**: A fenti 3. fejezetben bemutatottak szerint 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. Mind a szabályozás kiszámíthatósága, mind az egyes jogszabályok betartásáért felelős tagállami hatóságok feladat- és hatásköreinek egyértelmű elkülönülése érdekében szükséges jogszabályi szinten szabályozni a következőket: i) amennyiben egy sötét megoldás kizárólag egy jogterület alá tartozik, ezen sötét megoldások ellenőrzése az adott jogterület felügyeletére hatáskörrel bíró hatóságok kizárólagos hatáskörébe utalása (pl. az árkommunikációra vonatkozó, Fttv-be ütköző sötét megoldások esetén a GVH kizárólagos hatásköre), ii) figyelemmel arra, hogy az i) opció sok esetben nem alkalmazható, mert ugyanaz a sötét megoldás a konkrét esettől függően egyszerre sért fogyasztóvédelmi és adatvédelmi rendelkezéseket, megfelelő együttműködési csatornák alakítandók ki a hatáskörrel bíró hatóságok között. Továbbá, az alábbi, tanúsítási programokra és magatartási kódexekre irányuló javaslatokkal

kapcsolatban az egyes hatóságok kompetenciáira vonatkozó hatásköri szabályok között meg kell határozni az ezek létrehozásáért, felügyeletéért felelős, és megsértése esetén eljáró hatóságokat, független tanúsító szervezeteket, vagy a tanúsító szervezetté váláshoz teljesíteni szükséges kritériumokat.

- **Egységes megnevezések**: Javasolt a „dark patterns" angol kifejezés egységes magyar fordításának meghatározása a szabályozásban érintett hatóságok (NAIH, GVH, NMHH, mint digitális szolgáltatási koordinátor) közötti egyeztetés során, tekintettel az eltérő fordításokra: a NAIH 2022-es éves beszámolójában a „sötét minták" míg a GVH az online közzétett, „Repjegyet venne? Vigyázzon, így befolyásolhatják döntését!" c. tájékoztatójában a „sötét mintázat" kifejezést használja. Javasolt továbbá az eddig főként angol nyelven azonosított és tárgyalt egyes sötét megoldások magyar nyelvre ültetése. Ez az átültetés több, mint az egyszerű szóról-szóra fordítás, tekintettel arra, hogy az angol kifejezések (pl. „sneaking") szó szerinti átfordítása nem ugyanazt a jelentéstartalmat hordozza a magyar nyelvben (így pl. a szó szerinti fordítás „settenkedés", „lopakodás", holott a „csempészés" megfelelőbben leírja a sötét megoldás lényegét). Ez az egységes magyar taxonómia lehet pl. egy hatósági, vagy több hatóság (pl. NAIH, GVH, NMHH) együttműködésével megalkotott ajánlás, iránymutatás, amely megalkotásában a hivatásos fordítókon kívül pl. nyelvészek is részt vesznek, akár előzetes, felhasználók meginterjúvolásán alapuló kvantitatív kutatások eredményeit is felhasználva.
- **Független tanúsítási programok**: Hasonlóan az adatvédelem területén a GDPR 42-43. cikke szerint megszerezhető tanúsításokhoz, vagy a gyártói felelősség körében szükséges CE-jelöléshez, megfontolandó egyfajta „etikus design" tanúsítás létrehozása, amely bizonyos előre meghatározott feltételek mentén, határozott időre, vagy a feltételek teljesülése esetén határozatlan időre megszerezhető. Ez a tanúsítás kettős célt szolgálhat, egyrészt jelzi a szabályozó hatóságoknak a weboldal- vagy platformüzemeltető megfelelését, másfelől erősítheti a felhasználókban keltett bizalmat. A tanúsítások szabályozásakor szükséges annak jogszabályi szintű meghatározása, hogy mely szervezetek és milyen kritériumok teljesülése esetén válhatnak tanúsító szervezetté. Ilyen kritériumok lehetnek például függetlenség, tagok képzettségére (pl. webdesigner, akadémikus, meghatározott évnyi tapasztalattal rendelkező jogász, szabályozó szervnél dolgozó szakértő) és összetételére vonatkozó szabályok – a kritériumokat arra tekintettel kell meghatározni, hogy a tanúsító szervezetnek rendelkeznie kell megfelelő szakmai kompetenciákkal annak értékelésére, hogy egy weboldal vagy applikáció az etikus, átlátható megjelenés feltételeit teljesíti-e, valamint ennek periodikus felülvizsgálatára.
- **Etikus tervezési magatartási kódex**: A magatartási kódexek kidolgozása és az azoknak való önkéntes megfelelés az önszabályozás egyik elterjedt eszköze (például reklámpiaci szereplőknél, felhőszolgáltatások nyújtása körében). A sötét megoldásokra irányuló magatartási kódexének célja, hogy útmutatást nyújtson az érdekelteknek a sötét megoldások alkalmazásakor. A magatartási kódexeknek olyan eszköznek kell lenniük a kódexgazdák - például a kereskedelmi, szakmai, képviseleti vagy nonprofit szervezetek - számára, amely támogatja az ágazatukban jellemzően alkalmazott sötét megoldásokra vonatkozó jogszabályoknak való megfelelést. A magatartási kódexek lehetnek i) uniós vagy

tagállami szinten horizontálisan alkalmazható kódexek, ii) nemzetközi szervezetek által kiadott kódexek (pl. OECD) vagy iii) iparágspecifikus kódexek (pl. kizárólag webáruházak üzemeltetőire, vagy a fent említett német példa szerint fizetési szolgáltatókra alkalmazandók). A magatartási kódexek kidolgozásának szabályait javasolt úgy meghatározni, hogy a sötét megoldások szabályozására hatáskörrel rendelkező hatóságok (Magyarországon jelenleg a NAIH és a GVH, illetve a DSA alatti digitális szolgáltatási koordinátornak kijelölt hatóság, pl, az NMHH) részt vehessenek a kódexek megalkotásában. A piaci érdekeltek csatlakozhatnak egy említett hatóságok valamelyike által jóváhagyott magatartási kódexhez, hogy fokozzák és bizonyítsák jogszabályoknak való megfelelésüket.

5.2 Jogon kívüli eszközök

- **Tudatosság-növelő és ismeretterjesztő kampányok**: Ahogy a fenti 2. pontban említett, Bongard-Blanchy, és mtsai (2021) által végzett kutatás is rámutatott, a sötét megoldások és a sötét megoldások által kiváltani kívánt felhasználói viselkedés felismerésében és tudatos értékelésében szerepet játszik a felhasználók előzetes tudása és előismeretei a sötét megoldásokra vonatkozóan. Tekintettel arra, hogy a sötét megoldások az online térben jelennek meg, a sötét megoldások felhasználói szintű ismerete mellett szerepet játszik az internet felhasználói szintű ismerete, digitális írástudás és a digitális készségek. Az alacsony adattudatosság egy digitális írástudatlansággal együtt járó (nemzetközileg is jelentős) probléma, amely ahhoz vezet, hogy a lakosság nem érti saját személyes adatainak értékét a digitális működésben, ezért hajlamos több személyes adatot megadni a feltétlenül szükségesnél. Ezért javasolt a hatóságok által országos szintű, regionális vagy intézményi pl. oktatási intézményekben információs kampányokat szervezni, lehetőség szerint minél fiatalabb generációk megcélzásával. Ennek oka, hogy a kiskorú gyerekek a sötét megoldások célkeresztjében a felnőtt felhasználóknál sérülékenyebb csoportnak tekintendők.

- **Felhasználóbarát UX tervezési irányelvek**: Az UX (felhasználói élmény) tervezési irányelvek kidolgozása azért hasznos, mert konkrét gyakorlatokkal („best practice”), és javaslatokkal orientálja a weboldal- és platformtervezőket az etikusabb online környezet kialakításában. Az irányelvekben alapelvi szinten fogalmazható meg a „fairness by design”, azaz az átlátható és felhasználóbarát kialakítás követelménye. Ezek az irányelvek kiegészíthetik, tartalommal tölthetik meg a jogalkotásban helyt kapó általános definíciókat. A tervezési irányelvek kidolgozása során szabályozó hatóság, iparági érdekeltek, akadémiai szereplők, és közvetve, pl. közvélemény-kutatás alapján a felhasználók álláspontja is becsatornázható, így segítve a teljes körű megfelelés feltételeinek észszerű gyakorlati ráfordítások mellett megvalósítható, és egyben felhasználóbarát, és jogszerűséget biztosító meghatározását.

- **Sötét megoldásokat felismerő és jelző algoritmusok fejlesztése vagy fejlesztés ösztönzése**: A sötét megoldások a digitális fejlődés hozadékai, így célszerű digitális eszközöket bevetni a sötét megoldások térnyerése ellen. Javasolt az olyan technikai megoldások, algoritmusok és applikációk saját fejlesztése, vagy harmadik felek (vállalkozások, egyéni vállalkozók, PhD- vagy egyéb kutatási programban részt vevők)

fejlesztésének támogatása, amelyek akár önmagukban, akár böngészőkhöz hozzáadható bővítményként automatikusan azonosítják, a felhasználó böngészése során valós időben jelzik és jelölik (például kis figyelemfelkeltő zászlóval, háromszöggel) a megjelenő sötét megoldásokat. Az ilyen technikai megoldások képesek azonnali közbelépésre, így a felhasználó számára okozott hátrány bekövetkezésének megakadályozására, és egyúttal segítik a felhasználók edukálását is.

- **Felhasználói visszajelzési csatornák**: A felhasználók bíztatása szabályozó hatóságok, iparági szereplők, nonprofit-szervezetek, fogyasztóvédelmi egyesületek által szervezett kampányok, ismeretterjesztő anyagok segítségével, hogy a sötét megoldások jelzése céljából képernyőfelvételeket, képernyővideókat osszanak meg (EDPS, 2021). Ez az elsősorban információs célt szolgáló visszajelzési módszer lehetőséget ad a hatóságoknak egy kiterjedt adatbázis létrehozására, és megkönnyíti a folyamatosan új formában megjelenő, vagy teljesen újfajta sötét megoldások proaktív felderítését.

Irodalomjegyzék

ACM (2023). “Leidraad bescherming online consument”, elérhető online: https://www.acm.nl/nl/publicaties/voorlichting-aan-bedrijven/acm-leidraad/leidraad-bescherming-online-consument.

AEPD (2022). “Dark patterns: Manipulation in Internet services”, elérhető online: https://www.aepd.es/en/prensa-y-comunicacion/blog/dark-patterns-manipulation-in-internet-services#:~:text=The%20term%20dark%20patterns%20refers,protection%20of%20their%20personal%20data.

BaFin (2022). “Dark Patterns in Trading Apps unzulässig”, elérhető online: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2022/meldung_2022_11_21_Dark_Patterns_in_TradingApps_Experten.html.

Bongard-Blanchy, K. és mtsai (2021). “I am Definitely Manipulated, Even When I am Aware of It. It’s ridiculous! – Dark Patterns from the End-User Perspective” Designing Interactive Systems Conference 2021, https://doi.org/10.1145/3461778.3462086.

Bösch, C. és mtsai. (2016). “Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns”, Proceedings on Privacy Enhancing Technologies, 2016 évfolyam, 4. szám, 237-254 oldal, https://doi.org/10.1515/popets-2016-0038.

Bowman, D. (2009). “Goodbye, Google 1. rész.” elérhető online: https://stopdesign.com/journal/2009/03/20/goodbye-google.html, utolsó hozzáférés ideje: 2023. május 30.

Calo, R. (2014). “Digital Market Manipulation”, 82 George Washington Law Review 995 (2014), University of Washington School of Law Research Paper No. 2013-27, http://dx.doi.org/10.2139/ssrn.2309703.

Conti, G. és Sobiesk, E. (2010). “Malicious interface design: Exploiting the User”, 271-280, https://doi.org/10.1145/1772690.1772719.

CNIL (2020). “Shaping Choices in the Digital World”, elérhető online: https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf

Domokos, M. (2023) “EU: Practical aspects of the EDPB's guidelines on deceptive design patterns”. elérhető online: https://www.dataguidance.com/opinion/eu-practical-aspects-edpbs-guidelines-deceptive

Domokos, M. és Horváth A., (2021). “Dark patterns – napvilágra kerülő sötét megoldások” elérhető online: https://www.jogiforum.hu/blog-ip-it-vedjegy-domain-internet-jogi-blog-11/2021/09/02/dark-patterns-napvilagra-kerulo-sotet-megoldasok/.

EDPB (2019). „4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről”, elérhető online: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf

EDPB (2023). “03/2022 iránymutatás a közösségi médiaplatformok felületeinek megtévesztő tervezési mintáiról: hogyan ismerjük fel és kerüljük el őket?”, elérhető online: 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.

EDPS (2019). “We need to talk about terms and conditions”, elérhető online: https://edps.europa.eu/press-publications/press-news/blog/we-need-talk-about-terms-and-conditions_en

EDPS (2021). “Democratic Societies In the Digital Age 2: Dark Patterns and Online Manipulation” 3 részes podcast-sorozat, 2. rész, elérhető online: https://edps.europa.eu/podcasts/edps-air/democratic-societies-digital-age-2-dark-patterns-and-online-manipulation_en

Európai Bizottság (2020). A Bizottság Közleménye az Európai Parlamentnek és a Tanácsnak “Új fogyasztóügyi stratégia”, “A fogyasztói reziliencia erősítése a fenntartható helyreállítás érdekében”, elérhető online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52020DC0696

Európai Bizottság (2021a). „A Bizottság Közleménye “Iránymutatás a belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól szóló 2005/29/EK európai parlamenti és tanácsi irányelv értelmezéséhez és alkalmazásához”, elérhető online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52021XC1229(05)

Európai Bizottság (2021b). „A Bizottság Közleménye a „fogyasztók jogairól szóló 2011/83/EU európai parlamenti és tanácsi irányelv értelmezésére és alkalmazására vonatkozó iránymutatásról”, elérhető online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52021XC1229(04)

Európai Bizottság (2022). “Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation”, elérhető online: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1.

Európai Bizottság (2023). “Fogyasztóvédelem: 399 átvilágított webáruházból 148 alkalmazott manipulatív online gyakorlatot”, elérhető online: https://ec.europa.eu/commission/presscorner/detail/hu/ip_23_418.

BEUC. (2022). “Dark Patterns and the EU consumer law acquis - Recommendations for better enforcement and reform” elérhető online: https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf

Flayelle, M. és mtsai (2023), “A taxonomy of technology design features that promote potentially addictive online behaviours”, Nature Reviews Psychology, 2023. évfolyam, 2. szám, 136–150. oldal, https://doi.org/10.1038/s44159-023-00153-4.

Garante (2023). “Modelli di progettazione ingannevoli (Dark Pattern)”, elérhető online:

Gray, C. M. és mtsai. (2018). “The dark (patterns) side of UX design.” In Proceedings of the 2018 CHI conference on human factors in computing systems, 1-14. oldal, https://doi.org/10.1145/3173574.3174108.

Gazdasági Versenyhivatal. (2022). “Repjegyet venne? Vigyázzon, így befolyásolhatják döntését!”, elérhető online: https://gvh.hu/pfile/file?path=/sajtoszoba/sajtokozlemenyek/sajtokozlemenyek/2022-es-sajtokozlemenyek/sk_2022_10_28_legitarsasagok-sweep&inline=true.

Gazdasági Versenyhivatal (2023). “Terjed a jogsértő, rejtett befolyásolás az online kereskedelemben”, elérhető online: https://www.gvh.hu/pfile/file?path=/sajtoszoba/sajtokozlemenyek/sajtokozlemenyek/2023-as-sajtokozlemenyek/sk_2023_01_31_cpc-sotet-mintazatok&inline=true.

Horváth, A. (2023). “Szabályozói célkeresztben a sötét megoldások” Datapatron online magazin, 1. évfolyam 2. szám, elérhető online: https://datapatron.hu/wp-content/uploads/2023/03/datapatron-02.pdf.

Jarovsky, L. (2022). “Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness” https://dx.doi.org/10.2139/ssrn.4048582

Kahneman, D (2011). “Gyors és lassú gondolkodás”., MacMillan Publishers kiadó, 1. kiadás.

Kitkowska, A., Högberg, J., & Wästlund, E. (2022). “Barriers to a well-functioning digital market: Exploring dark patterns and how to overcome them” In 55th Hawaii International Conference on System Sciences.

Leiser, M. (2022). “Illuminating Manipulative Design: from ‘Dark Patterns’ to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive” http://dx.doi.org/10.2139/ssrn.4418586.

Mathur, A. és mtsai. (2019). “Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites” Proceedings of the ACM on Human-Computer Interaction, 3. évfolyam (CSCW) 81. cikk, https://doi.org/10.1145/3359183.

Mathur, A., Mayer, J., Kshirsagar, M. (2021). “What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods” In CHI Conference on Human Factors in Computing Systems (CHI ’21), https://doi.org/10.1145/3411764.3445610.

Narayanan, A. és mtsai. (2020). “Dark Patterns: Past, Present, and Future - The evolution of tricky user interfaces”, ACM online folyóirat, 18. évfolyam, 2. szám, 67-92. oldal, https://doi.org/10.1145/3400899.3400901.

NCC (2018). “Deceived by design”, elérhető online: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

OECD (2021). “Roundtable on Dark Commercial Patterns Online: Summary of discussion”, elérhető online: https://one.oecd.org/document/DSTI/CP/CPS(2020)23/FINAL/en/pdf.

OECD (2022). “Dark commercial patterns”, *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en.

Rachadel, J. (2022) “Data protection and fairness by design”, in European Journal of Public Health, 32. évfolyam, 3. szám kiegészítése, https://doi.org/10.1093/eurpub/ckac129.083.

Sibony, O. (2019). “Döntéshozatali csapdák. Hogyan visznek tévútra a torzítások (és mit tehetünk ellenük)? szerk.: Illényi Balázs, HVG Könyvek kiadó.

Szokolszky, Á., Kádár, E (1999) “James J. Gibson ökológiai pszichológiája”. Pszichológia, 19. évfolyam, 2. szám, 245-285. o.

Tversky, A., Kahneman, D (1974). “Judgment under uncertainty: Heuristics and biases,” Science, 145. évfolyam, 4157. szám, 1124–1131. o.

Yeung, K. (2016). ‘Hypernudge’: Big Data as a mode of regulation by design. Information, Communication & Society. https://ssrn.com/abstract=2807574.

Waldman, A.E. (2020). “Cognitive biases, dark patterns, and the ‘privacy paradox”. 31 Current Issues in Psychology 2020, https://ssrn.com/abstract=3456155.

1. melléklet: Rövidítések jegyzéke

ACM	Holland Fogyasztóvédelmi és Piacfelügyeleti Hatóság (Autoriteit Consument & Markt)
AEPD	Spanyol adatvédelmi hatóság (Agencia Española de Protección de Datos)
AVMSD	Az Európai Parlament és a Tanács (EU) 2018/1808 irányelve (2018. november 14.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról szóló 2010/13/EU irányelvnek (Audiovizuális médiaszolgáltatásokról szóló irányelv) a változó piaci körülményekre tekintettel való módosításáról
BaFin	Német Fizetési Szolgáltatók Szövetségi Felügyelete (Bundesanstalt für Finanzdienstleistungsaufsicht)
BEUC	Európai Fogyasztóvédelmi Szervezet
CNIL	Francia adatvédelmi hatóság (Commission nationale de l'informatique et des libertés)
CPC	Fogyasztóvédelmi Hatóságok Együttműködési Hálózata (Consumer Protection Cooperation Network
CRD	Az Európai Parlament és a Tanács 2011/83/EU irányelve (2011. október 25.) a fogyasztók jogairól, a 93/13/EGK tanácsi irányelv és az 1999/44/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 85/577/EGK tanácsi irányelv és a 97/7/EK európai parlamenti és tanácsi irányelv hatályon kívül helyezéséről
Data Act	Javaslat 2022/0047 (COD), az Európai Parlament és a Tanács rendelete a méltányos adathozzáférésre és adatfelhasználásra vonatkozó harmonizált szabályokról (Adatmegosztási jogszabály)
DETOUR Act	Deceptive Experiences To Online Users Reduction Act S.3330, 2021, US, Az online felhasználókat megtévesztő tapasztalatok visszaszorításáról szóló törvény, Egyesült Államok
DSA	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)

DMA	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)
EDM	elektronikus direktmarketing (jellemzően az elektronikus úton küldött hírlevél)
EDPB	Európai Adatvédelmi Testület
EDPS	Európai Adatvédelmi Biztos
Eker Irányelv	Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (Elektronikus kereskedelemről szóló irányelv)
Ekertv.	2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
ePrivacy Irányelv	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)
EGT	Európai Gazdasági Térség
EU	Európai Unió
EUB	Európai Unió Bírósága
EUMSZ	Európai Unió Működéséről Szóló Szerződés egységes szerkezetbe foglalt változata
Fgytv.	1997. évi CLV. törvény a fogyasztóvédelemről
FTC	Szövetségi Kereskedelmi Bizottság (Federal Trade Commission), Amerikai Egyesült Államok
Fttv.	2008. évi XLVII. törvény a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról
Garante	Olasz adatvédelmi hatóság (Garante per la protezione dei dati personali)
GDPR	Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Grt.	2008. évi XLVIII. törvény a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól
GVH	Gazdasági Versenyhivatal
ICPEN	Fogyasztóvédelmi Felügyeleti Hatóságok Nemzetközi Hálózata (International Consumer Protection and Enforcement Network)
OECD	Gazdasági Együttműködési és Fejlesztési Szervezet
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság
NMHH	Nemzeti Média- Hírközlési Hatóság
NCC	Norvég Fogyasztóvédelmi Tanács (Forbrukerrådet, Norwegian Consumer Council)
Mttv.	2010. évi CLXXXV. törvény a médiaszolgáltatásokról és a tömegkommunikációról
Ptk.	A Polgári Törvénykönyvről szóló 2013. évi V. törvény
P2B Rendelet	Az Európai Parlament és a Tanács (EU) 2019/1150 Rendelete (2019. június 20.) Az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról
Tptv.	1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról
UCPD	A belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól, valamint a 84/450/EGK tanácsi irányelv, a 97/7/EK, a 98/27/EK és a 2002/65/EK európai parlamenti és tanácsi irányelvek, valamint a 2006/2004/EK európai parlamenti és tanácsi rendelet módosításáról szóló 2005/29/EK irányelv (tisztességtelen kereskedelmi gyakorlatokról szóló irányelv)
UCTD	A Tanács 93/13/EGK irányelve (1993. április 5.) a fogyasztókkal kötött szerződésekben alkalmazott tisztességtelen feltételekről

2. melléklet: Sötét megoldások kategorizációs rendszerei, taxonómiák

Jelen 2. melléklet tartalmazza az elemzés 1.2.1. pontjában felsorolt kategorizációs rendszerek részletes bemutatását. A táblázatok Leiser (2022) "Illuminating Manipulative Design: from 'Dark Patterns' to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive" c. összefoglaló és korábbi taxonómiákat feldolgozó cikkének magyar fordításai.

1. táblázat
Conti és Sobiesk sötét megoldások taxonómiájának összefoglalása

Kategória	Megcélzott felhasználói viselkedés	A kategorizáció alapja
Kényszerítés („coercion")	A felhasználó fenyegetése vagy kényszerítése, hogy engedelmeskedjen, és végrehajtson egy műveletet, pl. kötelezően kitöltendő mezők /megadandó adatok, vagy félelemkeltő üzenetekkel	Az alkalmazott módszerek jellemzői
Zavarás („confusion")	A felhasználónak olyan kérdések feltétele, vagy olyan információkat adása, amelyeket nem ért, nem tud követni, pl. dupla tagadást tartalmazó kérdések („*Kérjük, ne adja meg az e-mail címét, ha nem kíván üzeneteket kapni.*")	A felhasználókra gyakorolt várható hatás
Elterelés („distraction")	A felhasználó figyelmének elterelése az aktuális feladatról az érzékelési folyamatok, különösen a preattentív feldolgozás kihasználásával.	A felhasználókra gyakorolt várható hatás
Hibák kihasználása („exploiting errors")	A felhasználói hibák kihasználása a felhasználói felület tervezőjének céljai elősegítése érdekében, például reklám mutatása segítség helyett, ha a felhasználó rossz URL-t ad meg.	Az alkalmazott módszerek jellemzői
többletcselekvés („forced work")	A felhasználó által elvégzendő felhasználói műveletek („munka") szándékos növelése, vagy az időráfordítás által (szándékos várakoztatás), vagy a megteendő lépések számának indokolatlan növelésével (pl. fióktörlés, applikáció eltávolításának megnehezítése)	Az alkalmazott módszerek jellemzői
Megszakítás („interruption")	A felhasználó feladatfolyamatának megszakítása (pl. felugró reklámablakkal)	Az alkalmazott módszerek jellemzői
A navigáció manipulálása („manipulating navigation")	Olyan információs architektúra és navigációs mechanizmus, amely a felhasználót a tervező által meghatározott feladatok teljesítése felé tereli, pl. sehova nem mutató link („dead-end trails"), vagy önmagába visszatérő választások	Az alkalmazott módszerek jellemzői

	(„infinite trails”), adatvédelmi útvesztő (például, leiratkozás ellehetetlenítése, „privacy maze”)	
Homályosítás („obfuscation”)	A kívánt információk és felületelemek (menük, ablakok) elrejtése.	Az alkalmazott módszerek jellemzői
Funkcionalitás korlátozása („restricting functionality”)	A felhasználói feladat elvégzését megkönnyítő vezérlőelemek korlátozása vagy elhagyása.	Az alkalmazott módszerek jellemzői
Sokkolás („shock”)	Sokkoló tartalom megjelenítése a felhasználónak	A felhasználókra gyakorolt várható hatás
Trükk („trick”)	A felhasználó félrevezetése vagy egyéb megtévesztési kísérlet, például további szoftverek telepítése a felhasználó tudta vagy beleegyezése nélkül, vagy hamis reklámozás.	Az alkalmazott módszerek jellemzői

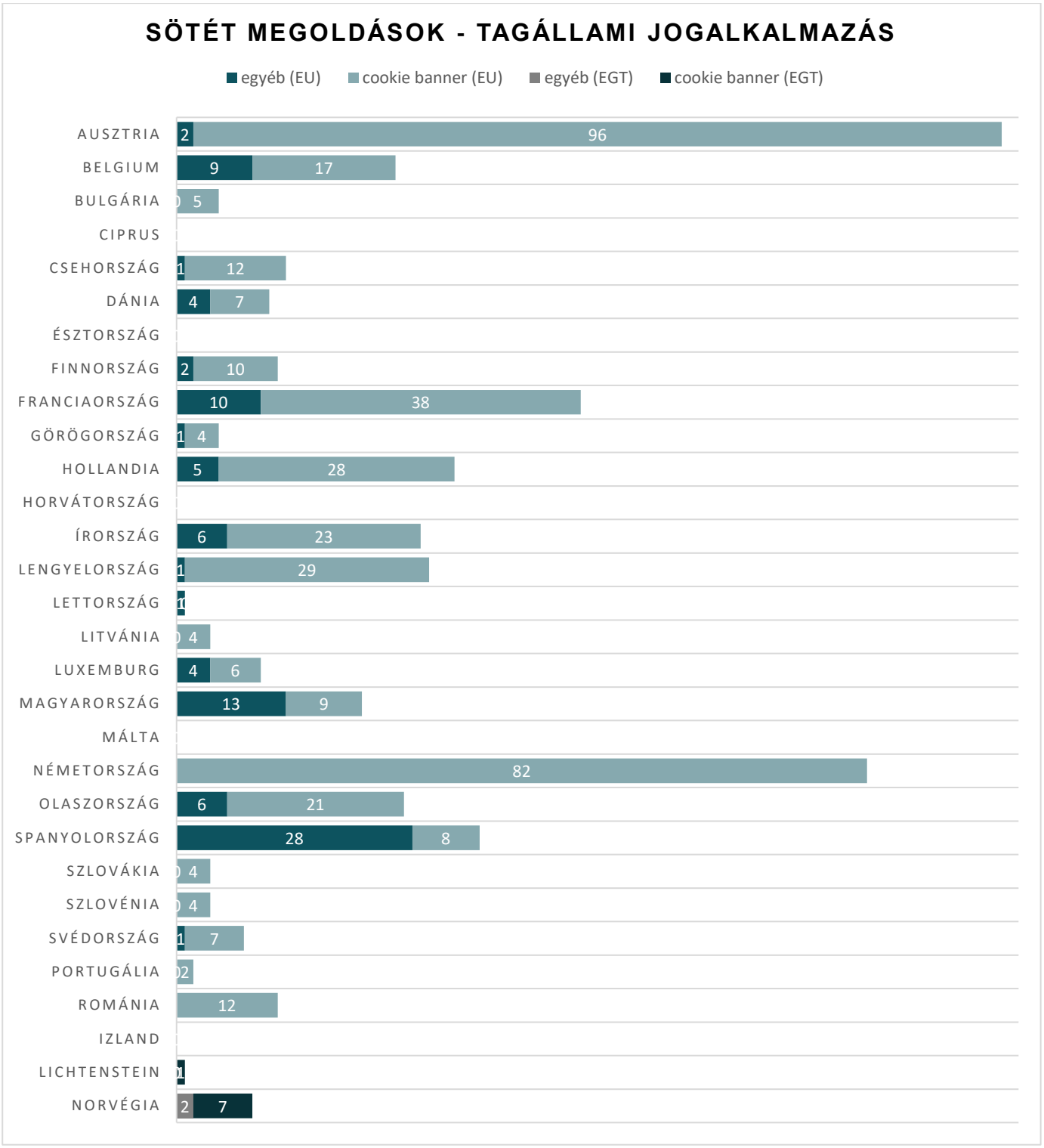
2. táblázat Gray és mtsai. sötét megoldások taxonómia összefoglalás		
Kategória	**Leírás**	**Kategorizáció alapja, példák**
Zaklatás („Nagging”)	Az elvárt működés irányának megváltozása, amely egy vagy több interakción keresztül fennmaradhat.	A rendszeres interakció során ismétlődő zavarás, amely megzavarja vagy eltéríti a felhasználó figyelmét, mint például a felugró ablakok.
Akadályozás („Obstruction”)	Egy folyamat megnehezítése a kelleténél jobban, azzal a szándékkal, hogy bizonyos cselekvés(ek)től eltántorítson.	“Csótánymotel” (“Roach Motel,’), árösszehasonlítás megakadályozása.
Csempészés („Sneaking”)	A felhasználó számára fontos információk elhallgatása, elrejtése, vagy késleltetett megjelenítése	„Kényszerű folytonosság”, („Forced Continuity”), „Rejtett költségek” („Hidden Costs”), „Kosárba csempészés” („Sneak into Basket”) és “Csalás és átverés” (“Bait and Switch)
Felületi zavarás („Interface Interference”)	A felhasználói felület olyan manipulálása, amely bizonyos műveleteket előnyben részesít másokkal szemben, ezáltal összezavarja a felhasználót, vagy korlátozza fontos műveleti lehetőségek felfedezhetőségét.	Három altípust foglal magában: 1) „Rejtett információ”, 2) „Előválasztás”, azaz a felhasználó előre kiválasztott vagy elfedett választási lehetőségei) és 3) „Esztétikai manipuláció”, azaz a felhasználói felület esztétikai jellemzőinek manipulálása a hierarchia vagy a tartalom típusának félreértése vagy a sürgősség irreális érzése érdekében.
Többletcselekvés („Forced Action”)	Bizonyos funkciók eléréséhez (vagy további eléréséhez) a felhasználónak meghatározott műveletet kell végrehajtania, ami vagy ténylegesn szükséges lépésnek tűnik (de nem az,), vagy egy olyan lehetőségnek, ami úgy tűnik, mintha hasznos lenne a felhasználó számára.	Ún. „Privacy Zuckering”, azaz ösztönzés egyre több személyes adat megadására, „Gamification” (a szolgáltatás bizonyos funkcióit csak bizonyos cselekvések megismétlésével lehet "kiérdemelni", például játékokban szörnyek ismételt megölése a felhasználó karakterének szintlépéséhez szükséges tapasztalati pontok megszerzéséhez, vagy ún. „lootboxok”, vásárlására késztetés, azzal az ígérettel, hogy az a következő szint eléréséhez szükséges eszközöket tartalmaz), vagy „Társas piramis” („Social Pyramid”), azaz olyan gyakorlatok, amelyek megkövetelik a felhasználóktól, hogy más felhasználókat toborozzanak a szolgáltatás használatára – más néven „Friends Spam”.

3. táblázat Mathur és mtsai. sötét megoldások taxonómia összefoglalás		
Kategória megnevezése	**Típus**	**A felhasználóra gyakorolt hatás módja**
Csempészés (“sneaking”)	**Kosárba csempészés** (“Sneak into Basket”)	Megtévesztő, elrejti az információt
	Rejtett árak (“Hidden Costs”)	Megtévesztő, elrejti az információt
	Rejtett feliratkozás (“Hidden Subscription”)	Megtévesztő, elrejti az információt
Sürgetés (“urgency”)	**Visszaszámláló** (“Countdown Timer”)	Leplezett, Megtévesztő
	Időbeni korlátozást / korlátozott idejű elérhetőséget jelző üzenetek („Limited-time Message”)	Leplezett, elrejti az információt
Félrevezetés (“misdirection”)	**Megszégyenítés** (“Confirm Shaming”)	Aszimmetrikus
	Vizuális zavarás („Visual Interference”)	Aszimmetrikus, leplezett, megtévesztő
	Becsapós kérdések („Trick Questions”)	Aszimmetrikus, leplezett
	Vásárlásra késztetés („Pressured Selling”)	Aszimmetrikus, leplezett
Társadalmi megerősítés (“social proof”)	**A felületen más felhasználók aktivitását jelző üzenetek** („Activity Message”)	Leplezett, megtévesztő
	Ajánlások („Testimonials”)	Megtévesztő
Korlátozottság (“scarcity”)	**Alacsony készletet jelző üzenetek** („Low-stock Message”)	Leplezett, megtévesztő, elrejti az információt
	Magas keresletet jelző üzenetek („High-demand Message”)	Leplezett, megtévesztő
Akadályozás (“obstruction”)	**Nehéz lemondás** („Hard to Cancel”)	Elrejti az információt, korlátozó
Többletcselekvés (“forced action”)	**Kényszerített feliratkozás** („Forced Enrolment”)	Aszimmetrikus, korlátozó

4. táblázat Leiser és Yang négy szintű hierarchikus taxonómiája és kapcsolódó sötét megoldás típusok				
Kategória			**Típus**	**Magyarázat**
Információs aszimmetria	Aktív félrevezetés tevés formájában	Félrevezető információ	**Bizonytalan forrásból érkező ajánlások** (“Testimonials of Uncertain Origin”)	A felhasználók félrevezetése hamis, zavaró, megtévesztő vagy túlzó információkkal.
			Korlátozottság (“Scarcity”)	A felhasználók félrevezetése hamis, zavaró, megtévesztő vagy túlzó információkkal.
			Barátok behívása (“Friend Spam”)	A felhasználók félrevezetése megtévesztő információkkal.
			Hamis visszaszámláló (“Fake Countdown Timers”)	A felhasználók félrevezetése csalárd/hamis információkkal.
			Időbeni korlátozást / korlátozott idejű elérhetőséget jelző üzenetek („Limited-timeMessages”)	A felhasználók félrevezetése megtévesztő vagy túlzó információkkal.
		Félrevezető megjelenés	**Becsapós kérdések** (“Trick Questions”)	A felhasználók félrevezetése a megfogalmazás által.
			Elirányítás – vizuális megzavarás (“Misdirection - Visual Interference”)	A felhasználók félrevezetése a felhasználói felület vizuális megjelenésével.
	Passzív félrevezetés mulasztás formájában	Információ elrejtése	**Árösszehasonlítás megakadályozása** (“Price Comparison Prevention”)	A felhasználók félrevezetése a világos és érthető árinformációk visszatartásával.
		Késedelmes információ-adás	**Rejtett árak** (“Hidden Costs”)	Az árra vonatkozó információk késleltetett megjelenítése.
A szabad választás	Nemkívánatos zavarás	Nyomás-gyakorlás	**Vásárlásra késztetés (ismétlődő felugró ablakok vagy megszégyenítés** (“Pressured Selling (Repeated Popup Dialogs	A felhasználókra történő nyomásgyakorlás olyan ismételt megkeresésekkel vagy megfogalmazásokkal, amelyek a felhasználókban bűntudatot vagy szégyenérzetet keltenek.

			or Confirm Shaming”)	
		Kényszerített elfogadás	**Kosárba csempészés** („Sneak into Basket”)	A felhasználók kényszerítése, hogy elfogadják a kéretlen termékeket azáltal, hogy a termékeket közvetlenül a kosarakba helyezik.
			Könnyű regisztráció **„**Privacy Zuckering (Easy to Register)”	A felhasználók nem kívánt előfizetés elfogadására kényszerítése olyan trükkökkel, amelyek az előfizetések felé terelik őket.
			Kényszerű folytonosság – rejtett feliratkozás („Forced Continuity - Hidden Subscription”)	A felhasználók kényszerítése az előfizetés folytatására a tagságuk rejtett megújításával.
			“csalás és átverés” (“Bait and Switch”)	A felhasználók rábírása egy adott megállapodás elfogadására azáltal, hogy manipulatív módon eltérítik őket eredeti céljuktól.
			Álcázott hirdetés („Disguised Advertisement”)	A felhasználók kényszerítése egy hirdetés megtekintésére azáltal, hogy a felhasználói felület manipulatív módon olyan helyre navigálja a felhasználókat, amire nem számítottak, függetlenül attól, hogy érdekli-e őket a reklám.
	Nemkívánatos korlátozás	Bizonyos felhasználók korlátozása	**Kényszerűség - beiratkozás a hozzáféréshez, Fizetés az átugráshoz, elfogadás a hozzáféréshez** („Forced Action (Enrol to Access, Pay to Skip, and Accept to Access”)	A nem fizető vagy leiratkozott felhasználók kizárása az olyan lehetőségekből, mint a tartalomhoz való hozzáférés vagy a hirdetések átugrása.
		Egyes tevékenysé-gek korlátozása	**“Csótánymotel” - nehéz lemondás** („Roach Motel” - Hard to Cancel)	Bizonyos műveletek, például a leiratkozás bonyolultabbá tétele a szükségesnél.

3. melléklet: EGT-tagállamok szabályozó hatósági gyakorlat, statisztika



A jelen diagram szemlélteti a sötét megoldásoknak tekinthető gyakorlatokkal kapcsolatos EU és EGT tagállami jogalkalmazást 2020-2023 március közötti időszakban.

A diagram az egyes tagállamok adatvédelmi fogyasztóvédelmi és versenyhatóságai által indított eljárásokat összesítve szemlélteti. Ennek oka a tagállami szabályozási kompetenciák eltérő megoszlása, ahogy a fenti 4.2.2 pontban bemutatottak szerint az egyes tagállamokban eltérés mutatkozik a tekintetben, hogy jellemzően mely hatóságok járnak el a sötét megoldásoknak minősülő gyakorlatok esetében.

A diagram az EGT-tagállamok adatvédelmi és versenyhatóságainak nyilvánosságra hozott határozatai alapján azonosított, és az alábbi adatbázisokban szereplő, már lezárt, vagy még folyamatban lévő hatósági eljárásokat tartalmazza:

- EDPB tagállami döntések tára, elérhető online: https://edpb.europa.eu/news/news_en?news_type=2&field_edpb_member_states_target_id=All
- GDPR hatósági döntések tára („Enforcement Tracker”), elérhető online: https://www.enforcementtracker.com/
- Sötét megoldásokkal összefüggő döntések tára, elérhető online: https://www.deceptive.design/cases
- „Cookie banner” felületeken alkalmazott sötét megoldásokkal összefüggésben tagállami adatvédelmi hatóságoknál benyújtott panasz alapján folyamatban lévő adatvédelmi felügyeleti eljárások, elérhető online: https://noyb.eu/en/project/cookie-banners