GDPR-tudatosság, a digitális platformok használati intenzitása és az AI-attitűdök generációs mintázatai

1. Dr. Csiszár Csilla Margit, csilla.csiszar@uni-miskolc.hu
2. Rácz Benjámin, benjamin.racz@student.uni-miskolc.hu

Absztrakt: A tanulmány azt vizsgálja, hogy az életkor és a GDPR-hoz kapcsolódó alapismeretek miként függnek össze a mobilplatformok használati intenzitásával, a platformspecifikus kockázatészleléssel és az AI-val kapcsolatos attitűdökkel Magyarországon. Az empirikus elemzés nem reprezentatív online kérdőíves felmérésre épül. Az eredmények szerint a GDPR alapvető rendelkezéseinek ismerete alacsony, ugyanakkor a tájékozottabb válaszadók körében gyakoribb a védekező adatvédelmi gyakorlat, különösen a regisztráció során megadott pontatlan adatok tekintetében. A TikTok egyszerre szerepel kiemelten a kockázati besorolásokban és a használati preferenciákban, ami a hasznosság és a kontrollélmény közötti feszültségre utal. Az AI-val kapcsolatos aggodalom az életkor előrehaladtával erősödik, miközben a fiatalabb korcsoportok a gyakori használat mellett is ritkábban korlátozzák saját platformtevékenységüket. A következtetések szerint indokolt a platformokra szabott adatvédelmi oktatás erősítése, valamint olyan fogyasztóvédelmi tájékoztatás, amely közérthetően bemutatja a beállítások gyakorlati következményeit.

Abstract: This study examines how age and basic GDPR-related knowledge are associated with the intensity of mobile platform use, platform-specific risk perceptions, and attitudes toward AI in Hungary. The empirical analysis is based on a non-representative online questionnaire survey. The results indicate that knowledge of core GDPR provisions is generally low; however, respondents with higher levels of awareness are more likely to engage in defensive privacy practices, particularly by providing inaccurate information during account registration. TikTok is simultaneously prominent in risk classifications and in usage preferences, pointing to a tension between perceived usefulness and the sense of control over personal data. Concern about AI increases with age, while younger cohorts, despite frequent use, are less likely to restrict their own platform-related activities. The findings support the need to strengthen platform-tailored privacy education and to expand consumer-protection communication that explains, in accessible terms, the practical consequences of privacy and security settings.

Kulcsszavak: adatvédelem, GDPR, digitális bizalom, platformhasználat, generációs különbségek
JEL-kód: D18, D83, K24, L86, O33

Bevezetés

A digitális platformok gyors terjedése és az algoritmikus tartalomajánlás mindennapossá válása alapvetően átformálta a felhasználói döntési helyzeteket. A személyre szabott működés és a kényelmi funkciók növelik a platformok észlelt használati értékét, miközben az adatgyűjtés, a profilozás és az automatizált következtetések folyamata a felhasználók jelentős részének továbbra is csak részben átlátható. A GDPR uniós szinten egységes keretet biztosít a személyes adatok védelméhez (Európai Parlament és a Tanács, 2016), ugyanakkor továbbra is nyitott kérdés, hogy a szabályozás milyen mértékben épül be a mindennapi felhasználói rutinokba, és mennyiben alakítja a tényleges online viselkedést. A deklarált adatvédelmi aggályok és a valós platformhasználat közötti eltérés a szakirodalomban régóta ismert jelenség, amelyet többek között a választási korlátok, a hálózati hatások, valamint a beállítási lehetőségek átláthatósága is magyarázhat (Barth & Jong, 2017; Solove, 2021). Az információs aszimmetria elméletére építve több szerző rámutat, hogy a fogyasztók rendszerint kevesebb ismerettel rendelkeznek az áruk és szolgáltatások kockázatairól, mint a szolgáltatók, ami strukturálisan hátrányos helyzetet eredményezhet (Kiss, 2020). Az AI szerepe ebben a folyamatban különös jelentőséget kap, mert az ajánlórendszerek nem csupán a tartalomhoz való hozzáférést alakítják, hanem a figyelem eloszlását is irányítják, ezáltal a magánélethez kötődő kockázatok észlelésének és értelmezésének keretei is módosulhatnak (Mühlhoff, 2023). A tanulmány ezért arra fókuszál, hogy a generációs különbségek, a GDPR-hoz kapcsolódó ismeretek és az AI-val összefüggő

attitűdök milyen eltérő kockázatkezelési mintázatokat rajzolnak ki a magyarországi felhasználók körében.

1. Irodalmi áttekintés

Napjainkban a digitális eszközök sok ember számára elengedhetetlenné váltak, hiszen a digitális technológia már a társadalmunk nagy részét elérte. Az okoseszközök fejlődése nemcsak az egyéni felhasználói szokásainkat változtatta meg, hanem mélyebb társadalmi változásokat is előidézett. A digitalizáció miatt új kommunikációs csatornák jöttek létre, felgyorsult és egyszerűbb lett az információk elérése, valamint átalakultak a munkavégzési és tanulási szokások is. Manapság már nem tudnánk elképzelni az életünket digitális eszközök nélkül, hiszen már majdnem mindenki használ valamilyen okoseszközt, ami számos területen könnyíti meg az életünket, legyen szó munkáról, tanulásról, kapcsolattartásról vagy szórakozásról. A technológia fejlődésének sebessége folyamatos alkalmazkodást kíván a felhasználóktól, és ez nemcsak a fiatal generációra van hatással, hanem az idősebb korosztály mindennapjait is jelentősen átalakítja. A digitális eszközök folyamatos jelenléte nemcsak a mindennapi élet kényelmét növeli, hanem új készségek elsajátítását is megköveteli a felhasználóktól. Az információs társadalomban való boldogulás szinte elképzelhetetlen megfelelő digitális kompetenciák nélkül, ezért a technológiai eszközök használatának tudatossága kulcsfontosságúvá vált. A digitális eszközök hatása a társadalom működésére már olyan mértékű, hogy a gazdasági, oktatási és szociális folyamatok is jelentősen átalakultak. A digitális technológia azonban ma már kihat mentális egészség védelmére, valamint a személyes adatok védelmére is egyaránt. Továbbá a technológia fejlődésével az adatvédelem szerepe is egyre fontosabbá válik. Sok felhasználó nem is gondol bele, hogy a mindennapi alkalmazáshasználat közben mennyi személyes információt ad át különböző szolgáltatóknak vagy cégeknek, ezzel kockáztatva adataik biztonságát.

A platformalapú digitális környezetben az adatvédelem egyszerre szabályozási és magatartási kérdés. A magánélet paradoxonára épülő kutatások azt hangsúlyozzák, hogy az adatvédelmi aggályok nem feltétlenül vezetnek a platformhasználat visszafogásához (Barth & Jong, 2017). A kritikai megközelítések szerint az eltérés gyakran a választási lehetőségek korlátozottságából fakad, és a felhasználók a hasznosság, a társas kapcsolatok és a kilépési költségek mérlegelése mellett maradnak aktívak (Solove, 2021; Ooijen et al., 2024). A szabályozási környezet mellett a bizalom szerkezete is meghatározó, mivel uniós mérési eredmények alapján az online cégek adatkezelésébe vetett bizalom jellemzően alacsonyabb, mint a klasszikus intézményi szereplők esetében, ami önmagában is kedvez a közösségi média kockázati kategóriaként való kiemelődésének (Csiszár, 2019).

Az AI-val összefüggő adatvédelmi kérdések ezzel párhuzamosan felerősödtek, mert az automatizált következtetések és a személyre szabás új típusú kockázatokat hoz létre, amelyek egy része kollektív jellegű (Mühlhoff, 2023). Generációs dimenzióban több kutatás is rámutat, hogy a fiatalabb felhasználók magasabb expozíció mellett is alacsonyabb óvatosságot tanúsíthatnak, illetve túlértékelhetik adatvédelmi ismereteiket (Ma & Chen, 2023; Maier et al., 2023). A platformok közötti különbségek ugyancsak lényegesek, mert az adatvédelmi stratégiák erősen kontextusfüggők, és a felületi kialakítás a döntéseket is tereli (Chung et al., 2021). Jelen kutatás e megállapításokra építve vizsgálja a GDPR-hoz kapcsolódó alapismeretek és a platformhasználat kapcsolatát, különös tekintettel az AI-val összefonódó tartalomkörnyezetre.

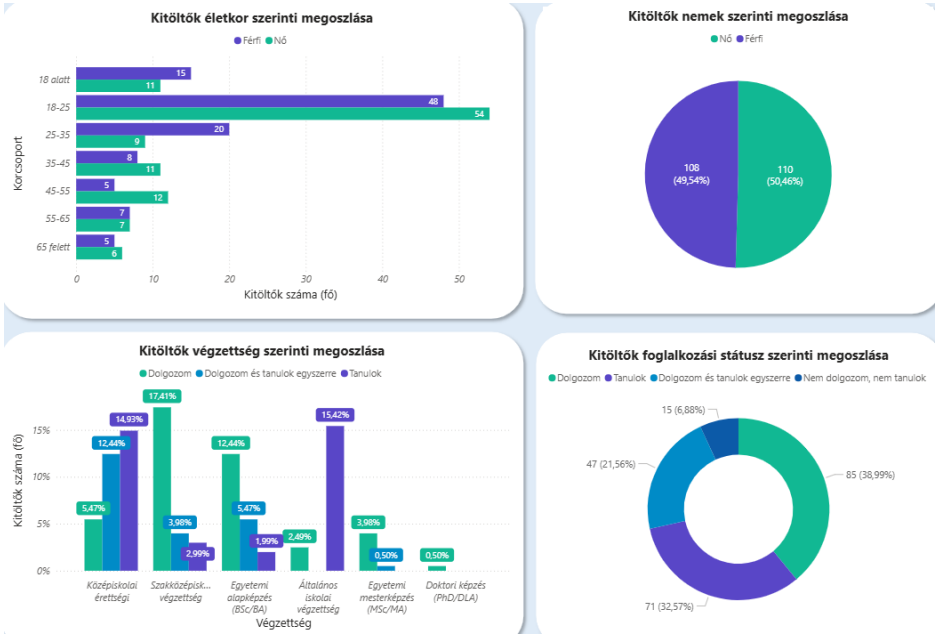
2. Módszertan

A tanulmány vegyes módszertani megközelítést alkalmaz az életkor, a GDPR-tudatosság és a mesterséges intelligencia toleranciája közötti kapcsolatok vizsgálatára a digitális viselkedésben. A kutatás tervezése ötvözi a kvantitatív felmérési adatokat a nyitott kérdésekre adott válaszokból származó kvalitatív eredményekkel, ami lehetővé teszi a demográfiai csoportok felhasználói mintáinak alapos vizsgálatát. Kettős módszertani stratégiánk integrálja az elsődleges felmérési adatokat (N=218) az Eurostat-jelentések és a GDPR végrehajtási minták kiegészítő vizsgálatával. A felmérés dokumentálja az eszközhasználatot, a titkosságra vonatkozó nézőpontokat és a mesterséges intelligenciával való interakciókat, demográfiai tényezők, például életkor, nem és végzettség szerint kategorizálva. A Power BI támogatja a keresztmetszeti trendek dinamikus megjelenítését. Az elsődleges adatokat egy strukturált kérdőív segítségével gyűjtöttük, amelyet 2025. június 25. és október 10. között a Microsoft Forms segítségével terjesztettünk. A felmérés logikai elágazásokat alkalmazott a relevancia biztosítása érdekében, és a válaszadóknak átlagosan 26 kérdés (az összesen 119 kérdésből) tettünk fel, az eszközhasználati szokásaik és adatvédelmi magatartásuk függvényében. A felmérési eszköz négy tematikus részből állt: 1) szociodemográfiai adatok (életkor, nem, végzettség, foglalkoztatási helyzet), 2) a különböző közösségi média platformokon töltött idő, 3) az információbiztonsággal kapcsolatos gyakorlatok és a GDPR-rendeletek ismerete, valamint 4) a mesterséges intelligencia által létrehozott tartalmakkal kapcsolatos tapasztalatok. Különböző típusú kérdéseket, például Likert-skálát, többválasztós és nyitott kérdéseket használtunk a kvantitatív mutatók és a kvalitatív betekintés összegyűjtéséhez. A mintavételi stratégia a közösségi médián keresztül történő terjesztéssel különböző demográfiai csoportokat célozott meg, ami 218 teljes válaszhoz vezetett. A minta kiegyensúlyozott nemi megoszlást mutatott (49% férfi, 51% nő) és többségében fiatalabb résztvevőket (58,7% 25 év alatti), ami összhangban áll Magyarország digitálisan aktív demográfiai adataival. A foglalkoztatási státuszt és az oktatási szintet is rögzítették, hogy a későbbi elemzésekben kontrollálni lehessen a társadalmigazdasági változókat. A kvantitatív adatokat a Power BI segítségével elemeztük, kihasználva annak kapcsolódását a Microsoft ökoszisztémájához a zökkenőmentes adatátalakítás és vizualizálás érdekében. A Power Query szűrők alkalmazása támogatta az adatok tisztítását a hiányos vagy inkonzisztens bejegyzések kiszűrésével, míg a DAX (Data Analysis Expressions) lehetővé tette a változók közötti kapcsolatok kifinomult modellezését. Interaktív dinamikus irányítópultokat hoztunk létre a képernyőn töltött idő trendjeinek, a GDPR-tudatosság mutatóinak és az AI-expozíciós adatoknak a megjelenítésére, amelyek szeletelőket tartalmaznak, amelyek támogatják a keresztelemzést életkor, nem és végzettség szerint. A mélyebb statisztikai elemzéshez Python szkripteket ágyaztunk be a Power BI-ba, hogy korrelációs mátrixokat és regressziós ábrákat generáljunk. A legfontosabb mutatók között szerepelt az átlagos képernyőidő platformonként, a GDPR-megértési pontszámok (6 pontos Likert-skálán) és az AI-val kapcsolatos aggodalmak indexei korcsoportok szerint rétegezve. Az elsődleges eredmények szélesebb keretbe helyezése érdekében a kutatás kiegészítő Eurostat-adatokat (2025) tartalmazott a mesterséges intelligencia elterjedéséről és az általános adatvédelmi rendelet betartásának mintáiról az Európai Unió országaiban.

3. Eredmények

A szakasz a kutatás főbb empirikus megállapításait ismerteti a demográfiai jellemzők, a telefonhasználati mintázatok, valamint az adatvédelmi aggályok és a GDPR-ismertség összefüggéseinek bemutatásával. Az eredmények a korcsoportok, a szabályozási ismeretek szintje és a környezeti sajátosságok mentén kirajzolódó digitális viselkedésbeli eltérésekre adnak rálátást. A kutatási minta 218 válaszadóból állt (1. ábra), és közel kiegyensúlyozott nemi

megoszlást mutatott, a résztvevők 49 százaléka férfi, 51 százaléka nő volt. Az életkori szerkezetben a fiatalabb korcsoportok domináltak, a válaszadók 46,8 százaléka 18-25 év közötti, további 11,9 százaléka pedig 18 év alatti volt. A 25 év alattiak együttesen a minta 58,7 százalékát tették ki, ami azt jelzi, hogy a vizsgálatban meghatározó súllyal szerepeltek a diákok és a fiatalabb résztvevők. A középkorú és idősebb korcsoportok részvétele mérsékeltebb volt. A 25-35 évesek aránya 13,3 százalék, a 35-45 éveseké 8,7 százalék, a 45-55 éveseké 7,8 százalék, az 55-65 éveseké 6,4 százalék, a 65 év felettieké pedig 5 százalék volt. A foglalkoztatási és végzettségi szerkezet a minta fiatalos profilját tükrözi: a válaszadók 38,99%-a dolgozik, 32,57%-a tanul, további 21,56% pedig egyszerre dolgozik és tanul, míg 6,88% egyik kategóriába sem tartozik. A végzettségi megoszlásban a tanulói csoportoknál dominálnak az alacsonyabb végzettségi szintek, miközben a dolgozóknál erősebb a szakközépiskolai háttér és számottevő a felsőfokú végzettség jelenléte is.



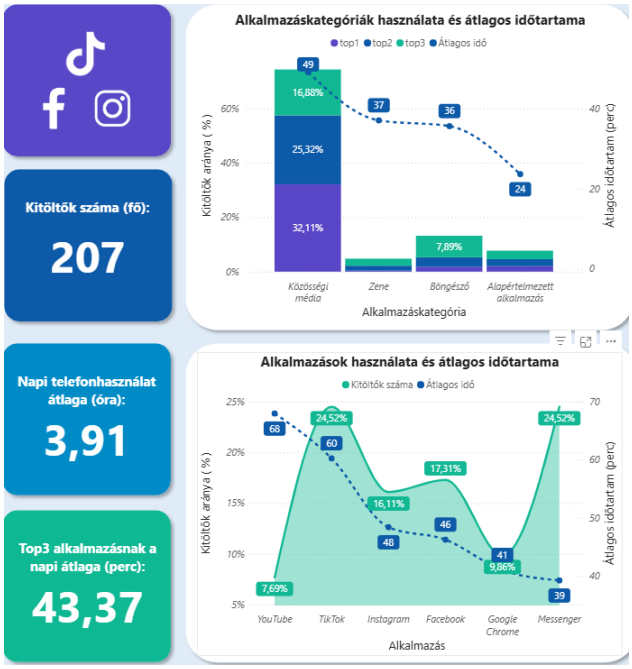
1. ábra: Demográfiai adatok

Forrás: Saját szerkesztés a primer kutatás alapján (N=218)

Mindez azt jelzi, hogy az eredmények elsősorban a fiatalabb, oktatáshoz kötődő felhasználók digitális magatartásának értelmezésére alkalmasak, az idősebb és nem oktatásban érintett csoportok alacsonyabb aránya pedig korlátozza az általánosíthatóságot.

Telefonhasználati szokások

A telefonhasználatra vonatkozó blokk 207 érvényes választ tartalmaz (2. ábra). A napi telefonhasználat átlaga 3,91 óra volt. A három leggyakrabban használt alkalmazásra jutó átlagos napi idő 43,37 perc, ami a teljes képernyőidő közel 19 százalékát adja. Az alkalmazáskategóriák között egyértelműen a közösségi média szerepelt az első helyen. Első helyre 32,11 százalék sorolta, második helyre 25,23 százalék, harmadik helyre 16,88 százalék.



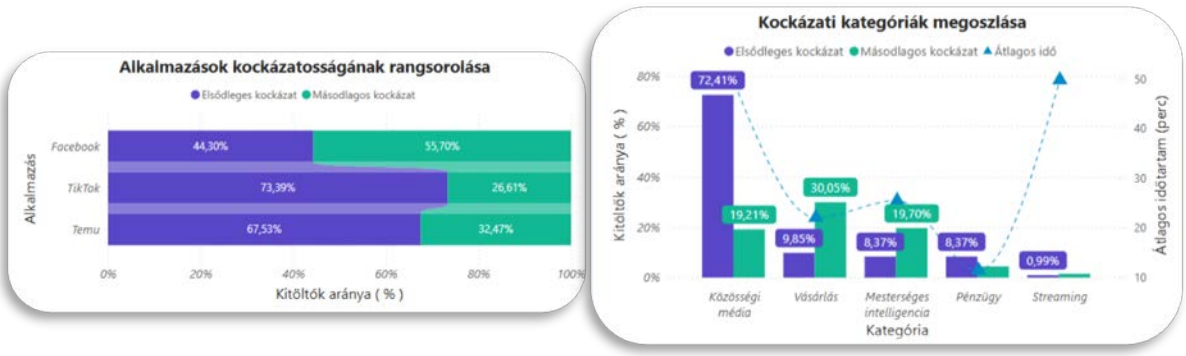
2. ábra: Telefonhasználati szokások

Forrás: Saját szerkesztés a primer kutatás alapján (N=207)

A közösségi média kategóriában mért átlagos napi idő 49 perc volt, amely érdemben meghaladta a zene és a böngésző kategóriát. Az egyes alkalmazások szintjén a TikTok és a Messenger fordult elő a leggyakrabban, közel 25 százalékos megjelenéssel. A YouTube hozzávetőleg 8 százalékot tett ki, míg a Facebook és az Instagram megközelítőleg 17 százalékot. Az időtartamok alapján a YouTube vezetett körülbelül 68 perces átlaggal, ezt követte a TikTok 60 perccel, a Facebook 44 perccel, az Instagram 41 perccel és a Messenger 39 perccel.

Adatvédelmi aggályok és az alkalmazás használata

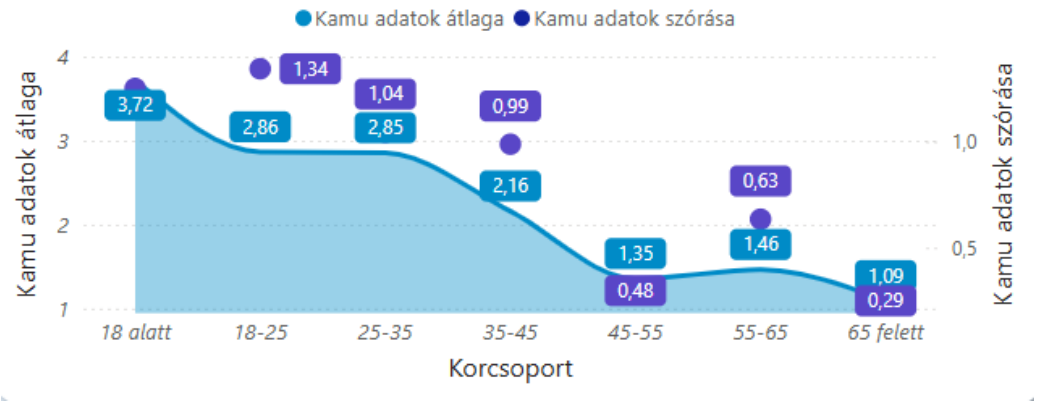
Az adatvédelmi kérdésekre adott válaszok alapján a közösségi média emelkedett ki a legfontosabb kockázati kategóriaként. A 207 érvényes válasz közül 72,41 százalék jelölte meg elsődleges adatvédelmi aggályként a közösségi médiát. Ettől jelentősen elmaradtak a vásárlással kapcsolatos alkalmazások, amelyek 30,05 százalékban másodlagos kockázatként jelentek meg, míg a pénzügyi alkalmazások a válaszok alapján minimális fenyegetésként rajzolódtak ki. A minta mintázata illeszkedik azokhoz a megállapításokhoz, amelyek szerint a felismert adatvédelmi kockázatok ellenére a platformokhoz való kötődés és a tényleges használat magas maradhat (Barth & Jong, 2017). Az alkalmazásspecifikus kockázati percepciók ugyanakkor markáns eltéréseket mutattak (3. ábra). A TikTok kapta a legmagasabb elsődleges kockázati besorolást 73,39 százalékkal, ezt követte a Temu 67,53 százalékkal, majd a Facebook 44,3 százalékkal. Ezzel párhuzamosan a használati mutatók más logikát követtek. Az elterjedtségben a TikTok és a Messenger osztozott az első helyen, mindkettő 24,52 százalékos aránnyal, miközben a napi használati időben a YouTube dominált 68 perccel, majd a TikTok 60 perccel és az Instagram 48 perccel. A kockázati megítélés és a használat dominanciája közötti ellentmondás összhangban értelmezhető azzal az érvvel, amely szerint a felhasználók a kockázatok felismerése mellett is fenntartják a platformhasználatot, és a kompromisszumot a lemondás logikája mentén rendezik (Ooijen et al., 2024).



3. ábra: Adatvédelmi aggályok
Forrás: Saját szerkesztés a primer kutatás alapján (N=207)

Az adatgyűjtéssel kapcsolatos attitűdök kifejezetten korosztály szerint rétegződtek. A résztvevők 36 százaléka jelezte, hogy zavarja, ha az alkalmazások adatokat gyűjtenek róla, ez a nyugtalanság azonban az idősebb korosztályokban erősebb volt. Az 55-65 évesek 1,8-szor nagyobb zavart mutattak, mint a 18-25 évesek. Ezzel szemben a fiatalabbak differenciáltabb megközelítést jeleztek, 52 százalékuk azt válaszolta, hogy a megítélés attól függ, melyik alkalmazásról van szó. Ez az alkalmazásfüggő értékelés alkalmazkodóképességre utal, és illeszkedik az online interakciós minták életkor szerinti különbségeiről szóló megfigyelésekhez (Maier et al., 2023).

A védekező magánélet-védelmi magatartás hasonló demográfiai lejtőt mutatott. A regisztráció során megadott hamis információk átlagos pontszáma a hatfokú skálán 2,59 volt, ugyanakkor az eloszlás korcsoportonként jelentősen különbözött, amit a 4. ábra is jelez. A fiatalabb és az idősebb válaszadók között számottevő eltérések jelentek meg, a 18-25 éveseknél 1,34, a 65 év felettieknél 0,29 értékkel. A jelenség összhangban áll az életkor és az adatmanipuláció között dokumentált negatív korrelációval (Montgomery et al., 2017), amennyiben a fiatalabbak nagyobb digitális jártassága többféle, tudatosabban alkalmazott adatvédelmi ellenintézkedést tesz lehetővé.



4. ábra: Hamis adatok megadása a regisztráció során
Forrás: Saját szerkesztés a primer kutatás alapján (N=207)

A kutatás három, egymást erősítő összefüggést emel ki. Egyrészt a GDPR-ról tájékozott válaszadók aránya 35,27 százalék volt, és körükben a hamis információk megadása 16 százalékkal meghaladta a mintára számított átlagot, ami dinamikusabb adatvédelmi kontrollra utal. Másrészt a kockázatészlelés nem járt együtt a használat következetes visszafogásával,

mivel a leggyakrabban használt alkalmazások között a YouTube és a TikTok egyszerre jelentek meg domináns használati és magas bizalmatlansági mintázatokkal. A harmadik összefüggés az életkor hatása, amely egyszerre formálta az aggodalmak mértékét és a védekező magatartások jellegét. Az idősebbek következetesebb, ugyanakkor kevésbé kifinomult stratégiákat mutattak, miközben a fiatalabbaknál paradox módon az adatgyűjtés nagyobb elfogadása mellett proaktív védekezési eszközök, például hamis információk megadása jelent meg. Ez a kettősség a szakirodalomban leírt adatvédelmi pragmatizmus keretében értelmezhető (Berriman & Jaynes, 2022).

A nemzetközi összevethetőség szempontjából a platformokhoz kapcsolódó kockázati prioritások is figyelmet érdemelnek. A mintában a TikTok dominált a magánélet-védelmi aggályok terén, 73,39 százalékos értékkel a Facebook 44,3 százalékával szemben. Ez eltérést jelez azoktól a leírásoktól, amelyek szerint nyugat-európai kontextusban gyakran a Meta-platformok állnak az adatvédelmi viták fókuszában (Bruin, 2022). A különbség magyarázatában szerepet játszhat a TikTok magyarországi megjelenésének időzítése és az ebből következő újdonsághatás, valamint a platform iránti bizalmat befolyásoló kulturális tényezők is (Durmishi, 2024).

A GDPR ismerete és annak hatása az adatvédelmi magatartásra

A tanulmány markáns viselkedésbeli eltéréseket jelez a GDPR-t ismerő és a GDPR-t nem ismerő válaszadók között. A GDPR-tudatos csoport a minta 35,27 százalékát képviseli (n=71), és összességében óvatosabb adatkezelési gyakorlat rajzolódik ki náluk. Az 1. ábra alapján a GDPR-t ismerő résztvevők a teljes minta átlagához ($\bar{x}$=2,59) viszonyítva gyakrabban adtak meg pontatlan adatokat online regisztráció során ($\bar{x}$=3,01 a hatfokú skálán). Ez arra utal, hogy a szabályozás ismerete nem feltétlenül a platformhasználat visszaszorításában, hanem a magánélet védelmét célzó tudatos, védekező jellegű megoldások erősödésében jelenik meg. A megfigyelés illeszkedik (Mühlhoff, 2023) következtetéseihez, amelyek a szabályozást ismerő felhasználók körében gyakoribb álnevesítési, azonosítást csökkentő magatartásformákat írnak le.

A platformhasználati mintázatok szintén eltértek a két csoportban. A TikTok mindkét csoportban erős elkötelezettséget mutatott, a GDPR-t ismerők körében 21,90 százalékos használati aránnyal. Ezzel szemben a Meta platformjai visszafogottabb elfogadottságot jeleztek, különösen a Facebook és a Messenger esetében, ahol a GDPR-tudatos felhasználók 18 százalékkal kevesebb interakcióról számoltak be. Az Instagram kivételt jelentett, mivel a tájékozott csoportban a felhasználói bázis 78 százaléka megmaradt, ugyanakkor a napi használati idő 12 perccel mérséklődött. Ez a szelektív alkalmazkodás inkább platformonként differenciált kockázatértékelésre utal, nem pedig az adatigényes szolgáltatásoktól való általános visszavonulásra. Az értelmezés összhangban áll (Garcia-Rivadulla, 2016) helyzet-specifikus adatvédelmi döntéshozatali keretrendszerével, amely szerint a felhasználói adatvédelmi döntések kontextusfüggően alakulnak. A kockázatészlelési eredmények tovább erősítik ezt a kettősséget. A GDPR-tudatos csoporton belül 83,33 százalék jelölte meg a közösségi médiát a legfontosabb adatvédelmi problémaként, ami 15 százalékos emelkedés a teljes mintához képest. Miközben a TikTok kockázati besorolása magas szinten maradt (65,79 százalék), a teljes minta átlagához viszonyítva 7,6 százalékpontos csökkenés figyelhető meg. Ezzel párhuzamosan a Facebook észlelt veszélyessége 9,8 ponttal magasabb értéket vett fel (54,2 százalék a 44,3 százalékkal szemben). A mintázat arra utal, hogy a szabályozási előírások növelhetik a tudatosságot bizonyos adatkezelési gyakorlatokkal kapcsolatban, ideértve a Meta-platformok közötti nyomon követés érzékelését, miközben enyhíthetik az aggodalmakat egyes, újabb

szolgáltatásokkal, például a TikTokkal összefüggésben. Ez az eredmény eltér attól az elvárástól, amely a kockázatészlelés következetes emelkedését vagy egységes szerkezetét feltételezné (Agboola, 2025).

Az életkor szerinti bontásban végzett elemzés azt mutatta, hogy a GDPR-ról tájékozottabb fiatalok, azaz a 18–25 évesek körében a pontatlan, hamis adatok megadása gyakoribb volt, az átlagpontszámuk 3,24 volt, míg a tájékozatlan kortársaiké 2,91 egy hatfokú skálán. Ez inkább arra utal, hogy a szabályozási ismeretek a fiataloknál már meglévő adatvédelmi stratégiákat erősítik fel, és kevésbé arra, hogy teljesen új viselkedésmintákat alakítanának ki. Ugyanez a csoport mutatta a legárnyaltabb adatgyűjtési attitűdöket is, mivel 77,78 százalékuk jelezte, hogy az aggodalma alkalmazásfüggő. Ez 25 százalékponttal magasabb arány, mint az ugyanilyen korú, de GDPR-ról nem tájékozott résztvevők esetében. Az alkalmazásspecifikus megkülönböztetés képessége összhangban áll (Ma & Chen, 2023) megállapításaival, amelyek szerint a fiatalabb felhasználók képesek finom különbségeket érzékelni a platformarchitektúrák között. Az eredmények összességében azt támasztják alá, hogy indokolt az egyes platformokra szabott adatvédelmi oktatás, amely kifejezetten kezeli az egymásnak ellentmondónak tűnő viselkedésformákat.

Bár a GDPR ismerete a mintában több ponton is a védekező jellegű magatartásokkal együtt járt, az ismertség alacsony szintje, 35,27 százalék, arra utal, hogy a felhasználók többsége a jogait részben vagy teljesen ismeretlen keretrendszerben gyakorolja. A különbség különösen látványos az idősebb korosztályok esetében, ahol magasabb aggodalomszint mellett is alacsonyabb tudásszint rajzolódik ki. A célzott beavatkozások ezért egyrészt építhetnek a fiatalok technológiai rugalmasságára (Sas et al., 2023), másrészt reagálhatnak az idősebb felnőttek igényére az egyszerű, követhető és azonnal alkalmazható adatvédelmi megoldások iránt.

A 4. ábra három, GDPR-tudatossághoz kapcsolódó mintázatot emel ki. A hamis adatok benyújtásának gyakorisága minden korosztályban magasabb a tájékozottabb résztvevők körében, és ez a különbség a 25–35 éveseknél a legerősebb, ahol az átlag 3,45 volt. Emellett a jól ismert adatgyűjtőkkel, például a Facebookkal kapcsolatban erősebb kockázatészlelés jelenik meg. Végül az is látható, hogy a képközpontú platformokkal, például a TikTokkal és az Instagrammal való aktív kapcsolat fennmarad akkor is, ha a magánélet védelmével kapcsolatos aggodalmak erősek. Mindez arra utal, hogy a GDPR-előírások nem feltétlenül mérséklik következetesen a platformhasználat intenzitását, inkább átalakítják az interakciók jellegét, amit (Solove, 2021) az adatvédelmi tudatossággal együtt járó részvételként ír le. A nyílt végű válaszokból származó kvalitatív megfigyelések kontextusba helyezik a fenti tendenciákat. A GDPR-tudatos résztvevők gyakran számoltak be adatminimalizálási stratégiák alkalmazásáról, például ideiglenes e-mail cím használatáról regisztrációkor vagy a hirdetéskövetés kikapcsolásáról, miközben a platform alapfunkcióit továbbra is igénybe vették. Egy 24 éves női résztvevő megfogalmazása ezt jól illusztrálja: „Tisztában vagyok azzal, hogy az Instagram gyűjti a személyes adataimat, de korlátozom, amit posztolok, és virtuális magánhálózatot használok.” Az ilyen válaszok azt jelzik, hogy a platformhasználat értéke sok esetben meghaladja az észlelt kockázatot, amennyiben a felhasználó úgy érzi, képes a kockázatot kezelni. Az elemzés egy, a várakozásokkal részben ellentétes összefüggésre is rámutat a GDPR-tudatosság és az általános elutasítás viszonylatában. Azt lehetett volna feltételezni, hogy a szabályozás mélyebb megértése a platformok teljes elutasításának irányába tolja a felhasználókat, ezzel szemben egyetlen GDPR-t ismerő válaszadó sem jelölte azt, hogy az adatgyűjtés egyáltalán nem érdekli. Ez éles kontrasztban áll a tájékozatlan résztvevők 8,3 százalékával, akik ezt a véleményt képviselték.

A magyarországi szabályozási és információs környezet tovább árnyalja az eredmények értelmezését. Egyes európai összevetésekben a GDPR-ismertség 50 százalék feletti értéket is elér (Milošević et al., 2018), ehhez képest a vizsgált mintában mért 35,27 százalékos arány tartós oktatási és tájékoztatási hiányosságokra utal. E hiányosságok mögött szerepet játszhat a helyi nyelvű, közérthető források korlátozott elérhetősége, valamint az a környezet is, amelyben a megfelelési ösztönzők és a mindennapi adatvédelmi diskurzus kevésbé erőteljes (Molnár-Gábor et al., 2022). Ez a háttér magyarázhatja azt is, hogy a GDPR-t ismerő válaszadók esetében sem minden viselkedés következetes, mivel a részleges vagy töredezett tudás a normák eseti, ingadozó alkalmazásához vezethet. Az eredmények egyszerre hordoznak szakpolitikai és platformtervezési következtetéseket. A GDPR megértése és a magánélet védelmét szolgáló intézkedések, például a hamis adatok megadása közötti kapcsolat arra utal, hogy a személyre szabott, célcsoport-specifikus oktatási programok erősíthetik a felhasználói önrendelkezést, különösen az idősebb korosztályokban, ahol az adaptív stratégiák kevésbé jelennek meg. Ugyanakkor a magas kockázatúnak tartott platformok iránti tartós függés azt jelzi, hogy a puszta szabályozási tudatosság sok esetben nem elegendő a strukturális kötődések oldásához, ezért a technikai jellegű megoldások, például a decentralizált architektúrák irányába mutató törekvések is relevánsak lehetnek (Mehta, 2023). A tanulmány fő üzenete ebben a keretben az, hogy a GDPR-ismeret nem egyszerűen kétállapotú tényezőként működik, hanem viselkedést formáló hatásként jelenik meg. Nem feltétlenül megszünteti, inkább átalakítja az adatigényes platformokkal való interakciót, ami részben ellentmond azoknak a megközelítéseknek, amelyek a szabályozási tudatosságtól automatikusan nagy léptékű platformváltást várnak.

4. Korlátozások

A kutatás eredményeinek értelmezését korlátozza, hogy a minta demográfiai összetétele a fiatalabb, magasabban képzett magyar válaszadók felé tolódik, így az általánosíthatóság az idősebb korosztályokra és más kulturális kontextusokra mérsékelten érvényes. További bizonytalansági forrás, hogy több változó önbevalláson alapult, ezért a képernyőidő és az adatvédelmi viselkedések, különösen az érzékeny tevékenységek, például a hamis adatmegadás esetén válaszadói torzítások nem zárhatók ki. Ennek megfelelően a megfigyelt mintázatok inkább egy adott időpontban rögzített, átmeneti viselkedési állapotokat tükröznek, mint stabil, hosszabb távon fennmaradó jellemzőket.

5. Következtetés

A vizsgálat eredményei alapján a GDPR-tudatosság, a platformhasználat és az AI-hoz kapcsolódó attitűdök között érdemi összefüggések azonosíthatók, amelyek generációs metszetben eltérő mintázatokat mutatnak. A GDPR alapismereteinek viszonylag alacsony szintje mellett is megjelennek magánélet-védelmi, védekező stratégiák, ugyanakkor ezek a stratégiák jellemzően nem a platformok következetes elhagyásában öltenek testet. Inkább a használat tudatos „finomhangolásában” és az adatközlés feletti kontroll erősítésében ragadhatók meg, például a megadott információk körének szűkítésében, a beállítások módosításában, illetve egyes felületek esetében a használati idő csökkentésében. Ez a minta arra utal, hogy a szabályozási ismeretek gyakorlati hatása sok esetben nem bináris, hanem adaptív jellegű, vagyis a felhasználói viselkedést inkább átrendezi, mintsem megszünteti a kockázatosnak ítélt digitális rutinokat. A kockázati rangsorokban a TikTok tartósan kiemelt pozíciója különösen fontos következtetéshez vezet. A magas kockázatészlelés önmagában nem jelenti a használat visszaesését, ami a digitális platformok értékajánlata és a felhasználók kontrollélménye közötti feszültségre utal. A felhasználók egy része úgy tűnik, hogy a kockázatot nem a kilépéssel, hanem az észlelt irányíthatóság növelésével, azaz mikroszintű

beavatkozásokkal kezeli. Ezzel párhuzamosan a közösségi média, mint kiemelt adatvédelmi probléma erősödő megjelölése azt jelzi, hogy a szabályozási keretekre vonatkozó tudás és a mindennapi platformgyakorlat között sokaknál nem alakul ki közvetlen, lineáris kapcsolat. A viselkedés inkább kompromisszumos és kontextusfüggő, ahol a hasznosság, a társas kapcsolati érték és a szórakoztatási funkciók gyakran felülírják az elutasítási szándékot. Az AI-val kapcsolatos attitűdök életkor szerinti erősödése további társadalmi értelmezési szempontot nyit. Az algoritmikus közvetítéssel szembeni nyugtalanság növekedése idősebb korban arra utal, hogy az AI elfogadása nem homogén jelenség, hanem eltérő tapasztalati háttérhez, digitális kompetenciához és kontrollérzethez kötődik. A kockázatok értelmezése így nem pusztán technológiai kérdésként jelenik meg, hanem bizalmi és érthetőségi dimenziókat is magában foglal. Ebben a keretben a generációs különbségek nem kizárólag a használati intenzitásban, hanem a kockázatkezelés logikájában és a technológiával szembeni elvárásokban is megmutatkoznak.

Oktatási és fogyasztóvédelmi szempontból mindez megerősíti a platformspecifikus adatvédelmi ismeretek fejlesztésének szükségességét. A jövőbeni beavatkozások akkor lehetnek hatékonyak, ha nem általános elveket ismételnek, hanem gyakorlati helyzetekhez kapcsolják a GDPR alkalmazását. Kiemelt jelentősége van annak, hogy a felhasználók értsék a beállítási döntések következményeit, az adatkezelési célok és jogosultságok logikáját, valamint azokat a tipikus pontokat, ahol az adatgyűjtés intenzívebbé válik. A kutatás alapján indokolt olyan célzott oktatási megoldások kialakítása, amelyek külön kezelik a fiatalabb korcsoportokra jellemző, tudatos, de kompromisszumos platformhasználatot, és az idősebbek esetében hangsúlyosabbá teszik az egyszerű, lépésről lépésre követhető védelmi mechanizmusokat. Összességében a tanulmány arra mutat rá, hogy a GDPR-tudatosság növelése önmagában nem elegendő a kockázatos platformfüggőségek oldásához, viszont érdemben hozzájárulhat ahhoz, hogy a felhasználók a mindennapi digitális döntéseikben nagyobb kontrollt és tudatosságot érvényesítsenek.

Felhasznált források

Agboola, O.(2025)., The Evolving Landscape of Data Privacy: How Regulations are Shaping the Digital World. http://dx.doi.org/10.2139/ssrn.5187183

Barth, S., & Jong, M. D. T. de (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34(7),* 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Berriman, L., & Jaynes, V. (2022). Displaying family in a digital age: How parents negotiate technology, visibility and privacy. *Negotiating Families and Personal Lives in the 21st Century.* https://doi.org/10.4324/9781003039433

Bruin, R. D. (2022). A comparative analysis of the EU and US data privacy regimes and the potential for convergences. *Hastings Sci. & Tech. LJ.* https://doi.org/10.2139/ssrn.4251540

Chung, K.-C., Chen, C.-H., Tsai, H.-H., & Chuang, Y.-H. (2021). Social media privacy management strategies: A SEM analysis of user privacy behaviors. *Computer Communications, 174*, 122–130. https://doi.org/10.1016/j.comcom.2021.04.012

Csiszár, Cs. M., 2019. Adatvédelem a digitális térben avagy mennyire vagyunk biztonságban. In: Veresné, Somosi Mariann; Lipták, Katalin (szerk.) Mérleg és Kihívások XI. Nemzetközi Tudományos Konferencia. Miskolc, Magyarország: Miskolci Egyetem, Gazdaságtudományi Kar (2019) 565 p. pp. 62-68.

Durmishi, C. (2024). Adoption of Digital Platforms For Knowledge Sharing: A Comparative Study Of SMEs In Western Balkan Countries. *KNOWLEDGE-International Journal*.
Garcia-Rivadulla, S. (2016). Personalization vs. Privacy: An inevitable trade-off? *IFLA Journal*. https://doi.org/10.1177/0340035216662890

Európai Parlament és a Tanács (2016): Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) … (GDPR). HL L 119., 2016.5.4., 1–88. o. CELEX: 32016R0679.

Kiss, G., 2020. Az információ hatalom? In Tavaszi Szél - Spring Wind 2019: Tanulmánykötet 2. pp. 298–305.

Ma, S., & Chen, C. (2023). Are digital natives overconfident in their privacy literacy? Discrepancy between self-assessed and actual privacy literacy, and their impacts on privacy protection behaviour. Frontiers in Psychology, 14, 1224168. https://doi.org/10.3389/fpsyg.2023.1224168

Mai, J. (2019). Situating personal information: Privacy in the algorithmic age. *Human Rights in the Age of Platforms*. https://doi.org/10.7551/mitpress/11304.003.0009

Maier, E., Doerk, M., Reimer, U., & Baldauf, M. (2023). Digital natives aren't concerned much about privacy, or are they? i-com, 22(1), 83–98. https://doi.org/10.1515/icom-2022-0041

Mehta, D. (2023). Privacy-preserving machine learning architecture for cross-channel advertising optimization in a large-scale social media platform. *Social Science Research Network* http://dx.doi.org/10.2139/ssrn.5424002

Milošević, N., Dobrota, M., & Barjaktarović Rakočević, S. (2018). Digital economy in Europe: Evaluation of countries' performances. Zbornik Radova Ekonomskog Fakulteta u Rijeci, 36(2), 861–880. https://doi.org/10.18045/zbefri.2018.2.861

Molnár-Gábor, F., Sellner, J., Pagil, S., et al. (2022). Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four member states and ways to overcome them by EU measures: Insights from Germany, Greece, Latvia and Sweden. *Seminars in Cancer Biology*. https://doi.org/10.1016/j.semcancer.2021.12.001

Montgomery, K., Chester, J., et al. (2017). Ensuring young people's digital privacy as a fundamental right. *International Handbook of Media Literacy Education.* https://doi.org/10.4324/9781315628110

Mühlhoff, R. (2023). Predictive privacy: Collective data protection in the context of artificial intelligence and big data. *Big Data & Society*, *10*(1). https://doi.org/10.1177/20539517231166886

Ooijen, I., Segijn, C. M., & Opree, S. J. (2024). Privacy cynicism and its role in privacy decision-making. *Communication Research*, *51*(2), 146–177. https://doi.org/10.1177/00936502211060984

Sas, M., Denoo, M., & Mühlberg, J. (2023). Informing children about privacy: A review and assessment of age-appropriate information designs in kids-oriented F2P video games. *Proceedings of the ACM on Human - Computer Interaction*. https://doi.org/10.1145/3611036

Solove, D. (2021). The myth of the privacy paradox. *George Washington Law Review vagy Social Science Research Network Vol. 89 No. 1* http://dx.doi.org/10.2139/ssrn.3536265