KARDOS VIVIEN KATA*

Joghallgatók adatvédelmi tudatossága

„A műveltség nem azt jelenti, hogy tudjuk, hanem azt, hogy tesszük."

(Napoleon Hill)

I. Bevezetés

A XXI. század vezérszavai között említhető a digitalizáció, a különféle technológiai vívmányok megjelenése és fokozatos elterjedése, az adatvédelem, a közösségi média felületek, valamint nem utolsó sorban ezen tendenciáknak a jog világára is kiemelt szereppel bíró hatásai. Kérdésként merülhet fel, hogy az adatvédelem miért kapott helyet e felsorolásban. *Meglena Kuneva* már 2009-ben felhívta a figyelmet nyilatkozatában a személyes adatok kardinális jelentőségére. *„Az internet egy hirdetésekkel támogatott szolgáltatás, amelyet a profilalkotáson és a személyes adatokon alapuló marketing fejlődése mozgat. A személyes adat az internet új olaja és a digitális világ új fizetőeszköze."*[1] Ezzel összefüggésben nem számít újkeletű megállapításnak, hogy az elmúlt időszakban az adatvédelem fontossága még inkább felértékelődött.

Gyakorlati szempontból is meghatározó jelentőséggel bír az Európai Parlament és a Tanács (EU) 2016/679 rendelete[2], amely alapvetően meghatározza a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmét és az ilyen adatok szabad áramlását. Ugyanakkor – a részletes ismertetéstől eltekintve – megjegyzendő, hogy az adatvédelem magyar jogrendszerben történő megvalósulása az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény[3], valamint a további ágazati jogszabályok által – az átfogó uniós jogi szabályrendszer bevezetését megelőzően is – szigorú szabályozási kultúrát teremtett meg. Ennek alátámasztásaként szolgál *Péterfalvi Attila* kijelentése, amely szerint a magyar adatvédelmi szabályozás

* Szegedi Tudományegyetem Állam- és Jogtudományi Kar

1 MEGLENA KUNEVA (az Európai Bizottság fogyasztóvédelemért felelős biztosa 2007–2010): *Keynote Speech, Roundtable on Online Data Collection, Targeting and Profiling.* Brussels. 2009.03.31. – ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156 [2019.12.11.] A szakirodalmi álláspont nem egységes „az adat az új olaj" megítélésével és értelmezésével kapcsolatban.

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

3 A továbbiakban: Info. törvény.

szintjét nem szigorította a GDPR, hiszen az egyébként is nagyon szigorú volt, méghozzá *„az egyik legszigorúbb a világon”*. Mindazonáltal megállapítható, hogy lényeges változásokat eredményezett, különösképpen az adatkezelés jogalapjára és struktúrájára vonatkozóan.[4]

A tendenciákat tükröző jogi keretek megalkotása, valamint ezek gyakorlati alkalmazásának és megvalósulásának vizsgálata kizárólag az érme egyik oldalát világítja meg. Homály fedheti, hogy a természetes személyek hogyan viszonyulnak az adatvédelem komplexitásához, milyen fokú ismeretek birtokában állnak, valamint az adatvédelmi tudatosságuk miképpen illeszkedik a jogforrásokban deklarált adatvédelmi garanciákhoz. E tudatosság pedig nélkülözhetetlen ahhoz, hogy az adatvédelem, pontosabban az adatalanyok védelme ténylegesen és a lehető legmagasabb szinten realizálódhasson.

1. Témafelvetés

Az ipar 4.0 következményei között említhető az adatvédelmi kihívások megjelenése, valamint az adatvédelmi igény egyre növekvő megnyilvánulása.[5] Az *Internet World Stats* legfrissebb adatai szerint világviszonylatban megközelítőleg 4,54 milliárd internethasználó van.[6] Ennélfogva a virtuális tér mindennapjainkba történő beágyazódása az adatvédelem területén is új kihívásokat eredményez. A megfelelő jogszabályi keretek biztosítása mellett a természetes személyek részéről elengedhetetlen a kellő mértékű tájékozottság megléte, továbbá az ismeretekkel összhangban történő tudatos cselekvés.

A jogásztársadalom tekintetében az adatvédelem kettős megvilágításban is értelmezhető. Egyrészt természetes személyként a „saját” személyes adatai vonatkozásában, másrészt csekély mértékben elképzelhető, hogy akár napjainkban, akár a jövőben egy jogász a munkája során – elegendő például az adatkezelésre gondolni – az adatvédelem területét teljes egészében elkerülje, bármely jogágról legyen is szó. Ezzel összefüggésben példaként említhető, hogy az adatvédelmi tudatosság *expressis verbis* az általános adatvédelmi rendeletben is kifejezésre jut az adatvédelmi tisztviselő feladatainak meghatározásánál[7], amely szerint a feladatkörébe tartozik annak ellenőrzése, hogy a személyzet megfelelő adatvédelmi tudatossággal látja-e el tevékenységét.[8] Ebből következően az adatvédelmi tudatosság előírásként szerepel a személyzet tekintetében, e szempontból pedig a személyzet tág körben értelmezendő. Ehhez kapcsolódóan a munkavégzéssel összefüggésben megjelenik az adatvédelem, ugyanakkor kérdéseket vethet fel,

---

[4] OPH – OrientPress Hírügynökség: *Péterfalvi: Európai adatvédelmi rezsimváltás történt, a GDPR csak az egyik elem.* 2019.05.08. – www.orientpress.hu/cikk/2019-05-08_peterfalvi-europai-adatvedelmi-rezsimvaltas-tortent-a-gdpr-csak-az-egyik-eleme [2019. 12. 12.]

[5] OESTERREICH, THUY DUONG – TEUTEBERG, FRANK: *Understanding the implications of digitisation and automation in the context of Industry 4.0: A triangulation approach and elements of a research agenda for the construction industry.* Computers in Industry, Vol. 83. (2016) 136. p.

[6] INTERNET WORLD STATS: *World Internet Usage and Population Statistics*. 2019 Mid-Year Estimates. 2019.06.30. – www.internetworldstats.com/stats.htm [2019.12.19.]. Összesen 4.536.248.808 internethasználó.

[7] GDPR 39. cikk (1) bekezdés b) pont

[8] SZABÓ ENDRE GYŐZŐ: *Az adatvédelmi tisztviselőről – A GDPR szabályainak elemzése,* Infokommunikáció és Jog 2018/1. (70.) – infojog.hu/szabo-endre-gyozo-az-adatvedelmi-tisztviselorol-a-gdpr-szabalyainak-elemzese-20181-70-3-10-o/ [2019. 12. 15.] 8. p.

hogy vajon a magánéletben például a közösségi média használatakor ez milyen mértékben jelenik meg.

Nem számít újkeletű megállapításnak, hogy a közösségi oldalak használata a „digitális bennszülöttek”[9] korosztályában mindennaposnak tekinthető. Ezzel összefüggésben kérdésként merül fel, hogy a hallgatók ezen oldalak használata során példának okáért milyen személyes adatokat, milyen hozzáférhetőséggel osztanak meg a nagyvilággal, figyelmet fordítanak-e mások személyes adatainak védelmére. Összefoglalva, milyen mértékben jelenik meg az adatvédelmi tudatosság, esetlegesen annak hiánya állapítható meg.

2. Célkitűzések

Jelen dolgozat alapját képező empirikus kutatás[10] a joghallgatók adatvédelmi tudatosságát hivatott felmérni a közösségi oldalak használatának kontextusában. A kutatás központi elemét képezi annak feltérképezése, hogy a joghallgatók körében milyen mértékben figyelhető meg az adatvédelmi tudatosság, valamint általánosságban véve hogyan viszonyulnak az adatvédelemhez, milyen fokú tájékozottsággal rendelkeznek, valamint cselekedeteik mennyire állnak összhangban megszerzett ismereteikkel.

Jogosan merülhet fel a kérdés, hogy miért fontos ezen témakört vizsgálni. A kutatás célja egyrészt, hogy valós képet mutasson a joghallgatók jelenlegi adatvédelmi tudatosságáról azáltal, hogy az adatvédelemről megszerzett ismereteik, az attitűdjük, valamint a szokásaik milyen módon jelennek meg a mindennapokban, mint például a közösségi média világában. Ezáltal lehetőséget biztosít a joghallgatók figyelmének felhívására, hogy esetlegesen nem kellő figyelmet fordítanak személyes adataik védelmére, hiszen a szokások, az attitűd a jövőjüket illetően is mérvadó. Ezenkívül az esetleges tudásbéli hiányosságok feltárása esetén visszacsatolásként szolgál, hogy mely területeken szükséges a tudásbázisuk bővítése, valamint a „nem kifejezetten személyes adataik védelmét támogató” szokásaik realizálására nyílik mód, adott esetben a jelenlegi beállítások tekintetében módosításokat eszközöljenek.

3. Hipotézisek

A kutatás főbb hipotézisei az alábbiak szerint kerültek meghatározásra:

A joghallgatók adatvédelmi tudatossága tekintetében jelentős hiányosságok figyelhetők meg.

---

[9] PRENSKY, MARC: *Digital Natives, Digital Immigrants, On the Horizon*. MCB University Press Vol. 9. No. 5. (2001) www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20 Part1.pdf [2019. 12. 04.] 1. p.

[10] A kutatást az EFOP-3.6.2-16-2017-00007 azonosító számú, Az intelligens, fenntartható és inkluzív társadalom fejlesztésének aspektusai: társadalmi, technológiai, innovációs hálózatok a foglalkoztatásban és a digitális gazdaságban című projekt támogatta.

Az adatvédelem jelentőségének elismerése megjelenik ugyan a joghallgatók körében, ezzel ellentétben a közösségi oldalakon megjelenő „aktivitás" nem teljesen ennek megfelelően alakul.

A személyes adat gyakorlati példákon keresztül történő azonosítása nehézséget okoz. Egy bizonyosfajta ismerethiány figyelhető meg arra vonatkozóan, hogy pontosan milyen információk minősülnek személyes adatnak.

A képmegosztási szokásokat illetően az adatvédelmi tudatosság a „saját" személyes adatok tekintetében érvényesül, más személyek személyes adatainak védelme viszont a háttérbe szorul, jelentős tudásbéli hiányosságok nyernek megállapítást.

A hozzájárulás megadása szempontjából a hallgatók nem kellő mértékben körültekintők mind az attitűddel, mind a szokásokkal összefüggésben.

4. A dolgozat struktúrája

Az adatvédelmi tudatossággal kapcsolatos terminológia szakirodalmi áttekintését – beleértve a közösségi oldalak használatára vonatkozó részt – a dolgozat alapját képező empirikus kutatás részletgazdag ismertetése követi. A kutatási eredmények részletes bemutatása és elemzése révén a kutatás főbb konzekvenciáinak levonása áll a dolgozat fókuszpontjában. A kutatás összegzése, valamint a jövőre vonatkozó *de lege ferenda* javaslatok megfogalmazása a dolgozat záróakkordjaként jelenik meg.

II. Az adatvédelmi tudatossággal kapcsolatban felmerülő tárgykörök szakirodalmi áttekintése

1. Az empirikus kutatás tárgyával összefüggő alapfogalmak

1. 1. Adatvédelem

Jelen dolgozat a joghallgatók adatvédelmi tudatosságának kérdéskörét hivatott feltérképezni, mindazonáltal elengedhetetlen szűkkörűen kitérni az adatvédelem különböző dimenzióira, különösképp az adatvédelem definiálására, amely az információs önrendelkezési joggal is korrelációban áll. Az Alkotmánybíróság 15/1991. (IV. 13.) határozatában kifejtette, hogy *„a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként értelmezi, hanem annak aktív oldalát is figyelembe véve, információs önrendelkezési jogként".* Az adatvédelem definíciója olyan jogi védelmet foglal magában, amelynek elődleges célja az egyének magánszférájának védelme az egyénnel kapcsolatba hozható adatok (személyes adatok) kezelésére vonatkozó szabályozás meghatározásával.[11] Tágabb értelmezésben az adatvédelem fogalmi körébe alapvetően a

[11] JÓRI ANDRÁS (szerk.): *A GDPR magyarázata*. HVG ORAC, Budapest, 2018. 26. p.

személyes adatok jogszerű kezelése, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége is beletartozik.[12]

A hazai jogforrási hierarchia különböző szintjein is kiemelt szereppel bír az adatvédelem. Ennek megfelelően az előzőekben említett uniós rendeleti szabályozáson túlmenően az Alaptörvény VI. cikk (3) bekezdése deklarálja, hogy mindenkinek joga van személyes adatai védelméhez, valamint a (4) bekezdésben foglaltak alapján e jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság, a Nemzeti Adatvédelmi és Információszabadság Hatóság[13] ellenőrzi. Az általános adatvédelmi rendeleten kívül az egyik legfőbb jogszabály az Info. törvény. Mindazonáltal hangsúlyozandó, hogy az adatvédelem különböző aspektusai számos jogszabály rendelkezései között kaptak helyet, példaként említhető a Polgári Törvénykönyvről szóló 2013. évi V. törvény, továbbá teljesen más perspektívából tekintve a Büntető Törvénykönyvről szóló 2012. évi C. törvény.

1. 2. „Privacy awareness" avagy az adatvédelmi tudatosság

Jelenleg sem a hazai, sem a nemzetközi szakirodalomban nem került még sor az adatvédelmi tudatosság terminológiájának egzakt, teljeskörű meghatározására. Az adatvédelmi tudatosság fogalmának *Deuker* szerinti megközelítése kettős célkitűzésre terjed ki, mégpedig az egyéni felhasználók azon képességére, hogy egyrészt azonosítsák, másrészt felmérjék a személyes adatok nyilvánosságra hozatalához kapcsolódó kockázatokat.[14] Az adatvédelmi tudatosság definiálásának további megközelítése magában foglalja, annak „megértését", hogy ki követi nyomon és gyűjti a személyes adatokat, mikor kerül sor az adatok gyűjtésére, más szervezetek milyen adatokat „kapnak", tárolnak, használnak, valamint hogyan valósul meg az adatok feldolgozása a felhasználók profiljainak részletesen felépítése érdekében.[15]

Ennek szűkebb körű meghatározása értelmében az adatvédelmi tudatosság az egyén azon ismereteit öleli fel, hogy a személyes adatokat ki, mikor, hogyan, valamint milyen mértékben kezeli és használja fel a tevékenységével összefüggésben.[16] *Pötzsch* álláspontja, hogy az emberek általában tisztában vannak a magánélet tiszteletben tartásá-

---

[12] NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG: *Adatvédelmi értelmező szótár* – www.naih. hu/adatvedelmi-szotar.html [2019. 11. 23.]

[13] A továbbiakban: NAIH.

[14] DEUKER, ANDRÉ: *Addressing the Privacy Paradox by Expanded Privacy Awareness – The Example of Context-Aware Services.* IFIP PrimeLife International Summer School on Privacy and Identity Management for Life Privacy and Identity: Privacy and Identity Management for Life (2009) 278. p. – link.springer.com/content/pdf/10.1007/978-3-642-14282-6_23.pdf [2020.01.20.]

[15] MALANDRINO, DELFINA – PETTA, ANDREA – SCARANO, VITTORIO – SERRA, LUIGI – SPINELLI, RAFFAELE – KRISHNAMURTHY, BALACHANDER.: *Privacy Awareness about Information Leakage: Who knows what about me?* Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society. 2013. – www.di-srv.unisa.it/~delmal/papers/UNISA-ISIS-082913TR.pdf [2020.01.16.] 2. p.

[16] PÖTZSCH, STEFANIE: *Privacy Awareness: A Means to Solve the Privacy Paradox?* The Future of Identity in the Information Society. IFIP Advances in Inf. and Commun Tech. Vol. 298. Springer Boston, 2009. 226. p. – link.springer.com/content/pdf/10.1007/978-3-642-03315-5_17.pdf [2020.01.20.]. OMORONYIA, INAH – CAVALLARO, LUCA – SALEHIE, MAZEIAR – PASQUALE, LILIANA – NUSEIBEH, BASHAR: *Engineering adaptive privacy: on the role of privacy awareness requirements. In: 35th International Conference on Software Engineering* (ICSE 2013). 18-26 May 2013. San Francisco. CA. USA (forthcoming). 2013. 633. p.

val[17], mindazonáltal az adatvédelmi paradoxon arra világít rá, hogy nem a kijelentéssel összhangban valósul meg a cselekvés.[18] Az adatvédelmi tudatosság az adatvédelmi paradoxon feloldásának egyik lehetséges eszközeként jelenik meg.[19]

Jelen dolgozatban az adatvédelmi tudatosság tág értelmezése a mérvadó. Ok-okozati összefüggésben magában foglalja a megszerzett ismereteket, továbbá a mindezeknek megfelelő cselekvést, figyelembe véve, hogy az adott magatartás milyen kockázati következményeket rejt a személyes adatok vonatkozásában.

1. 3. „Privacy literacy" avagy az adatvédelmi műveltség

Az adatvédelmi tudatosság fejlesztésében meghatározó jelentőséggel bír az adatvédelmi műveltség, amely kérdéskörének tárgyalásakor először is distinkciót szükséges tenni a digitális műveltség (*„digital literacy"*) fogalmától. Először úgy tűnhet, hogy ugyanazt a jelentéstartalmat foglalják magukban, ennek ellenére hangsúlyozandó, hogy a két terminológia között jelentős különbségek mutatkoznak.

Az online adatvédelmi műveltség fogalma a személyes adatok online térben történő megosztásával kapcsolatos felelősség és kockázatok megértésére koncentrál, ezzel szemben a digitális műveltség az információ feladat-alapú felhasználására összpontosít a digitális környezetben.[20] Az online adatvédelmi műveltség a digitális műveltség keretein belül elengedhetetlen a felhasználók tudásának és tudatosságának javításához, valamint a készségek fejlesztéséhez annak érdekében, hogy képesek legyenek felmérni a technikai mechanizmusok és stratégiák kockázatát az internetes veszélyek elleni küzdelemben, következésképpen hatékony védelemben részesíthessék önmagukat.[21] A műveltség a tudás és a készségek terminológiájának összefonódásaként definiálható.[22]

Baek álláspontja alapján úgy tűnik, hogy a digitális műveltség pozitív hatást gyakorol az online magánélet védelmére[23], miközben ennek szintjét a technikai kifejezések – például a „sütik", a viselkedésalapú célzott reklámok, az adatbányászat – megértésének előfeltételeként rögzítették.[24] Az egyik általánosan megfogalmazott érv, hogy a magasabb szintű adatvédelmi ismeretekkel rendelkező emberek – beleértve az elméleti „tudni azt" és az gyakorlati „tudni hogyan" tudást – jobban védik magánéletüket. Az adatvé-

[17] Jelen esetben értsd: adatvédelem.
[18] PÖTZSCH 2009, 226. p.
[19] PÖTZSCH 2009, 227. p.
[20] WISSINGER, CHRISTINA L.: *Privacy Literacy*: *From Theory to Practice.* Communications in Information Literacy Vol. 11. No. 2. (2017) 379. p.
[21] SIDERI, MARIA – KITSIOU, ANGELIKI – TZORTZAKI, ELENI – KALLONIATIS, CHRISTOS – GRITZALIS, STEFANOS: *Enhancing university students' privacy literacy through an educational intervention: a Greek case-study*. Int. J. Electronic Governance. Vol. 11. No. 3/4. (2019) 336. p.
[22] SIDERI et al. 2019, 336. p.
[23] BAEK, YOUNG MIN – KIM, EUN-MEE – BAE, YOUNG: *My privacy is okay, but theirs is endangered: why comparative optimism matters in online privacy concerns*. Computers in Human Behavior Vol. 31. (2014) 132. p. PARK, YOUNG JIN: *Digital literacy and privacy behavior online.* Communication Research Vol. 40. No. 2. (2011) 220. p.
[24] HARGITTAI, ESZTER: *An update on survey measures of web-oriented digital literacy*. Social Science Computer Review Vol. 27. No. 1. (2009) 133. p.; PARK 2011, 227. p.

delmi műveltség ennek az ötvözetéből áll, ugyanis mindkét elemet magába foglalja.[25] E kérdéskör kapcsán *Napoleon Hill* idézett szavai kiemelt hangsúlyt kapnak, hiszen az, hogy bizonyos ismeretek elsajátításra kerültek, mégsem annak megfelelő – adott esetben azzal ambivalens – cselekvésre kerül sor, avagy válik szokássá ellentétben áll a műveltséggel. Kiegészítésként a megszerzett ismeretek a műveltség előfeltételeként értelmezendők.

A közösségi oldalak használatával összefüggésben a tanulmányok azt mutatják, hogy a műszaki ismeretek, készségek és az adatvédelmi beállítások ismerete pozitív korrelációban áll az adatvédelmi beállítások megváltoztatásával.[26] *Benson et al.* is a felhasználók tudatossága és az információk csökkenő közzététele között lévő pozitív kapcsolatot erősíti meg.[27] *Sideri et al.* tanulmányában kifejtettek alapján az adatvédelmi műveltség kettős vetülettel rendelkezik, egyrészt a felhasználóknak az adatvédelem technikai szempontú ismereteire vonatkozik, másrészt a felhasználók azon képességeire, amelyek lehetővé teszik, hogy stratégiát alkalmazhassanak az egyéni adatvédelmi szabályozáshoz.[28] *Park* és *Debatin* kutatásainak fókuszpontjában a felhasználók tudásának és készségeinek hiánya áll a magánélet védelmének biztosítása érdekében, ezen helyzet meghatározása a kognitív hiányosság elméletén keresztül történik.[29]

A jogalkotáson és a szolgáltatók adatvédelmi módszerein túlmenően a felhasználók adatvédelmi tudatosságának növelése és a releváns adatvédelmet szolgáló viselkedés kialakulása kiemelt jelentőséggel bír. Az adatvédelmi műveltség kulcsfontosságú az online adatvédelem megerősítése érdekében.[30] Az adatvédelmi műveltség fejlesztését célzó oktatás segítséget nyújthat a közösségi média felhasználóinak, hogy felmérjék a személyes adataik online térben történő megosztásának kockázatait.[31] Ezen túlmenően az adatvédelmi tudatosság fejlesztése körében is megerősítést nyert az oktatás jelentő-

---

[25] TREPTE, SABINE – TEUTSCH, DORIS – MASUR, PHILIPP. K. – EICHER, C. – FISCHER, MONA – HENNHÖFER, ALISA – LIND, FABIENNE: *Do people know about privacy and data protection strategies? Towards the 'online privacy literacy scale' (OPLIS)*. In: GUTWIRTH, S. – LEENES, R. – de HERT, P. (eds.): Reforming European Data Protection Law. Springer, Heidelberg, 2015. 343. p.

[26] BOYD, DANAH – HARGITTAI, ESZTER: *Facebook privacy settings: Who cares?*. First Monday Vol. 15. No. 8. (2010) – firstmonday.org/ojs/index.php/fm/article/view/3086/2589 [2019.11.16.]. KEZER, MURAT – SEVI, BARIS – CEMALCILAR, ZEYNEP – BARUH, LEMI: *Age differences in privacy attitudes, literacy and privacy management on Facebook. Cyberpsychology:* Journal of Psychosocial Research on Cyberspace 10(1). Article 2. (2016) – cyberpsychology.eu/article/view/6182/5912 [2019.11.02.] 1. p.

[27] BENSON, V. – SARIDAKIS, G. – TENNAKOON, H.: *Information disclosure of social media users. Does control over personal information, user awareness and security notices matter?* Information Technology and People Vol. 28. No. 3. (2015) 429. p.

[28] SIDERI et al. 2019, 336. p.

[29] PARK 2011, 226. p. DEBATIN, BERNHARD – LOVEJOY, JENNETTE P. – HORN, ANN-KATHRIN – HUGHES, BRITTANY. N.: *Facebook and online privacy: attitudes, behaviors, and unintended consequences.* Journal of Computer-Mediated Communication Vol. 15. (2009) 83–108. pp.

[30] BARTSCH, MIRIAM – DIENLIN, TOBIAS: *Control your Facebook: an analysis of online privacy literacy*. Computers in Human Behavior Vol. 56. (2016) 149. p.

[31] CORREIA, JOHN – COMPEAU, DEBORAH: *Information Privacy Awareness (IPA): A review of the use, definition and measurement of IPA*. In: *Proceedings of the 50th Hawaii International Conference on System Sciences*. Waikoloa HI, 2017. 4021–4030. pp. pdfs.semanticscholar.org/b9e7/0317060e75bdaf52174391fb1f93e77b5268.pdf [2019. 11. 25.] 4022. p. WISSINGER 2017, 382. p.

ségének elismerése mint lehetséges megoldási útvonal.[32] Ennek alátámasztásaként a nemzetközi pódiumon is kimagasló finn oktatási rendszer említhető, amely a legműveltebb nemzet „kitüntetést" is elnyerte[33]. A médiaműveltségre oly mértékben fektetnek hangsúlyt az oktatásba történő becsatornázása által, hogy külön nemzeti szakpolitika is megjelent, amely rögzíti, hogy *„[a] médiaműveltséget a magas szintű, rendszeres és mindenre kiterjedő médiaoktatás segíti elő és támogatja."*[34]

1. 4. Adatvédelmi paradoxon

Az előzőekben említett meghatározásoknál is megjelent az adatvédelmi paradoxon tárgyköre, amely az adatvédelmi tudatossággal szoros kapcsolatban áll. *Barnes* az adatvédelem, valamint a magánszférát övező ellentmondásosságára már 2006-ban ráirányította a figyelmet a fiatalok kontextusában. A tinédzser fiatalok egyrészt az interneten keresztül feltárják bizalmas gondolataikat és viselkedésüket, másrészt a kormányzati ügynökségek és a marketingszakemberek személyes adatokat gyűjtenek. A fiatalok megosztják magánéletüket az online térben, hatalmas mennyiségű adatot szolgáltatva, mivel nem teljesen értik az internet nyilvános természetét, valamint annak mögöttes folyamatait és esetleges következményeit. Sokan nincsenek tudatában annak, hogy a magánéletüket veszélyeztetik, és nem tesznek lépéseket annak érdekében, hogy megvédjék személyes adataikat a mások által történő felhasználástól.[35]

Az idő múlásával egyidejűleg új adatvédelmi paradoxon figyelhető meg, mivel a közösségi oldalak oly mértékben beágyazódtak a felhasználók magánéletébe, hogy annak ellenére is közzéteszik a rájuk vonatkozó személyes információkat, hogy ezek az oldalak nem biztosítanak megfelelő adatvédelmi ellenőrzést.[36] Az adatvédelmi paradoxon abból a konfliktushelyzetből eredeztethető, hogy egyrészt az emberek félnek, hogy a közzétett személyes adatok miatt megfigyelés alatt állnak és ezáltal sebezhetővé válnak, másrészt – ennek ellentmondásképp – a közösségi oldalakon megvalósuló tényleges közzétételi cselekvésükből adódik.[37]

---

[32] Crosssec Solutions: *Az adatvédelmi tudatosság erősödik*. 2018.04.18. – blog.crosssec.com/az-adatvedelmi-tudatossag-erosodik [2020. 01. 15.]

[33] FLOOD, ALISON: *Finland ranked world's most literate nation*. The Guardian 2016.03.11. – www.theguardian.com/books/2016/mar/11/finland-ranked-worlds-most-literate-nation [2020. 01. 10.]

[34] MINISTRY OF EDUCATION AND CULTURE: *New national policy for media literacy published*. 2019.12.16. – minedu.fi/artikkeli/-/asset_publisher/uudet-suuntaviivat-medialukutaidolle-julkistettu?_101_INSTANCE_vnXMrwrx9pG9_ languageId=en_US [2020.01.11.]. EPALE: *Finnországban megjelent a médiaműveltségre irányuló új nemzeti szakpolitika*. 2020.01.06. – epale.ec.europa.eu/hu/content/ finnorszagban-megjelent-mediamuveltsegre-iranyulo-uj-nemzeti-szakpolitika [2020.01.11.]

[35] BARNES, SUSAN B.: *A privacy paradox: Social networking in the United States*, First Monday Vol. 11. No. 9. (2006) – journals.uic.edu/ojs/index.php/fm/article/view/1394/1312 [2020. 01. 05.]

[36] BLANK GRANT – BOLSOVER GILLIAN – DUBOIS ELIZABETH: *A New Privacy Paradox: Young People and Privacy on Social Network Sites.* University of Oxford - Oxford Internet Institution. Global Cyber Security Centre. 2014. – www.oxfordmartin.ox.ac.uk/downloads/A%20New%20Privacy%20Paradox%20April%202014.pdf [2019. 11. 29.] 3. p.

[37] ACQUISTI, ALESSANDRO – GROSS, RALPH: *Imagined communities: awareness, information sharing, and privacy on The Facebook*. In: DANEZIS, G. – GOLLE, P. (eds.): *Proceedings of the 6th Workshop on Privacy Enhancing Technologies (PET'06)*, *LNCS*, Vol. 4258. Springer, Heidelberg, 2006. 40. p. DIENLIN, TOBIAS – TREPTE, SABINE: *Putting the social (psychology) into social media. Is the privacy paradox a relic of the*

2. A hozzájárulás és az ingyenesség szerepe az adatvédelmi tudatosság kérdéskörében

2. 1. Az egyén részéről történő kifejezett hozzájárulás jelentősége

Az adatkezeléséhez való hozzájárulás valószínűleg az egyik legfontosabb mechanizmusnak tekinthető, amely jelenleg létezik annak meghatározására, hogyan és mikor lehetséges a személyes adatokat kezelni, továbbá felhasználni.[38] *Determann* 2012-es tanulmányában a közösségi média adatvédelmi kontextusát illetően fejti ki véleményét.[39] A digitális korban már nem a legaktuálisabb cikknek számít, – figyelembe véve azt, hogy azóta a Facebook havi aktivitású felhasználóinak száma közel másfélszeresére nőtt[40] – ennek ellenére olyan megállapításokat tartalmaz az attitűd vonatkozásában, amely jelen kutatás eredményeinek fényében is helytállónak bizonyul. Adatvédelmi szempontból az érintett hozzájárulásának azért is van kiemelt szerepe, mert a személyes adatok adatkezelésének jogszerűségét alapozza meg.[41] A legtöbb felhasználó a virtuális térben mindösszesen egy gyors kattintással hozzájárul a személyes adatainak kezeléséhez, anélkül, hogy az adatkezelési tájékoztatóban és szabályzatban foglaltakat elolvasta, valamint megértette volna.[42]

Emellett a felhasználók döntő többsége különösebb aggály nélkül átadja személyes adatai kezelésének lehetőségét a közösségi oldalak szolgáltatóinak, a személyre szabott, kitűnő minőségű szolgáltatásért cserébe. Ez a jelenség alapjaiban kérdőjelezi meg a privát szféra védelmének jövőjét, valamint főbb elveinek gyakorlati fenntarthatóságát.[43] Ezzel összefüggésben a kutatásban több kérdés is annak feltérképezésére irányult, hogy a joghallgatók e tekintetben mennyire körültekintően járnak el.

2. 2. Az ingyenesség mint külön vizsgálandó szempont

A Facebook üzleti modellje alapvetően arra épül, hogy a felhasználók minél több személyes adatot, tartalmat osszanak meg, valamint minél intenzívebb interakciót folytassanak egymással. Ahhoz, hogy ez hatékonyan érvényre jusson elengedhetetlen a bizalom megléte, amelyet a szolgáltatás manipulatív módon igyekszik kialakítani a

past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology. Vol. 45. (2015) 290. p. SIDERI et al. 2019, 335. p.

[38] LUBIS, MUHARMAN – KARTIWI, MIRA – ZULHUDA, SONNY: *Privacy and Personal Data Protection in Electronic Voting: Factors and Measures*. TELKOMNIKA. Vol. 15. No. 1. 2017. 515. p. WHITLEY, EDGAR A.: *Informational Privacy, Consent and the „Control" of Personal Data.* Information Security Technical Report Vol. 14. No. 3. (2009) 150. p.

[39] DETERMANN, LOTHAR: *Social Media Privacy: A Dozen Myths and Facts. Stanford Technology Law Review* 7. 2012. – papers.ssrn.com/sol3/papers.cfm?abstract_id=2298891 [2019. 11. 23.] 2. p.

[40] STATISTA: Number of monthly active Facebook users worldwide as of 3rd quarter 2019 – www.statista.com/ statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [2020.01.04.]

[41] GDPR 6. cikk (1) bekezdés a) pont

[42] DETERMANN 2012, 2. p.

[43] The Future of Privacy. Pew Research Center. 2014. – assets.pewresearch.org/wp-content/uploads/sites/14/2014/12/PI_FutureofPrivacy_1218141.pdf [2019. 12. 07.]. In: KOLTAY ANDRÁS: *A social media platformok jogi státusa a szólásszabadság nézőpontjából*. Medias Res 2019/1. – real.mtak.hu/95749/1/imr-2019-01-01.pdf [2019. 11. 02.] 25–26. pp.

felhasználókban.[44] A hirdetőknek nyomon követési információkra van szükségük a célzott hirdetésekhez, valamint a „közösségi médiát szolgáltató társaságoknak" a hirdetők finanszírozása szükséges ahhoz, hogy ingyenes szolgáltatásokat kínálhassanak a fogyasztók számára.[45] A legtöbb fogyasztó ismeri azt a kompromisszumot és tényt, hogy a személyes adataival és a hirdetések elviselésének hajlandóságával fizetnek a szolgáltatásokért.[46]

A szakirodalom áttekintése körében elkülönült gondolatot képzett, hogy az emberek jobban törődnek azzal, hogy ingyenesen jussanak a közösségi médiához, mint az adatvédelemmel.[47] Ezzel összefüggésben kérdésként merült fel, hogy vajon a joghallgatók számára a közösségi oldalak „ingyenes" igénybevétele mennyire minősül meghatározó szempontnak. Előrevetítve is kijelenthető, hogy kulcsfontosságú tényezőként hat a hallgatókra. Az ingyenességhez fűződő attitűd vizsgálatának jelentőségét erősíti, hogy a *Gazdasági Versenyhivatal* VJ/85/2016 ügyszámú döntésében megállapította, hogy a Facebook Ireland Ltd. jogsértést követett el, amikor ingyenesként hirdette szolgáltatását, mivel *„a fogyasztóknak ugyan valóban nem kellett díjat fizetniük a szolgáltatás igénybevételéért, de felhasználói aktivitásukkal és adataikkal üzleti hasznot hajtottak a vállalkozásnak és így fizettek a szolgáltatásért."*[48] Ezen döntés azért is bír kiemelt gyakorlati relevanciával az adatvédelmi műveltség kérdéskörét illetően, mivel egyrészt megjelenik a tudás „tudatában lenni annak, hogy a személyes adatok szolgáltatása *quasi* fizetési módot képez", valamint a megszerzett ismeretek lévén körültekintően történik-e a személyes adatok megosztása.

3. A közösségi oldalak használata

A közösségi oldalak számának növekedésével a felhasználók által megosztott személyes adatok mennyisége is folyamatosan nőtt.[49] Megemlítendő, hogy a legtöbb adatvédelmi fenyegetés abból származik, hogy az emberek miként használják ezeket a felületeket, mely személyes adataikat adják meg.[50] A közösségi oldalak működésének megfelelően a felhasználók profilokat hoznak létre, amelyekben az általuk választott módon ábrázolják „digitális személyiségüket" és személyes információkat osztanak meg más felhasználókkal. Ugyanakkor aggodalomra ad okot a magánéletük és személyes adataik biztonsága, mivel önkéntesen bocsátják rendelkezésre ezeket az adatokat, vagy meggondolat-

[44] WALDMAN, ARI EZRA: *Manipulating Trust on Facebook*. Loyola Consumer Law Review Vol. 29. (2016) 175. p. In: Koltay 2019, 6. p.
[45] DETERMANN 2012, 7. p.
[46] UO.
[47] DETERMANN 2012, 14. p. (April Dembosky, idézve Rebecca Liebet, az Altimeter Csoport elemzőjét.)
[48] GAZDASÁGI VERSENYHIVATAL: *1,2 milliárd Ft bírságot szabott ki a Gazdasági Versenyhivatal a Facebook-ra,* Budapest, 2019.12.06. – www.gvh.hu/sajtoszoba/sajtokozlemenyek/2019_es_sajtokozlemenyek/12-milliard-ft-birsagot-szabott-ki-a-gazdasagi-versenyhivatal-a-facebook-ra [2019.12.08.]
[49] WISSINGER, CHRISTINA L. – WILSON, B. GAIL: *Student perceptions of Facebook's privacy policies & rights*. Social Media Studies 2(1) (2015) 18. p.
[50] DETERMANN 2012, 7. p.

lanul járulnak hozzá azok gyűjtéséhez, figyelmen kívül hagyva azt a tényt, hogy a személyes adatok feletti irányítás jelenleg nem áll a rendelkezésükre.[51]

Kérdésként merülhet fel, hogy mit is jelent a közösségi média, hogyan definiálható. *Kaplan* és *Haenlein*[52] a közösségi médiát a Web 2.0-ra, mint technikai felületre épülő internet-alapú alkalmazások „gyűjteményeként" definiálja.[53] *Cohen*[54] stratégiaként azonosítja a közösségi médiát.[55] *Nair* szerint a közösségi média olyan eszközöket foglal magában, amelyek főbb elemei a tartalom-, a vélemények és nézetek megosztása, a média külön egységként értelmezhető, valamint kapcsolat a felhasználók és a vállalatok között.[56] Tekintettel arra, hogy a közösségi média számos alterületet felölel, jelen kutatás kizárólag a közösségi oldalakra fókuszál, nevezetesen elsődlegesen a Facebook, az Instagram, valamint a LinkedIn felületére.

4. Az adatvédelmi tudatosság vizsgálatával összefüggő nemzetközi kutatások

A közösségi oldalak használatának kontextusában az adatvédelem napjainkban megmutatkozó kihívásaival, valamint az adatvédelmi tudatosság témakörében számos tanulmány és elemzés jelent meg. Mindezek közül a terjedelmi korlátokra tekintettel jelen dolgozat mindösszesen az adatvédelmi tudatosság vizsgálatára vonatkozó kutatásokba nyújt bepillantást.

Mind relevanciáját, mind aktualitását tekintve kiemelkedő jelentőséggel bír *Sideri et al.* esettanulmánya[57], amely az egyetemi hallgatók közösségi média használatával összefüggő adatvédelmi tudatosságát hivatott felmérni. Ennek érdekében egy közösségi médiával kapcsolatos tizenhárom hétig tartó kurzus indítására is sor került 54 hallgató részvételével, közülük pedig 23 hallgató önkéntesen a kísérleti jellegű kutatásban is szerepet vállalt. A kurzus során a hallgatók képessé váltak arra, hogy a nem kívánt közönségtől elzárják a profiljukat, vagyis, hogy korlátozzák a láthatóságot. Az adatvédelmi tudatosság megerősítésének célja az oktatási intervenció által teljesült. Bár a hallgatók megerősítették, hogy felelősséggel tartoznak saját maguk és mások védelméért a Facebook felületén, a kutatás eredményei rávilágítottak arra, hogy nem rendelkeznek az ehhez szükséges ismeretekkel. Összességében a kurzus befejeztével jelentős számú

---

[51] CONGER, SUE – PRATT, JOANNE H. – LOCH, D. KAREN: *Personal information privacy and emerging technologies*. Information Systems Journal Vol. 23. No. 5. (2013) 410. p.

[52] KAPLAN, ANDREAS M. – HAENLEIN, MICHAEL: *Users of the World, Unite! The Challanges and Opportunities of Social Media.* Business Horisons Vol. 53. (2010) 60. p.

[53] MARKOS-KUJBUS ÉVA – GÁTI MIRKÓ: *A közösségi média mint online stratégiai eszköz*. In: piskóti István (szerk.): *„Coopetition". Verseny és együttműködés a marketingben*. Magyar Marketing Szövetség Marketing Oktatók Klubja 18. Országos Konferencia. 2012. augusztus 30-31. Miskolc. Miskolci Egyetem Marketing Intézet. Online marketing szekció. 8. sz. tanulmány. 2012. – unipub.lib.uni-corvinus.hu/886/1/MKE_GM_mok2012.pdf [2019. 10. 17.] 3. p.

[54] COHEN, LON S: *Is there a Difference between Social Media and Social Networking?* The Cohenside (2009) –cohenside.blogspot.com/2009/03/is-there-difference-between-social.html [2019. 11. 09.]

[55] KARDOS VIVIEN KATA: Jogi informatikai trendek vs. hallgatói valóság*. Acta Universitatis Szegediensis. FORVM. Publicationes Discipulorum Iurisprudentiae* 2019/1. 175. p.

[56] NAIR, MOHAN: *Understanding and Measuring the Value of Social Media. The Journal of Corporate Accounting & Finance* 22 (3). (2011) 45–51. pp.

[57] SIDERI et al. 2019, 342. p.

hallgató szigorúbban kezelte a profilja láthatóságát, továbbá a Facebook adatvédelmi beállításaira is nagyobb figyelmet fordítottak, a kémprogram-ellenes szoftverek hasznosságával szembeni bizonytalanságuk is csökkent.[58] Ez a kutatás is alátámasztja, hogy az adatvédelmi tudatosság fejlesztésében az oktatás milyen jelentős szerepet tölt be.

Kezer et al. tanulmányában az amerikai felnőttek Facebook felületén tanúsított adatvédelmi viselkedését vizsgálta. Az életciklus-elmélet alapján a fiatal felnőttek (18–40 év), a középkorú felnőttek (40–65 év), valamint az „érett felnőttek" (65 év felett) korcsoportját hasonlítja össze az adatvédelmi ismereteikkel, adatvédelmi aggályaikkal és attitűdjeikkel kapcsolatban, továbbá, hogy mindezen tényezők milyen hatást gyakorolnak a Facebook felületén a „önismertetés", valamint a magánélet védelmét szolgáló viselkedésüket illetően.[59]

A kutatás eredményei tükrében nem mutatkozott jelentős különbség a korosztályok között azzal a meggyőződéssel kapcsolatban, hogy az adatvédelem jogként érvényesül, valamint aggódnak saját személyes adataik védelméért. Ezzel ellentétben abban már különbözött a véleményük, hogy a saját adatvédelmük attól függ-e, hogy a körülöttük lévő emberek milyen mértékben figyelnek oda a saját személyes adataik védelmére. A fiatal felnőttek esetében kevésbé valószínű, hogy értékelik mások személyes adatainak védelmét.[60] Előrevetítve ezen megállapítás jelen kutatással is összhangban áll. Megjegyzendő, hogy a korosztályok között általánosságban véve az online adatvédelmi műveltség tekintetében nem volt szignifikáns különbség.[61]

Lewis et al. közös tanulmányukban[62] egy északkeleti amerikai magánegyetem 1 710 hallgatójának Facebook profilját, valamint közösségi hálóját vizsgálták kétéves időtartamban az adatvédelmi beállításaikkal összefüggésben. A megállapításaik között szerepel, hogy azok a hallgatók, akik privát Facebook profillal rendelkeztek, „aktívabb jelenlétet" tanúsítottak.[63]

Lawler és *Molluzzo* tanulmányában[64] 200 elsőéves hallgató adatvédelmi hozzáállását vizsgálta a közösségi háló kontextusában. A lakosság nagy része nincs tudatában a megfelelő adatvédelmi gyakorlatnak a közösségi oldalak világában.[65] Az eredmények alapján megállapítást nyert, hogy a válaszadók 61,5%-a nem olvasta el az adatkezelési szabályzatot, amely a jelen kutatási eredményekhez viszonyítva jelentősen pozitívabban értékelhető.[66] Az adatvédelmi tárgyú oktatás szükségességét szintén a figyelem középpontjába állította a tanulmány, tekintettel arra, hogy a vizsgálat alá vont személyi kör sok esetben nem tudta, hogy a személyes adataik kezelése hogyan valósul meg.[67]

---

[58] SIDERI et al. 2019, 353. p.
[59] KEZER et al. 2016, 1. p.
[60] KEZER et al. 2016, 7. p.
[61] KEZER et al. 2016, 9. p.
[62] LEWIS, KEVIN – KAUFMAN, JASON – CHRISTAKIS, NICHOLAS: *The taste for privacy: An analysis of college student privacy settings in an online social network.* Journal of Computer-Mediated Communication Vol. 14. No. 1. (2008) 81. p.
[63] LEWIS et al. 2008, 94. p.
[64] LAWLER, P. JAMES – MOLLUZZO, C. John: *A survey of first-year college student perceptions of privacy in social networking.* Journal of Computing in Colleges Vol. 26. No. 3. (2011) 36–41. pp.
[65] LAWLER – MOLLUZZO 2011, 40. p.
[66] LAWLER – MOLLUZZO 2011, 39. p.
[67] Uo.

III. Empirikus kutatás

1. Kutatásmódszertan

A dolgozat alapját képező empirikus kutatás eredményei elsődleges forráson alapul. A kvantitatív kutatás elsősorban annak feltérképezésére irányult, hogy a joghallgatók hogyan viszonyulnak az adatvédelemhez a közösségi oldalak használata során, valamint ezzel összefüggésben az attitűdjük és szokásaik mennyire tükrözik a tudatos cselekvést. Kulcsfontosságú szerepet töltött be, hogy a specializált személyi körön belül minél sokrétűbb közösség bevonására kerüljön sor, elősegítve a minél átfogóbb és sokrétűbb következtetések levonását. A válaszokkal összefüggésben hangsúlyozandó, hogy válaszadási hibák következhetnek be, amelyek a kérdőív kitöltők szándékos vagy önhibáján kívüli, nem valóságnak megfelelő válaszaiból fakad.[68]

2. Kérdőíves felmérés

Az önkéntes kitöltéssel megvalósuló kérdőíves felmérésre online felületen került sor, amelyben valamennyi magyarországi állam- és jogtudományi kar „képviseletében" összesen 205 joghallgató vett részt. A válaszadók 63%-a nő, míg 37%-a férfi, az átlagéletkor 24,5 év, a medián pedig 23 év. Az adatfelvétel 2019. december 28. és 2020. január 8. között valósult meg. Az adatfelvételi időkorlát viszonylag szűk meghatározásának célja az időbeli torzulások miatt esetlegesen fellépő adatminőség romlásának elkerülése[69] és a válaszadói hajlandóság növelése volt.

2.1. A résztvevői kör

A mintavétel speciális alanyi körre, mégpedig kizárólagosan a joghallgatókra korlátozódott, tekintettel arra, hogy a kutatás fókuszpontjában a joghallgatók adatvédelmi tudatosságának vizsgálata áll. A válaszadói kör meghatározásában döntő szereppel bírt a joghallgatói minőség, mivel – vélelmezhetően – a joghallgatók saját tapasztalataikon túlmenően a tanulmányaik során is az adatvédelem különböző aspektusaival találkozhattak, amely a tudásbázisuk gyarapítására pozitív hatást gyakorolhatott. Figyelembe véve, hogy a jelenleg még az egyetemek padsoraiban ülő joghallgatók a közeljövőben már a leendő jogásztársadalom szerves tagjaivá válnak, ezáltal elvárásként szembesülhetnek azzal, hogy az adatvédelemnek nemcsak a magánszférájukat illetően, hanem a mindennapi munkájuk végzése során is kiemelt jelentőség tulajdonítható.

---

[68] KATONA TAMÁS – KOVÁCS PÉTER – PETRES TIBOR: *Általános statisztika.* Negyedik, átdolgozott és kibővített kiadás. Pólay Elemér Alapítvány, Szeged, 2011. 144. p.

[69] GYULAVÁRI TAMÁS – MITEV ARIEL ZOLTÁN – NEULINGER ÁGNES – NEUMANN-BÓDI EDIT – SIMON JUDIT – SZŰCS KRISZTIÁN: *A marketingkutatás alapjai*. Akadémiai Kiadó, Budapest, 2014. 310. p. SIMAY ATTILA ENDRE – GÁTI MIRKÓ: *Nyilvánosság és magánélet a mobiltelefon és a közösségi média használat tükrében.* Egyesült a Marketing Oktatásáért és Kutatásáért XXI. országos konferencia cikk. Budapest, 2015. augusztus 27-28. – unipub.lib.uni-corvinus.hu/2046/ [2019.12.14.] 5. p.

A jövőbeni kilátások feltérképezéséhez kapcsolódóan fontos annak felmérése, hogy a „ma joghallgatója" milyen adatvédelmi tudatossággal rendelkezik, milyen ismeretek birtokában áll. Megjegyzendő, hogy az attitűd és a szokások vizsgálatának kérdésköre azért bír kardinális szerepkörrel, mert a jövőbeni kihívásokhoz való alkalmazkodás tekintetében döntő szerepet játszik. Annak érdekében, hogy minél szélesebb spektrumon történő vizsgálat valósuljon meg, a fókuszcsoport egyaránt magában foglalja az egyetemek padjaiban éppen csak helyet foglaló, valamint az abszolutórium kapujában álló joghallgatókat is, összegezve valamennyi évfolyam bevonásra került. A nappali tagozatos hallgatók általi kitöltés az elsődleges, mindazonáltal levelező tagozatos válaszadók is részvételükkel támogatták a kutatás sokrétűségét, tekintettel arra, hogy egyes kérdések vonatkozásában esetlegesen a generációkülönbségek adta differenciák is felszínre bukkanhatnak.

2.2. A kérdőív kérdései

A kvantitatív felmérés alapjául szolgáló kérdőív struktúráját tekintve egyaránt tartalmazott általános adatvédelmi, valamint a közösségi oldalak használatára vonatkozó kérdéskört, amely elsődlegesen a személyes adatok megosztásával, hozzáférhetőségével áll kapcsolatban. A kérdések megalkotásában orientációs pontként szolgált, hogy a tudás, az attitűd, valamint a szokások mérésére is alkalmazható legyen. Az adatvédelmi tudatosság széleskörű felmérésének biztosítása érdekében gyakorlati jellegű kérdések is helyet kaptak. A kérdések között egyszeres és többszörös válaszadásra is vonatkozott kérdés, továbbá egytől tízig terjedő skálán történő meghatározás is hangsúlyos szerepet kapott direkt és indirekt kérdések formájában. A joghallgatói vélemény széleskörű megnyilvánulása érdekében nyílt kérdések megfogalmazására is sor került.

IV. A kutatás eredményei

1. A közösségi oldalak használatával összefüggő kérdések

Jelen kutatás keretében a közösségi oldalak gyűjtőfogalma alatt a Facebook, az Instagram, valamint a LinkedIn értendő. A kérdőíves felmérés alapján a joghallgatók 94,63%-a napi szintű gyakorisággal használja a Facebook[70] felületét, mindösszesen egy válasz érkezett arra vonatkozóan, aki egyáltalán nem használja e közösségi oldalt. Az Instagram esetében ezen számok jelentősen másképp alakulnak, – figyelembe véve, hogy elsődlegesen képmegosztási szereppel bír – a válaszadók 67,8%-a naponta veszi igénybe e felület szolgáltatásait, ugyanakkor a válaszadók egyötöde egyáltalán nem használja. A LinkedIn, amely alapvetően szakmai és üzleti közösségi oldalként ismert, hallgatói szempontból az állás-, valamint gyakorlati hely-keresés folyamatában nyújthat segítséget a számos cikk és bejegyzés elérhetőségén túl. A válaszok alapján ennek elle-

[70] A Facebook megnevezés magában foglalja a Messengert mint elsődlegesen üzenetküldésre hivatott kommunikációs csatornát.

nére egyáltalán nem tekinthető elterjedtnek. A számok oldaláról megvilágítva, az előzőekben ismertetett magas gyakorisági aránnyal szemben, a kitöltők 19,51%-a használja valamilyen gyakorisággal, a naponta válaszlehetőséget pedig mindösszesen hárman jelölték. A LinkedIn jelenlét a hallgatók több mint háromnegyede (76,59%) esetében egyáltalán nem jelenik meg. Mindezek alapján megállapítható, hogy kizárólag szűkkörben alkalmazott.

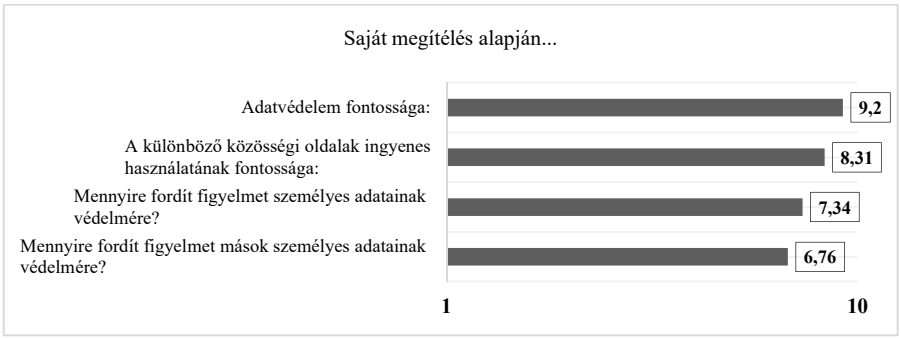
A válaszok alapján láthatóvá vált, hogy a közösségi oldalak használata elsődlegesen a Facebook aktivitásra korlátozódik. Mindemellett fontos megjegyezni az Instagram magas arányát. Mindazonáltal az aktív LinkedIn használat rendkívül csekély, amely a jövő vonatkozásában akár még lépéshátránnyal is szolgálhat, mivel a szakmai közösség építését „nem lehet elég korán elkezdeni", ezenfelül számos jogi területhez kötődő álláshoz hozzátartozik az aktív LinkedIn használat. Nemzetközi szinten ez oly mértékben számottevő, hogy e témakört illetően külön útmutató is rendelkezésre áll a megfelelő jelenlét biztosítása érdekében, kifejezetten jogászokra, valamint ügyvédi irodákra specializálva.[71]

2. Saját megítélésen alapuló általános jellegű adatvédelmi kérdések

A kérdőív elején a joghallgatók saját megítélését tükröző általános adatvédelmi kérdések kaphat helyet. Ennek megfelelően egytől tízig terjedő skálán annak meghatározása volt a feladat, hogy mennyire tartják fontosnak az adatvédelmet, valamint a különböző közösségi oldalak ingyenes használatát. Ezenfelül mennyire fordítanak figyelmet személyes adataik, valamint mások személyes adatainak védelmére. Az alábbi ábra e kérdések vonatkozásában a joghallgatói válaszok átlagát hivatott szemléltetni.

1. sz. ábra

A joghallgatók saját megítélése általános jellegű adatvédelmi kérdésekkel összefüggésben



Forrás: A kutatás alapjául szolgáló adatok (n=205; saját szerkesztés)

[71] CHEUNG, LINDA: *The Guide: Social media for lawyers* – CubeSocial (cubesocial.com/social-media-for-law-firms/ – [2019. 11. 19.]. CubeSocial – LinkedIn for lawyers: *How to get leads ans instructions from LinkedIn* – cubesocial.com/linkedin-for-lawyers/ [2019. 11. 19.]

A válaszok alapján megállapítható, hogy a joghallgatók nagyon fontosnak tartják az adatvédelmet, hiszen a válaszadók 61,46%-a a tízes pontot jelölte válaszként, az átlag tekintetében pedig 9,20 pontos eredmény született. Megjegyzendő, hogy hármasnál alacsonyabb „osztályzat" egyáltalán nem került megjelölésre, mindösszesen egy-egy hallgató értékelte hármas és négyes pontra. Meglepő módon a második legmagasabb értéket az ingyenes használat fontossága érte el. Mindösszesen négy hallgató válaszolt akként, hogy ezen szempont egyáltalán nem bír relevanciával, nem tölt be fontos szerepet. Ezzel szemben a hallgatók 39,51%-a a skála legmagasabb értékét választotta ki, továbbá az átlag eredménye is bőven 8 pont feletti.

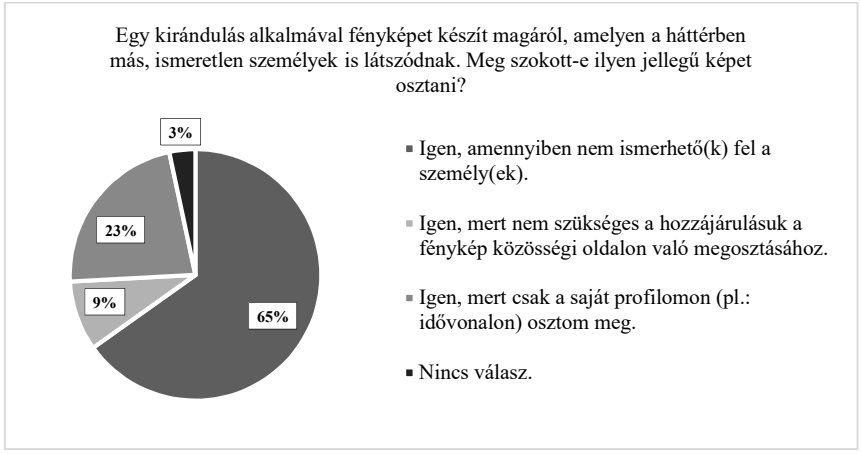
A kutatás eredményei rávilágítottak arra, hogy az ingyenes használat magasabb értékkel bír, mint a saját személyes adataikra való figyelem fordítása, hiszen általánosságban véve a skálán közel egy teljes értékkel alacsonyabb számot ért el. A számok alapján is jól látható, hogy a válaszadók jelentősen kevesebb figyelmet fordítanak más természetes személyek személyes adataira, olyannyira, hogy a joghallgatók több, mint negyede (25,85%) ötös vagy annál alacsonyabb értéket jelölt meg a válaszadás során.

3. Más természetes személyek személyes adatainak védelme

A hipotézisek között szerepelt, hogy a hallgatók saját személyes adataikra lényegesen nagyobb figyelmet fordítanak, mint más természetes személyekére. A válaszok alapján ez alátámasztást nyert, ugyanakkor kérdésként merül fel, hogy az ismerethiány, vagy egy bizonyosfajta hanyagság miatt valósul-e meg, esetleg más okra vezethető vissza. Az alábbi ábra a képmegosztási szokásokkal összefüggésben gyakorlati példa alapján mutatja be, hogy a vélt tudás is indokként szerepel.

2. sz. ábra

Fényképmegosztási arány a háttérben látszódó ismeretlen személyek esetében



Forrás: A kutatás alapjául szolgáló adatok (n=205; saját szerkesztés)

A joghallgatók döntő többsége – 174 válaszadó – egyáltalán nem szokott kirándulás során olyan jellegű képet megosztani, amelynek hátterében más személyek is azonosítható módon láthatók, vagy figyelmet fordít arra, hogy mások jogai ne csorbuljanak azáltal, hogy a hozzájárulásuk nélkül történik a fényképfelvételek megosztása. A vélt tudás jelenik meg a joghallgatók 14%-a esetében, hiszen nyolc hallgató úgy gondolja, hogy egyáltalán nincs szükség a hozzájárulásra, míg 20 hallgató esetében annak van jelentősége, hogy mindösszesen a saját profilján teszi közzé. Adatvédelmi szempontból ez valójában irreleváns tényező, a hozzájárulás szükséges.[72]

Annak ellenére, hogy a kisebbséget testesítik meg azon válaszadók, akik úgy vélik, hogy a megfelelő tudás birtokában állnak, összességében felhívják a figyelmet arra, hogy az ismeretek hiánya is közrehat abban, hogy más személyek személyes adataira kevesebb figyelem jut. E kérdéskör kapcsán életszerű példával összefüggésben a közös szórakozás alkalmával készült fényképet tizennégy joghallgató (6,83%) a barátai megkérdezése nélkül megosztja a közösségi oldalon. Jogosan felmerülhet indokként a baráti kötelék, mindazonáltal hangsúlyozandó, hogy ez esetben is a hozzájárulás primátusának szükséges érvényesülnie.

4. Mi minősül személyes adatnak?

A személyes adat fogalma rendkívül tág körben került meghatározásra. Az általános adatvédelmi rendelet 4. cikk 1. pontjában meghatározott definíció alapján a személyes adat az azonosított vagy azonosítható természetes személyre [érintett] vonatkozó bármely információ. Az a természetes személy azonosítható, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható. Ebből kifolyólag nemcsak az érintettel kapcsolatba hozható adat, hanem az adatból levonható, az érintettre vonatkozó következtetés is értendő alatta.[73]

Ahhoz, hogy az adatvédelem ténylegesen megvalósulhasson az adatalanyok részéről elengedhetetlen, hogy e fogalom ismerete a gyakorlatban is implementálásra kerüljön, vagyis, hogy az adatalanyok képesek legyen distinkciót tenni személyes adat, valamint nem személyes adat között. Az adatvédelmi tudatosság alappillérét képezi a személyes adat megfelelő azonosításának ismerete. A kérdőívben ez gyakorlatorientált kérdésként merült fel, hiszen a hétköznapokban is ilyen módon szükséges felismerni. A joghallgatóknak kilenc eltérő példa esetében kellett döntést hozniuk, hogy az adott információ személyes adatnak minősül-e.[74] Annak érdekében, hogy a tippelés aránya, és ezáltal az adatok torzító hatása csökkenthető legyen, a „nem tudom” is önálló válaszlehetőséget

[72] GDPR (32) bekezdés.

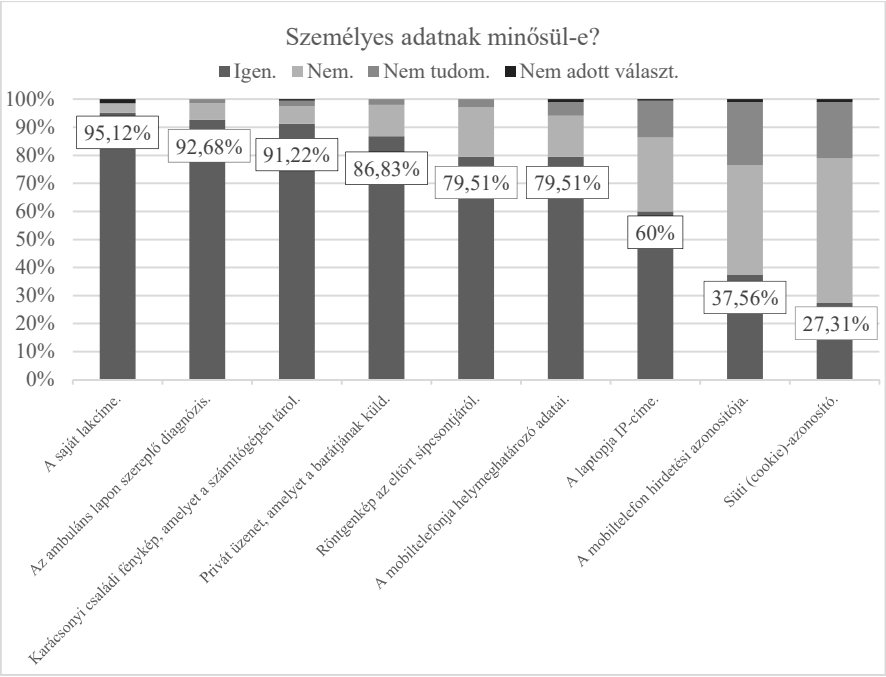
[73] NAIH: Adatvédelmi értelmező szótár – www.naih.hu/adatvedelmi-szotar.html [2019. 11. 23.]

[74] A kérdőívben szereplő példák meghatározásában segítségül szolgált: Európai Bizottság: *Mit nevezetünk személyes adatnak?* Példák személyes adatra. – ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hu [2019. 11. 24.]

képezett. A kutatás eredményeit az egyes személyes adatok vonatkozásában az alábbi ábra foglalja össze.

3. sz. ábra

A személyes adat gyakorlati példákon keresztül történő azonosítása



Forrás: A kutatás alapjául szolgáló adatok (n=205; saját szerkesztés)

Annak ellenére, hogy valamennyi meghatározás személyes adatnak minősül, mindösszesen 23 joghallgató (11,22%) válaszolt helyesen valamennyi esetben, ez meglehetősen csekélynek tekinthető. A válaszlehetőségek megoszlási arányait illetően jól látható, hogy meglehetősen nagyszámú téves válasz érkezett. Ebből következően megállapítható, hogy a hipotézisnek megfelelően alátámasztást nyert, hogy a gyakorlati példákon keresztül a személyes adatok minőségének megítélése nehézséget okoz, mivel nagymértékű az ismerethiány, valamint a helytelen válaszok száma. Csupán három esetben haladta meg a 90%-ot a helyes válaszok aránya. A szó hétköznapi értelmében is személyes adatnak minősülő információk, mint például a saját lakcím és a családi fénykép esetében a meghatározás egyszerűbbnek bizonyult. Hangsúlyozandó, hogy két esetben a helytelen válaszok száma a helyes válaszok számát is meghaladta, amely szintén vélt tudás feltételez.

A „süti" (cookie)-azonosítót a joghallgatóknak mindösszesen alig több, mint negyede (27,31%) minősítette személyes adatként. Ennek jelentősége azzal függ össze, hogy egy másik kérdés kapcsán, amely a „süti" jelentésének meghatározására irányult, hat válaszlehetőség közül a válaszadók 87,32%-a jelölte meg a helyes választ. Mindezek alapján általánosságban megállapítható, hogy a joghallgatók a jelentéstartalom tekintetében az ismeretek birtokában állnak, mindazonáltal a jogi természetét illetően jelentős hiányosságok mutatkoznak. E fogalom elméleti tudása, valamint a gyakorlatba történő implementálása elválik egymástól. A mobiltelefon helymeghatározó adatai és a mobiltelefon hirdetési azonosítója – azonos jogi természete ellenére – a hallgatói válaszok tükrében teljesen más megítélés alá esett. Szignifikáns eltérés tapasztalható, tekintettel arra, hogy a mobiltelefon hirdetési azonosítóját 77-en, ezzel szemben a mobiltelefon helymeghatározó adatait – több mint kétszerannyian – 163-an minősítették személyes adatnak. A példák között különleges személyes adatok, mégpedig egészségügyi adatok is helyet kaptak.[75]

A válaszok alapján nagymértékű – több mint 13%-os – különbségtétel figyelhető meg a röntgenkép és az ambulánslapon szereplő diagnózis jogi természetének meghatározásában, annak ellenére, hogy azonos megítélés alá tartoznak. A „nem tudom" válaszopciót a legmagasabb arányban a mobiltelefon hirdetési azonosítója (22,44%) és a „süti" (cookie)-azonosító (20%) esetében választották. A mobiltelefon hirdetési azonosítójával összefüggő eredmény kapcsán közrejátszó tényezőként jelenhetett meg, hogy a válaszadók nem ismerték ezt a fogalmat, nem tudták annak jelentését. A hirdetési azonosító definíciója alatt alapvetően a hirdetéshez biztosított egyedi és a felhasználó által visszaállítható azonosító értendő, amely egyrészt a felhasználóknak hatékonyabb ellenőrzést, másrészt a fejlesztőknek egy egyszerű, standardizált rendszert biztosít, amellyel az alkalmazásaikból befolyó bevételszerzést folytathatják.[76]

Összességében az utóbbi két személyes adat jogi minőségének meghatározása bizonyult a legnehezebb kérdésnek. A válaszok egészét értékelve a személyes adat tág értelmezése körében a joghallgatók ismereteit illetően jelentős hiányosságok állapíthatók meg. Ezen kutatási eredmény jelentősége abban is áll, hogy az egyik legalapvetőbb fogalom tekintetében mutatható ki a nem megfelelő – hiányos – tudás.

5. A „süti" (cookie)-azonosítóra vonatkozó kérdések

Napjainkban egyre nagyobb figyelmet kap a „sütik" kérdésköre. Reflektálva ezen tendenciára a kérdőívben több pilléren alapulva, széles körben és több szempontból is vizsgálat alá került. Az első kérdés az előzőekben említetteknek megfelelően a „süti" (cookie)-azonosító jelentéstartalmának válaszlehetőségek általi a meghatározására irányult. A válaszadók 87,32%-a válaszolt helyesen, hiszen a „süti" alatt alapvetően olyan rövid adatfájl értendő, amelyet a meglátogatott honlap helyez el a felhasználó számító-

[75] A különleges személyes adat fogalmát a GDPR 9. cikk (1) bekezdése határozza meg. Az egészségügyi adat a GDPR 4. cikk 15. pontjában került definiálásra. Egészségügyi adat: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

[76] Hirdetésazonosító – support.google.com/googleplay/android-developer/answer/6048248?hl=hu [2020. 01. 20.]

gépén azzal a céllal, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye, továbbá a segítségével nyomon követhetőek a felhasználók böngészési szokásai.[77]

Az előzőekben említettekre visszautalva a „süti" (cookie)-azonosító személyes adatként történő megítélése „próbatétel elé állította" a joghallgatókat. Ezzel kapcsolatban megjegyzendő, hogy a konkrét tudás vizsgálatán túlmenően kiemelt jelentőség tulajdonítható annak, amennyiben a hallgató egyértelműen elismeri, hogy nem áll az adott ismeret birtokában, hiszen ebben az esetben kizárható az esetleges tippelés lehetősége. Mindösszesen a joghallgatók 27,31%-a adott helyes választ, amely szerint személyes adatnak tekintendő.[78]

A harmadik kérdés a hallgatói tudásnak, véleménynek, valamint esetlegesen a jogérzéknek engedett teret azáltal, hogy a kérdés a „sütik" adatvédelmi kockázatosságának megítélésére vonatkozott. Hangsúlyozandó, hogy a joghallgatók mindösszesen alig több, mint egynegyede minősítette személyes adatnak, mindazonáltal a joghallgatók több, mint kétharmada (67,31%) adatvédelmi szempontból mégis „kockázatosnak" ítélte meg a „süti" (cookie)-azonosítót. Mindezek alapján megállapítható, hogy annak ellenére, hogy a mindennapok során gyakran találkoznak a felugró „süti-ablakkal", válaszopciók közül döntő többségük a helyes választ is meg tudja határozni, azonban a működésük, jogi természetük megítélése kapcsán jelentős hiányosságok fedezhetők fel.

6. A személyes adatok közösségi oldalakon történő megosztása

Az adatvédelmi tudatosság egyik lényeges elemét képezi, hogy milyen személyes – adott esetben különleges személyes – adat megosztására kerül sor. Ennek feltérképezése érdekében kérdésként szerepelt, hogy a joghallgatók jelenleg mit osztanak meg a közösségi oldalon, illetve mit osztottak meg öt és tíz év távlatában a táblázatban felsorolt személyes adatok és információk közül. Nem képezett külön szempontot a közösségi oldalak differenciálása. Többszörös választás keretében valósult meg a válaszadás. Tekintettel arra, hogy a kérdőív kitöltése önkéntes akaratelhatározáson alapult, így olyan válaszadó is akadt, aki nem minden esetben jelölt választ.

[77] NAIH: Adatvédelmi értelmező szótár – www.naih.hu/adatvedelmi-szotar.html [2019. 12. 16.]

[78] EURÓPAI BIZOTTSÁG: *Mit nevezünk személyes adatnak?* Példák személyes adatra –ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hu [2019.11.24.]

1. sz. táblázat

A személyes adatok közösségi oldalakon történő megosztása

Adat	Jelenleg megosztom, fő	Nem osztom meg, fő
Név	170	2
Profilkép	167	11
Iskola, egyetem	145	15
Feltöltött képek	141	21
Születési hónap, nap	126	17
Születési év	125	21
Lakóhely	77	79
Megosztások (pl.: hír, cikk, videó)	66	85
Szakmai pálya/életút	60	101
Családi kapcsolatok	49	93
Munkahely	49	116
E-mail cím	39	116
Családi állapot	37	113
Tartózkodási hely	32	120
Napi szokások (pl.: kávézás, edzés)	27	123
Telefonszám	9	155
Vallási nézet	9	160
Politikai nézet	4	164
Élő videó	3	161

Forrás: A kutatás alapjául szolgáló adatok (n=205; saját szerkesztés)

A fenti táblázat a kérdőíves felmérésben előre meghatározott személyes adatokat és információkat tartalmazza, szemléltetve a megosztási szokás két végpólusát, nevezetesen, hogy a joghallgatók mely információkat osztják meg jelenleg, valamint melyek azok, amelyeket egyáltalán nem. Az öt és tíz év vonatkozásában az életkor meghatározó jelentőséggel bírt, annak érdekében, hogy a generációk között megmutatkozó esetleges eltérésekre is felhívja a figyelmet. Az előzetes feltevés ellenére a válaszok alapján egyértelmű megállapításokra nem került sor.

A név, valamint a profilkép megosztása a válaszok tükrében a legáltalánosabbnak tekinthető, azonban meglepően magas arányt képvisel az oktatásra vonatkozó információk közzététele. A sorokat áttekintve látható, hogy a tartózkodási hely jelentősen kevesebb joghallgató esetében került megjelölésre, szemben a lakóhellyel, amely több, mint a kétszerese az előző személyes adatnak. Megfigyelhető, hogy a családi kapcsolatok megosztása gyakoribb, mint a családi állapoté. Az e-mail cím, valamint a telefonszám azért került elhelyezésre a felsorolásban, mert lépcsőzetesen a privát szférát illetően

rendkívül szoros összeköttetésben állnak, hiszen napjainkban telefonon keresztül szinte bárki, bármilyen időpontban *quasi* korlátok nélkül elérhető. Természetesen számos beállítás, funkció, applikáció szerepel a palettán, amely a magánszféra védelmét hivatott szolgálni példának okáért az éjszaka leple alatt.

Az adatvédelmi incidensek[79] között is nem egy esetben meghatározásra került a felhasználói fiókba történő jogszerűtlen belépés, valamint a telefonos úton történő megkeresés, annak ellenére, hogy a telefonszám nem volt nyilvános, és a hallgató sem járult hozzá az effajta megkereséshez. Az előzetes feltevést alátámasztva, amely a telefonszám kiemelt szerepének tulajdonított jelentőséget, a számadatokból nyilvánvalóvá vált, hogy a magánszféra olyan „védőbástyájaként" tekintenek rá a joghallgatók, amelyre ténylegesen figyelmet fordítanak. A vizsgált csoport körében kifejezetten ritka – a különleges személyes adatok közül – a vallási és politikai nézet közösségi oldalakon keresztül történő megosztása.

7. A Nemzeti Adatvédelmi és Információszabadság Hatósággal kapcsolatos kérdések

Az adatvédelmi ismeretek vizsgálatával összefüggésben a NAIH mint autonóm államigazgatási szerv[80] is szerepet kapott, amely legfőbb jogszabályi kereteit az Info. törvény rögzíti. A szervezetrendszer ismerete szintén szükséges az adatvédelmi műveltséghez, hiszen az aktív cselekedettel áll összhangban például egy adatvédelmi incidens bejelentése kapcsán.

A joghallgatók először azzal a kérdéssel találkozhattak, hogy mit is jelent a NAIH. A választ elsődlegesen úgy értelmezték, hogy mit jelent a rövidítés. Már önmagában véve ez is információt szolgáltat arra vonatkozóan, hogy miként történik a kérdés értelmezése. Összességében a joghallgatók kétharmada (65,85%) adott helyes választ nyílt kérdés keretében, azonban a hallgatók 13,66%-a válaszként a „nem tudom" lehetőség mellett döntött. Számos hibás válasz érkezett, például a hivatali jelző feltüntetése hatóság helyett, vagy adott esetben az „információszabadság" helytelen meghatározása. Négy korrekt válasz (1,95%) érkezett a jogrendszerben történő elhelyezése kapcsán, például, hogy autonóm államigazgatási szervnek minősül. Fontos megjegyezni, hogy a válaszadók 82,44%-a tudta, hogy a NAIH az adatvédelemhez kapcsolódik, csak számos esetben a pontos megnevezés jelentett kihívást.

A következő kérdés a NAIH feladataira vonatkozott, amely során válaszlehetőségek álltak a joghallgatók rendelkezésére. A válaszadók több, mint fele (56,59%) a helyes választ jelölte meg, amely szerint az érintett kérelmére és hivatalból adatvédelmi hatósági eljárást folytat[81]. Az előzetes feltevéssel ellentétben meglehetősen nagy számban érkezett helytelen válasz. A válaszadók harmada szerint nem a bírósághoz[82], hanem rendvédelmi szervhez fordulhat a NAIH közérdekű adatokkal és a közérdekből nyilvá-

[79] A GDPR 4. cikk 12. pontja alapján az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

[80] Info. törvény 38. § (1) bek.

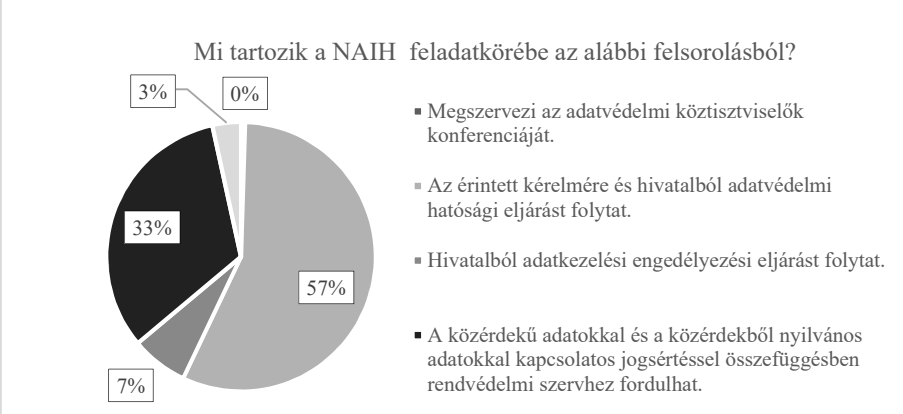
[81] Info. törvény 38. § (3) bek. b) pont.

[82] Info. torvény 38. § (3) bek. d) pont.

nos adatokkal kapcsolatos jogsértéssel összefüggésben. Továbbá tizennégy hallgató számára nem volt egyértelmű, hogy adatkezelési engedélyezési eljárást lefolytatása kizárólag kérelemre[83] lehetséges. Feltehetően az engedélyezés fogalmi keretei tekintetében is hiányosságok rejlenek. Összességében megállapítható, hogy adott válaszopciók közül is számos esetben nehézséget okozott a NAIH feladatának meghatározása, annak ellenére, hogy egy meglehetősen klasszikus feladatára irányult a kérdés. Az alábbi ábra a válaszok százalékos arányú megoszlását szemlélteti.

4. sz ábra

A NAIH egyik feladatkörének azonosítása



Forrás: A kutatás alapjául szolgáló adatok (n=205; saját szerkesztés)

Megfigyelhető, hogy azon 116 joghallgató közül, aki megfelelően választotta ki a NAIH feladatát az előző kérdésre mindösszesen a háromnegyedük (75%) válaszolt helyesen a jelentésére vonatkozóan. Következésképp a válaszlehetőségek által a feladat meghatározása egyszerűbb „próbatételnek" bizonyult, mint a nyílt kérdés keretében történő jelentés azonosítása. Mindezek alapján valószínűsíthető, hogy a legfőbb adatvédelmi intézmény jogállásával kapcsolatban is hiányosságok mutatkoznak a hallgatók tudásbázisában. Érdekességként megjegyzendő, hogy négy joghallgató megfelelően választotta ki a NAIH feladatát, azonban a meghatározásánál úgy nyilatkozott, hogy nem tudja. Feltehetően a következtetés játszhatott szerepet abban, hogy végül a helyes válasz került megjelölésre, mivel az előző kérdésből fakadóan nem az ismeretek bírtak jelentőséggel.

[83] Info. törvény 38. § (3) bek. g) pont.

8. Az adatvédelmi garanciák kérdésköre

Annak érdekében, hogy a személyes adatok védelme ténylegesen is megvalósuljon az adatvédelmi garanciáknak kardinális jelentőség tulajdonítható. Ehhez kapcsolódóan a GDPR is számos adatvédelmi garanciát biztosít például a személyes adatok kezelésére vonatkozó alapelvek alapján, amelyek közé tartozik a jogszerűség, a tisztességes eljárás és átláthatóság, a célhoz kötöttség, az adattakarékosság, a pontosság, a korlátozott tárolhatóság, az integritás és bizalmas jelleg, továbbá az elszámoltathatóság[84]. Mindezeken túlmenően az általános adatvédelmi rendelet nóvuma „az elfeledtetéshez való jog"[85], valamint az adathordozhatósághoz való jog[86] bevezetése. Ezenkívül – a teljessége igénye nélkül példaként említhető – az adatvédelmi tisztségviselő, az adatvédelmi incidens bejelentési lehetősége, illetve kötelezettsége, valamint önmagában és komplexitásában véve a NAIH intézményrendszere is ezt szolgálja.

Jelen kutatás fókuszpontjában nem a garanciák részletes ismertetése áll, hanem az, hogy a joghallgatók milyen mértékben tájékozottak, milyen ismeretek birtokába jutottak tanulmányaik során. Az adatvédelmi tudatosság kérdéskörén belül ez is fajsúlyos szerepet tölt be, tekintettel arra, hogy a felsorolt elvek is azt a cél kívánják elérni, hogy a személyes adatok védelme a lehető legmagasabb szinten érvényesülhessen. A kutatás eredményei jelentős ismerethiányra világítottak rá, mivel a joghallgatók megközelítőleg háromnegyede (74,15%) válaszként azt jelölte, hogy egyáltalán nem ismer adatvédelmi garanciát. Jelen kérdéskör kapcsán kizárólag ez az egy válaszlehetőség volt adott, egyéb esetben *quasi* nyílt kérdésként fejthették ki gondolataikat a válaszadók.

Összesen tizenkilenc hallgató válasza vonatkozott valamilyen konkrét jogosultságra, adatkezelési elvre. Példaként említhető a „felejtéshez való jog", a korlátozott tárolhatóság különböző aspektusainak körülírása, valamint a célhoz kötöttség. Ez utóbbi elv összesen kilenc hallgató (4,40%) válaszában jelent meg, amely meglehetősen csekélynek tekintendő. Ezzel összefüggésben további kérdés szerepelt a kérdőívben, amely esetében előrevetítve is elmondható, hogy szignifikánsan eltérő eredmények születtek. Következésképp feltételezhető, hogy a joghallgatók jelentős száma nincs tudatában annak, hogy a célhoz kötöttség adatvédelmi garanciának minősül.

Láthatóvá vált, hogy egy nyílt kérdés esetében nem feltétlenül jut eszükbe a célhoz kötöttség. Jelentős számú joghallgató kizárólag konkrét meghatározás alapján tudja megfelelően értelmezni, ebből következően az ismeretek összekapcsolásában anomália figyelhető meg. Hat hallgató jogforrás(ok) felsorolásával válaszolta meg a kérdést, az általános adatvédelmi rendeleten kívül egy-egy alkalommal az Alaptörvény, az Info. törvény, az Mt.[87], valamint az Nytv.[88] is megjelent. Az adatvédelmi tisztviselő két esetben tűnt fel a válaszok között, míg a NAIH mindösszesen egy alkalommal.

Összességében azon joghallgatók esetében, akik ténylegesen válasszal szolgáltak, látható, hogy ugyanazt a kérdést milyen sokféleképpen közelítették meg, még az adatkezelési szabályzat is a válaszok között volt olvasható. Megállapítható továbbá, hogy a

[84] GDPR 5. cikk (1)-(2) bek.
[85] GDPR 17. cikk.
[86] GDPR 20. cikk.
[87] A munka törvénykönyvéről szóló 2012. évi I. törvény rövidítése.
[88] A polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény rövidítése.

válaszadók jelentős száma egyáltalán nem tud adatvédelmi garanciát felsorolni, vagy körülírni. Ez az adatvédelem – megfelelő hatékonyságú – érvényesülését is megkérdőjelezheti. Mindezek alapján e kérdéskör egyértelműen azon területek közé sorolható, amely esetében az ismeretek mielőbbi bővítése, esetleges felelevenítése szükséges.

A célhoz kötött adatkezelésre vonatkozó megállapítások valóságtartalmának eldöntése

Az általános adatvédelmi rendelet (39) bekezdése, valamint az 5. cikk (1) bekezdés b) pontja a célhoz kötött adatkezelés elvéről is rendelkezik. Tekintettel arra, hogy az egyik legjelentősebb adatvédelmi garancia, a kérdőívben is hangsúlyos szerepet kapott, mégpedig hat állítás igazságtartalmának eldöntését illetően. Megjegyzendő, hogy e témakör kapcsán kizárólag a célhoz kötött adatkezelés definíciójának[89] lényegi elemei kerültek kiemelésre. Annak ellenére, hogy ténylegesen általános állítások kerültek meghatározásra, egyetlen esetben sem valósult meg, hogy valamennyi hallgató a helyes választ jelölje meg.

Az állításokat és a helyes választ adók arányát az alábbi táblázat tartalmazza.

2. sz. táblázat

A célhoz kötöttség elvére vonatkozó állítások

Állítás	Helyes válasz
Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető.	93,66%
Az adatkezelésnek csak az egyes szakaszokban kell megfelelnie az adatkezelés céljának.	90,73%
Az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie.	93,66%
Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas.	86,34%
A személyes adat csak a cél megvalósulásához szükséges mértékben, de korlátlan ideig kezelhető.	84,39%
Az adatkezelés során biztosítani kell, hogy az adatok pontosak, teljesek és naprakészek legyenek, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.	89,76%
Valamennyi állítás tekintetében helyesen válaszolók aránya:	63,9%

Forrás: A kutatás alapjául szolgáló adatok (n=205; saját szerkesztés)

Annak ellenére, hogy a fenti táblázat egyes állításai vonatkozásában a helyes válasz magas arányt képvisel, az adatvédelmi garanciák kérdéskörében – az előzőekben emlí-

[89] NAIH: Adatvédelmi értelmező szótár – www.naih.hu/adatvedelmi-szotar.html [2019. 12. 14.]

tetteknek megfelelően – mindösszesen kilenc joghallgató válaszában szerepelt nevesítve a célhoz kötöttség elve. Emellett megemlítendő, hogy ez esetben kizárólag az adott állítás valóságtartalmának eldöntése volt a feladat, amely egyrészt „egyszerűbbnek" tekinthető, másrészt a válaszadásban a tippelés, a következtetés is közrejátszó tényezőként értékelhető. A legtöbb helytelen válasz a korlátozott tárolhatóság elvével függ össze, amely az adatkezelés tekintetében kiemelt szereppel bír, mégis a hallgatók 15,61%-a úgy vélte, hogy korlátlan ideig kezelhető a személyes adat, annak ellenére, hogy számos ágazati jogszabály rögzíti a maximális megőrzési időt.

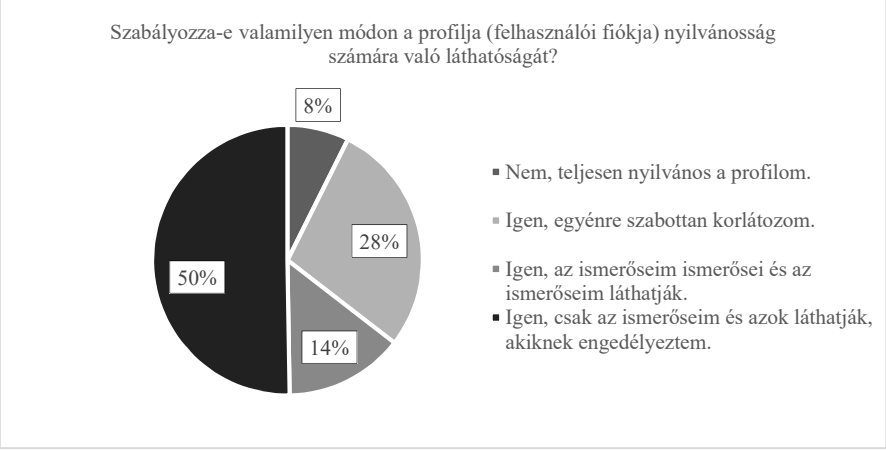
Amennyiben kizárólag egy-egy állítás értékelése történik, nem látható számottevő ismerethiány, azonban valamennyi állítás együttes elemzése esetében már észrevehető, hogy a célhoz kötöttség elvének lényegi elemeit sem ismeri a joghallgatók több, mint kétharmada (36,1%) maradéktalanul. Ez egy bizonyosfajta „felszínesebb" tudásra enged következtetni, hiszen az egyes állításoknál a megfelelő választ jelölték, míg más elemek vonatkozásában hiányosságok tapasztalhatók.

9. A felhasználói fiók közösségi oldalakon történő láthatósága

Ahhoz, hogy magasszintű adatvédelmi műveltségről és adatvédelmi tudatosságról lehessen beszélni, elengedhetetlen a személyes adatok védelemben részesítésének felismerése, továbbá ezzel összhangban az aktív cselekvés, amelyet az egyén az adatvédelmi beállítások révén tud eszközölni. Ennek egyik pillérét adja, hogy milyen személyi kör jogosult az adatok megtekintésére, vagyis, hogy a nyilvánosság számára milyen a hozzáférhetőség foka. A következő oldalon található ábra a felhasználói fiók láthatóságának szabályozására vonatkozó eredményeket hivatott szemléltetni.

5. sz ábra

A nyilvánosság számára való láthatóság alakulásának százalékos megoszlása



Forrás: A kutatás alapjául szolgáló adatok (n=205; saját szerkesztés)

Hangsúlyozandó, hogy a résztvevő joghallgatók több, mint háromnegyede (78%) alkalmazza az adatvédelmi korlátozásokat a közösségi oldalak használata során, a személyes adataik feletti kontrollt e módon gyakorolják, amely az adatvédelmi tudatosság egy lényegi elemeként definiálható. Mindazonáltal valamennyi válaszadó közül tizenöt joghallgató egyáltalán nem alkalmaz korlátozó beállításokat, amely nem éppen az adatvédelmi műveltségről tesz tanúbizonyságot. Ezzel összefüggésben több kérdés is felmerülhet, egyrészt, hogy az ismereteik hiányosak-e arról, hogy ilyen beállítások léteznek; másrészt, hogy amennyiben kellő tájékozottsággal rendelkeznek a lehetséges negatív következményekről, akkor milyen okra vezethető vissza, hogy mégsem alkalmazzák. E kérdések vonatkozásában szintén megoldást jelenthet az adatvédelmi műveltség fejlesztése.

10. A hozzájárulás kérdésköre

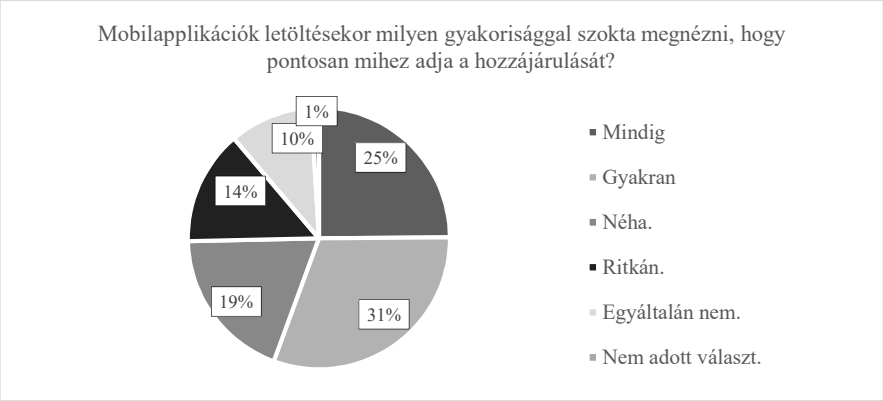
Determann tanulmányában megfogalmazott állítás napjainkban is a valóságnak megfeleltethető, hiszen a joghallgatók közel háromnegyede (74,63%) nem szokta elolvasni a közösségi oldalak adatkezelési szabályzatát, annak ellenére, hogy a válaszadók 97,07%-a napi szintű gyakorisággal használja a vizsgálat alá vont közösségi oldalak legalább egyikét, tehát hozzájárultak az adatkezeléshez.

Mindezek alapján megállapítható, hogy a hallgatók döntő többsége a személyes adataival úgy vesz részt a közösségi oldalak világában, hogy tulajdonképpen nem is tudja azt, hogy miként valósul meg az adatkezelés. Ez az attitűd szempontjából is egyfajta „érdektelenséget" sugall, mivel a kérdés tágabb körre irányult, nem kizárólagosan arra, hogy közvetlenül a hozzájárulás megadását megelőzően el szokta-e olvasni az adatkezelési szabályzatot, tájékoztatót. Ebből kifolyólag azok a válaszadók is az igen válaszlehetőséget jelölhették, akik adott esetben az időbeliség szempontjából lényegesen később olvasták el. A válaszokból egyértelműen következtethető, hogy relatíve csekély számú hallgató kíván utánajárni az adatkezelési folyamatnak.

A hozzájárulás a mobilapplikációk esetében is vizsgálandó szempontot képezett, mégpedig akként, hogy a hallgató letöltéskor meg szokta-e nézni, hogy pontosan milyen személyes adataihoz való hozzáféréshez adja a hozzájárulását. A szokások közel sem nevezhetők egységesnek, a százalékos arányok feltüntetésével a következő oldalon látható ábra foglalja össze a válaszokat.

6. sz. ábra

A mobilapplikációk letöltése során a hozzájárulás megadásának alakulása



Forrás: A kutatás alapjául szolgáló adatok (n=205; saját szerkesztés)

A számok oldaláról megvilágítva a joghallgatók közel egynegyede esetében képez olyan jelentős szempontot, hogy valamennyi esetben figyelembe vegye. Mindazonáltal a válaszadók 10%-a egyáltalán nem tekinti át. A kutatás ezen eredménye szintén alátámasztja azt, hogy általánosságban véve a hozzájárulás megadása tekintetében nem kellő megfontoltság jellemzi a hallgatókat, *quasi* nem érzik át annak a súlyát, hogy az egyszeri hozzájárulásuk megadása esetlegesen milyen jövőbeni negatív adatvédelmi kihatásokkal járhat. Ebből kifolyólag nem meglepő, hogy a szabályzatok, tájékoztatók elolvasása sem gyakori, hiszen az egyes – rövid – hozzájárulások áttekintése sem bizonyult egyértelműnek és általánosnak.

11. Az adatvédelem biztonsági vetületét érintő kérdések

Annak ellenére, hogy az adatvédelem és az adatbiztonság tekintetében jelentős distinkció megtétele szükséges, – hiszen az adatvédelem a személyre fókuszál, míg az adatbiztonság esetében az adat bír központi szereppel – elmondható, hogy esetükben komplex kapcsolatrendszer áll fenn. A lényegi elemek alapvetően két szegmenst testesítenek meg. Egyrészt az adatvédelmi szabályozás fejlődéstörténetét tekintve az adatbiztonság a személyes adatok vonatkozásában az adatvédelmi szabályozás tárgykörébe sorolható. Másrészt a magánszféra védelmi eszközeinek palettáján az adatbiztonságot szolgáló technológiák felértékelődő szereppel bírnak.[90] Ezen túlmenően olyan technológiai megoldások is rendelkezésre állnak, amelyek kifejezetten a magánszféra védelmére irányulnak, nevesítve a magánszféravédő technológiák (*privacy enhancing technologies*).[91] A hallgatók jelen kutatás keretében ugyan nem találkozhattak például minősített adatokra

[90] JÓRI 2018, 24. p.
[91] JÓRI 2018, 25. p.

vonatkozó kérdéskörrel, vagy az adatbiztonság különböző aspektusaival, mindazonáltal kiemelt szereppel bírt, milyen módon fordítanak figyelmet személyes adataik védelmére a különböző digitális eszközök használata során.

A digitális eszközök védelme

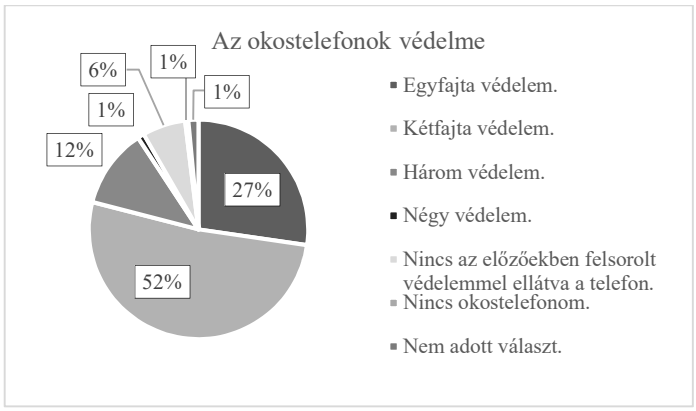
Az adatvédelmi tudatosságnak szerves részét képezi a biztonság témaköre, hiszen ahhoz, hogy a személyes adatok védelme megvalósuljon elengedhetetlen a kellő védelem megléte. Felmerül a kérdés, hogy a hallgatók vajon milyen mértékben fektetnek erre hangsúlyt digitális eszközeik vonatkozásában, amelyek az esetek döntő többségében az adattárolás helyszíneként is szolgálnak. A digitális korban az okostelefonok dominanciája érvényesül, az előzetes felvetés arra irányult, hogy a joghallgatók túlnyomó része az okostelefonját használja a közösségi oldalak látogatására.

A kutatás eredményei alapján alátámasztást nyert, hogy a válaszadók 88,29%-a esetében az okostelefon áll a preferencia legmagasabb fokán. Emellett megállapítható, hogy a joghallgatók döntő többsége (93,63%) valamilyen módon védi okostelefonja tartalmát. Ezzel összefüggésben megemlítendő, hogy a válaszadók közel háromnegyede (73,04%) biometrikus – ujjlenyomattal vagy arcképpel történő – azonosítással oldja fel mobilkészüléke zárját. Ennek jelentősége abban mutatkozik meg, hogy a GDPR 9. cikk (1) bekezdése alapján a biometrikus adat a személyes adatok különleges kategóriájának minősül, ezáltal szigorúbb szabályozás vonatkozik az adatkezelésre.

A hallgatók összesen hat válaszopció közül – többszörös válaszadás keretében – határozhatták meg, hogy milyen módon védik okostelefonjukat, mindezek a következők szerint kerültek meghatározásra: ujjlenyomat azonosító, arckép azonosító, zárképernyő jelszó, zárképernyő ábra vagy kód, alkalmazás zár, valamint az is külön válaszopciót képezett, hogy adott esetben nincs az előzőekben felsorolt védelemmel ellátva a telefon.

7. sz. ábra

Az okostelefonok védelemmel való ellátása



Forrás: A kutatás alapjául szolgáló adatok (n=205; saját szerkesztés)

Az ábra alapján jól látható, hogy a hallgatók jelentős része legalább kétfajta védelemmel is ellátja telefonját. Ennek ellenére szám szerint tizenhárom joghallgató egyáltalán nem fordít figyelmet okostelefonja védelmére. Annak ellenére, hogy előzetes feltevésként az került meghatározásra, hogy valamennyi joghallgató védi – valamilyen módon – telefonját. A válaszadók 6,34%-a ezen feltevést cáfolta, amely kellő mértékű tájékozottság hiányára utal, hiszen számos védelmi beállítási mód áll rendelkezésre.

Figyelembe véve, hogy nem kizárólag okostelefonok útján valósul meg a közösségi oldalak használata, az is meghatározó szempontot képezett, hogy a számítógép, laptop és tablet, továbbá a fájlok tekintetében mennyire jellemző a jelszavas védelem beállítása. A válaszok alapján megfigyelhető, hogy a joghallgatók 80%-a él a jelszóbeállítási lehetőséggel a számítógépek, laptopok és tabletek esetében. Elgondolkodtató, hogy a válaszadók egyötöde a számítógépén vagy laptopján sem alkalmazza a jelszavas védelmet, amely kifejezetten veszélyforrást jelenthet. Mindazonáltal amennyiben a digitális eszközökön tárolt fájlokról van szó az előző eredménnyel szemben, lényegesen alacsonyabb arányról beszélhetünk (38,54%). A fájlok jelszavas védelemmel való ellátása, a fokozott biztonságra törekvés nem kellően elterjedt. Azonban megjegyzendő, hogy közrejátszó szerepet tölthet be, hogy a válaszadó a számítógépét, illetve laptopját látja el védelemmel, és ebből kifolyólag nem érzi szükségesnek, hogy a fájljait is külön védelemben részesítse.

V. Következtetések és javaslatok

Az empirikus kutatás eredményei alapján egy speciális személyi kör, nevezetesen a joghallgatók esetében jelentős hiányterületek (pl. általános tájékozottság, adatvédelmi garanciák ismerete) feltárására került sor, amely az (1) hipotézisben foglaltakat támasztja alá. Megemlítendő, hogy az *„exceptio probat regulam”* jelen esetben is igaznak bizonyul, hiszen néhány joghallgató válaszai kifejezetten magasszintű adatvédelmi ismeretek elsajátításáról, valamint adatvédelmi tudatosságról tettek tanúbizonyságot.

Általánosságban véve az adatvédelmi tudatosság fejlesztéséhez elengedhetetlen a hallgatói attitűdben bekövetkező változás. Példaként említhető a mások személyes adatainak védelmére való nagyobb odafigyelés, mivel az eredmények alapján láthatóvá vált, hogy a hallgatók a saját személyes adataik védelmére lényegesen nagyobb figyelmet fordítanak, mint más személyekére. A (2) hipotézis is igazolást nyert, tekintettel arra, hogy a résztvevő joghallgatóknak szinte teljes mértékben azonos a véleménye az adatvédelem jelentőségének megítélésében, azonban a közösségi oldalakon való jelenlétük nem feltétlenül ezt tükrözi, továbbá a vélt tudás is nagymértékben meghatározó. Az intézményrendszer keretében a NAIH kapcsán szintén láthatóvá vált, hogy hiányos, adott esetben téves ismeretek birtokában állnak a joghallgatók.

A kutatás egyik legjelentősebb eredményeként értékelendő, hogy megállapítást nyert – a (3) hipotézis –, hogy a joghallgatók számára a személyes adatok gyakorlati példákon keresztül történő azonosítása kifejezetten nehéz feladatnak bizonyul. Egy bizonyosfajta ismerethiány figyelhető meg, amely egyrészt a kellő informatikai és technológiai háttértudás hiányára vezethető vissza, másrészt az egészségügyi adatok kapcsán jelentős kü-

lönbség mutatkozott azonos megítélésű személyes adatok jogi természetének meghatározásában, amely a „biztos tudás" hiányára utal. Mindezek a gyakorlatorientált oktatás fontosságát hangsúlyozzák. A (4) felvázolt hipotézis esetében a kutatás alapján pozitívabb képet mutat a valóság, mivel elsődlegesen a saját személyes adatokra fókuszálnak a hallgatók, de jelentős számú hallgató a képmegosztások tekintetében egyaránt odafigyel a háttérben látszódó személyekre is. Azonban az is megállapítható, hogy más személyek személyes adatai tekintetében számottevő tudásbéli hiányosságok kerültek a felszínre. A kutatás eredményei rávilágítottak arra, hogy az (5) hipotézisnek megfelelően a hozzájárulás megadása szempontjából a joghallgatók nem kellő mértékben körültekintők, a válaszok alapján feltételezhető, hogy nincsenek teljesen tudatában annak, milyen fajsúlyos szerepet tölt be a hozzájárulás az adatvédelem kérdéskörében.

Javaslatként fogalmazható meg joghallgatói részről a nemcsak „tudok róla", hanem az „úgy is cselekszem" szemléletmód gyakorlatba történő implementálása, valamint kellő nyitottság az új ismeretek, továbbá a tudásbázis bővítése iránt. Az odafigyelés, a lehetséges következmények, kockázatok átgondolása hatékonyabb adatvédelmet tesznek lehetővé. Mindazonáltal nélkülözhetetlen, hogy a hallgatók attitűdjében is tükröződjön annak felismerése, hogy valóban fontos az adatvédelem, és ezt cselekvés is kövesse mind szakmai, mind hétköznapi szempontból.

Ezen túlmenően az oktatás kardinális szerepet tölt be az adatvédelmi tudatosság kérdéskörében. Kutatási eredmények is bizonyítják, hogy pozitív hatást gyakorol a hallgatók adatvédelmi műveltségére, a közösségi oldalak vonatkozásában is a tudatos használatra ösztönöz. Hangsúlyozandó, hogy az oktatás alatt nem kizárólagosan a lexikális ismeretanyag értendő, hiszen a személyes adatokra „minősítésére" vonatkozó kérdés teljes mértékben kifejezésre juttatta, hogy egy olyan egyszerűnek tűnő kérdés, miszerint egy adott információ személyes adatnak minősül-e meglehetősen nehezen megválaszolhatóvá vált, kiemelve azt, hogy jelentős mértékű helytelen válasz érkezett. További javaslatként említhető, hogy az oktatás keretein belül bevezetésre kerülhetne a joghallgatók körében a bemeneti és kimeneti kompetenciamérés, amely teljeskörű megfigyelést tenne lehetővé kiküszöbölve a mintavételi limitációkból származó hibaforrásokat.

Jövőbeli kutatásként különböző képzési területek hallgatóinak – például közgazdászok, mérnökök, nyelvészek, orvosok, tanárok, zenészek – bevonása által komplexebb képet lehetne alkotni arról, hogy összességében milyen adatvédelmi tudatossággal rendelkeznek az egyetemi hallgatók. Lehetőséget biztosítva összehasonlító vizsgálatokra, mivel a tanulmányokból és a professzióból fakadóan feltételezhető, hogy a joghallgatók széleskörűbb ismeretek birtokában állnak.

VI. Összegzés

Napjainkban egyértelműen megállapítható, hogy a személyes adatok egyre értékesebbé válnak. Ahhoz, hogy adatvédelmi garanciák érvényesülni tudjanak, elengedhetetlen az egyének részéről, hogy figyelmet fordítsanak mindennapi szokásai körében is az adatvédelemre. Ez alól a közösségi oldalak használata sem képez kivételt, sőt hatványozottan kifejezésre jut, amelyen – néha észrevétlenül is – számtalan személyes adat megosztására kerül sor.

Az empirikus kutatás eredményei tükrében látható, hogy jelentős hiányterületek kerültek feltárásra. A korosztályból fakadóan is a joghallgatók körében a közösségi média meghatározó szerepet tölt be, viszont hangsúlyozandó, hogy a tudatos használat csökkenti az esetleges adatvédelmi incidensek bekövetkezésének kockázatát. Az ismeretek bővítése által jelentős mértékben növelhető az adatvédelmi műveltség, amely az adatvédelmi tudatosságra is pozitív hatást gyakorol. Az adatvédelmi paradoxon feloldására az adatvédelmi tudatosság növelése is segítséget nyújthat, hiszen a folyamatok ismerete és a lehetséges következmények átlátása által körültekintőbb viselkedés válhat általánossá az online közösségi felületeken egyaránt. Jelen kutatás iránymutatásként szolgál a jövőre vonatkozóan, hogy mely területekre szükséges nagyobb hangsúlyt fektetni, ezáltal biztosítva az adatvédelmi tudatosság fejlesztését.

KARDOS VIVIEN KATA

PRIVACY AWARENESS AMONG LAW STUDENTS

(Summary)

The focus of the study is to examine the privacy awareness of law students in particular to assess their level of knowledge in data protection, furthermore, to discover how prudent they are about data protection when using social networking sites (SNSs), and to establish any gaps of knowledge in the field of privacy awareness.

Foreign literature is crucial in exploring the topic, additionally, privacy literacy as a key element of it. The empirical research was carried out on a quantitative basis through a questionnaire with a total participation of 205 law students from all faculties of law and political sciences in Hungary. The questions were constructed as a point of orientation to cover knowledge, attitudes, and habits as well.

The results highlighted several gaps. In the light of the outcome, it can be concluded that law students pay significantly less attention to the protection of other people's personal data than to their own personal data and identifying personal data through practical examples causes difficulties. Law students are not sufficiently careful about giving consent, both in terms of attitudes and habits. The issue of the cookie identifier underlined significant shortcomings, with just over a quarter of law students classifying it as personal data. Nevertheless, more than two-thirds of the respondents considered it „risky" from a data protection perspective.

In order to data protection safeguards be properly enforced, it is essential that individuals actually pay attention to data protection in their everyday customs. Knowledge development in data protection can significantly increase privacy literacy, which is also crucial for privacy awareness. Social media, especially SNSs, is considerably relevant to personal data among law students, and conscious usage can reduce the risk of a potential personal data breach. It should be emphasized that education has a key role to play in developing privacy awareness in the field of data protection.