

OTDK-dolgozat

2023.

Miskolci Egyetem



SZEMÉLYES ADATOK VIZSGÁLATA AZ ONLINE TÉRBEN

EXAMINING PERSONAL DATA IN THE ONLINE WORLD

Szerző: Gulyás Nóra

Konzulens: Dr. Csiszár Csilla Margit

Kézirat lezárása: 2023. január 8.

Tartalomjegyzék

1. BEVEZETÉS	1
2. KUTATÁSI MÓDSZER ÉS TERMINOLÓGIA	4
2.1 KUTATÁSI MÓDSZEREK.....	4
2.2 ALAPFOGALMAK	6
3. A SZEMÉLYES ADATOK SZABÁLYOZÁSI KÖRNYEZETE	13
3.1 AZ ADATVÉDELEM KIALAKULÁSA EURÓPÁBAN.....	13
3.2 ADATVÉDELEM AZ EURÓPAI UNIÓBAN	17
4. SZEMÉLYES ADATAINK NYOMÁBAN	22
4.1 GOOGLE ADATGYŰJTÉS ÉS ADATKEZELÉS	27
4.1.1 Google alkalmazások vizsgálata	28
4.1.2 Google hirdetések és különleges adatok	31
4.2 FACEBOOK ADATGYŰJTÉS ÉS ADATKEZELÉS	34
4.3 TIKTOK ADATGYŰJTÉS ÉS ADATKEZELÉS.....	39
5. ADATVÉDELMI INCIDENSEK.....	44
5.1 A LEGNAGYOBB BÜNTETÉSEK	44
5.2 BEJELENTETT ADATVÉDELMI INCIDENSEK	46
5.3 ADATBIZTONSÁGI PROBLÉMÁK	49
5.4 SZEMÉLYES ADATOK VÉDELME	54
6. KÖVETKEZTETÉSEK, JAVASLATOK	56
7. ÖSSZEGZÉS.....	59
8. IRODALOMJEGYZÉK.....	62
9. MELLÉKLET	I
9.1 ADATVÉDELEM AZ EURÓPAI UNIÓN KÍVÜL	I
9.2 ORSZÁGOK JELÖLÉSE.....	IV
9.3 EGYÉB ADATVÉDELMI INCIDENSEK.....	V
9.4 A COVID-19 HATÁSA A SZEMÉLYES ADATOKRA.....	VII

Táblázatok- és ábrajegyzék

Képek:

1. kép: Google alkalmazások	27
-----------------------------------	----

Infografikák:

1. Infografika: Személyiségi jogok	20
2. Infografika: Az alkalmazások által gyakran gyűjtött adatok.....	23
3. Infografika: A Facebook által gyűjtött adatok	35

Táblázatok:

1. táblázat: A személyes adat magyar törvényekben található meghatározása	7
2. táblázat: A különleges adat magyar törvényekben található meghatározása	8

Ábrák:

1. ábra: A különleges adat típusai	9
2. ábra: Európai Unió adatvédelmi szabályozás fejlődéstörténete	13
3. ábra: Magyarország adatvédelmi szabályozás fejlődéstörténete.....	15
4. ábra: Az intézmények/vállalatok adatvédelmébe vetett bizalom (EU28; 2015)	18
5. ábra: Adatfelhasználási szabályok	19
6. ábra: A GDPR által biztosított jogok ismerete (2019)	21
7. ábra: Az adatvédelmi nyilatkozatokat olvasók aránya (2020, 2021)	26
8. ábra: A célzott hirdetésekről alkotott vélemény	31
9. ábra: Facebook felhasználók számának és a hirdetésekből származó bevételek növekedése (2009-2021)	34
10. ábra: Az adatvédelmi beállításokat módosítók aránya (EU27,2020)	38
11. ábra: A TikTok bevételeinek és az aktív felhasználók számának alakulása 2018-2022.....	39
12. ábra: A legmagasabb büntetések a GDPR megszegése miatt	44
13. ábra: A személyes adatokkal kapcsolatos jogok védelméért felelős hatóság ismerete (EU27;2019).....	46
14. ábra: Bejelentett adatvédelmi incidensek (2018-2021)	47
15. ábra: Adatbiztonsági problémák.....	49
16. ábra: Internetes tevékenységek.....	50
17. ábra: Az adatbiztonsággal kapcsolatos tapasztalat és az aggodalom kapcsolata (EU27;2019).....	50
18. ábra: A tapasztalt biztonsággal kapcsolatos problémák és az aggodalom közötti kapcsolat- outlierek nélkül.....	51
19. ábra: A tapasztalt biztonsággal kapcsolatos problémák és az aggodalom közötti kapcsolat-	52
20. ábra: A kibertámadással kapcsolatos tájékozottság és aggodalom kapcsolata.....	53
21. ábra: Adatvédelemmel kapcsolatos tevékenységek	54
22. ábra: Országcsoporthoz.....	55

1. BEVEZETÉS

Manapság a papír alapú dokumentumok helyett az elektronikus információ és adat került a középpontba. A gazdasági és technológiai fejlődésnek köszönhetően mára bármilyen adatot továbbíthatunk akárhová. A felhő alapú tárolórendszerekben végtelen mennyiségű adatot lehet tárolni. Az adatok bármennyiszer reprodukálhatók és romlás nélkül megoszthatók másokkal. Az évek során egyre kényelmesebbé vált az internetes böngészés. Ezzel párhuzamosan megnőtt a vállalatok által felhasznált személyes információk mennyisége, ami maga után vonta azt, hogy nőtt az adatok illetéktelen felhasználásának is a kockázata, így a személyes adatok védelme és az adatkezelés szabályozása kiemelten fontossá vált.

Azért választottam az adatvédelem témakörét, mert fontosnak tartom, hogy tudjuk, hogy a vállalatok hogyan és mire használják fel a személyes adatainkat és tisztában legyünk a jogainkkal. Mára szinte minden információt tud rólunk a telefonunk, rengeteg adatot tárolunk rajta, melyeket az egyes vállalatok ki is használnak. Az utóbbi időben észrevettem, hogy már olyan mobilalkalmazások is engedélyt kérnek a letöltéskor például a névjegyek vagy a kamera használatára, amelyek funkciói egyáltalán nem kapcsolhatók össze ezekkel. Felmerült a kérdés bennem, hogy vajon pontosan milyen adatokat gyűjtenek az egyes alkalmazások és hogyan akadályozhatom meg ezt? Az emberek tudnak tenni -és ha igen-, akkor tesznek azért, hogy kevesebb adatot használjanak fel róluk? Féltik a felhasználók az adataikat? Engem egyre jobban zavarnak a személyre szabott hirdetések. Valószínűleg mindannyiunkkal előfordult már, hogy rákerestünk egy-egy termékre, szolgáltatásra, majd ezt követően számos, a termékkel kapcsolatos hirdetéssel találkoztunk. Ez szinte már természetessé vált. Sokszor előnyös és kényelmes, ám elgondolkodtató is egyben. Tényleg minden lépésünket figyelik a vállalatok?

Az adatvédelem kialakulásának kezdete a XX. századra tehető. Jelenleg, 2018. május 25. óta GDPR (General Data Protection Regulation), azaz az Európai Unió általános adatvédelmi rendelete szabályozza a személyes adatok gyűjtését és felhasználását az Unió tagállamaiban. A rendelet azon az Európai Unió területén kívül működő vállalatokra is vonatkozik, amelyek árut értékesítenek vagy szolgáltatást nyújtanak az EU-n belül. A dolgozatban említést teszek néhány az Európai Unión kívüli ország szabályozásáról is, mint pl.: Kanada vagy Kína. Dolgozatom célja, hogy áttekintést adjak a személyes adatok szabályozási környezetéről, ezzel a személyiségi jogainkról az Európai Unióban. Az új szabályok bevezetésének következményeként a cégek számára sok nehézséggel jár a személyes adatok szabályszerű felhasználása. Azonban fontos, hogy betartsák ezeket, hiszen a rendelet megszegéséért 20 millió euróig, vagy az adott vállalat éves árbevételének 4%-áig terjedő

bírságot szabhatnak ki. (European Union, 2018). A leghíresebb cégek, mint pl.: az Amazon vagy a Whatsapp már súlyos, több 100 millió dolláros büntetést kaptak a GDPR megszegéséért. (CMS.Law, 2022.) A dolgozatom további célja, hogy szemléltessem, hogy a rendelet bevezetése óta mely országokban történt a legtöbb hivatalos bejelentés az adatvédelmi incidensek miatt. A DLA Piper multinacionális ügyvédi iroda adatvédelemmel foglalkozó csoportja minden évben végez felmérést a bejelentett adatvédelmi incidensek számáról. Ezeket a kutatási eredményeket használom fel a szemléltetéshez.

További célom az volt, hogy megvizsgáljam, hogy az egyes országokban milyen adatbiztonsági problémákat tapasztaltak és melyek azok, amiktől a legtöbben tartanak? Melyek a személyes adatokkal kapcsolatos aggodalmak meghatározó tényezői? A feltételezésem vizsgálatához Pearson-féle korrelációs elemzést és regresszió számítást végeztem. Ezzel megállapítom, hogy milyen mértékű és irányú kapcsolat van a vizsgált ismérvek között. Vizsgálatom során az Európai Unió adatvédelemmel és digitális biztonsági készségekkel kapcsolatos kutatásait használom fel.

A vállalatoknak hatalmas lehetőség az, hogy a legismertebb és leggyakrabban használt alkalmazásokon keresztül célzott hirdetéseket tudnak megjeleníteni, amiért természetesen fizetnek nekik. Mi pedig ahhoz, hogy „ingyenesen” tudjuk használni az alkalmazásokat, weboldalakat, sokszor a személyes adatainkkal „fizetünk”. Dolgozatom célja az is, hogy áttekintést adjak arról, hogy az olyan óriásvállalatok, mint a Google, a Facebook és a TikTok milyen személyes adatokat gyűjtenek be rólunk, mire használják fel ezeket, illetve hogyan követik a tevékenységünket az interneten. Ennek vizsgálatához dokumentumelemzést végeztem, amely során részletesen áttekintettem a három vállalat adatvédelmi irányelvét. Jellemző a felhasználókra, hogy legalább részben elolvassák ezeket a dokumentumokat? Azért választottam ezeket a cégeket, mert a keresőmotorok körében egyértelműen a Google-t használják a legtöbben és hozzá számos más alkalmazás is kapcsolódik, mint például a Gmail, a Drive, a Google Hírek, a Google Fordító, a Térkép. (Johnson, 2022. b) A Facebook a közösségi hálózatok csoportjában az első helyen szerepel, ezt használják a legtöbben. (Statista.com, 2022.d) A TikTok pedig mára a legtöbbször letöltött alkalmazások közé tartozik. (STH, 2022.) Az adatvédelmi dokumentumoknak azt is tartalmazniuk kell, hogy hogyan korlátozhatjuk vagy állíthatjuk le az adataink begyűjtését. Dolgozatom célja továbbá, az Unió fogyasztók adatvédelmi attitűdjének vizsgálata. Megvizsgálom, hogy az egyes országokban tesznek-e a felhasználók annak érdekében, hogy a vállalatok kevesebb adatot gyűjtsenek be róluk. A kutatási kérdések közé tartozik többek között, hogy az egyes országokban a fogyasztók milyen aránya módosította már az adatvédelmi beállításait. Kik azok, akik korlátozták vagy

visszaautasították már a személyes adataik felhasználását? Használják a fogyasztók olyan szoftvereket, amelyek korlátozzák a nyomon követést? Ellenőrzik a weboldalt, mielőtt megadják a személyes adataikat? Az eredmények alapján az Európai Unió országokat csoportokba rendeztem, ezzel megtudhatjuk, hogy melyek azok az országok, amelyekre jellemző, hogy a felhasználók tesznek az adataik megóvásáért.

A dolgozat szerkezeti felépítését tekintve, először bemutatom a vizsgálatok során alkalmazott kutatási módszereket és tisztázom az adatvédelem és a személyes adat fogalmát, amelyhez főként a törvényi meghatározásokat használom. Ezt követően bemutatom az adatvédelem kialakulását az Európai Unióban és Magyarországon. Majd megvizsgálom, hogy milyen szabályozási környezet jellemzi a személyes adatok gyűjtését és felhasználását. Ismertetem az adatfelhasználási szabályokat és a személyiségi jogokat. Részletesen áttekintem az Európai Unió általános adatvédelmi rendeletét és röviden bemutatom néhány az Európai Unió kívüli ország szabályait is. A továbbiakban elemzem a Google, a Facebook és a TikTok adatvédelmi szabályzatát. Vajon mennyire könnyen értelmezhető és átlátható? Meddig tart az átolvasása? Jellemző a felhasználókra, hogy elolvassák ezeket? Az adatvédelmi dokumentumok alapján összegzem, hogy milyen adatokat gyűjtenek be rólunk és mire használják fel azokat. Ezt követően bemutatom a legnagyobb büntetéssel járó adatvédelmi incidenseket, majd megnézzük, hogy a GDPR bevezetése óta az egyes országokban mennyi adatvédelmi bejelentés történt. Megvizsgálom a kiberbűnözéssel kapcsolatos aggodalom okait. Végül pedig az Európai Unió országait csoportokba rendezem annak függvényében, hogy mennyire tudatosak az adataik védelmét illetően. A tudatosságot több szempont mentén vizsgálom, ilyen például az adatvédelmi beállítások módosítása, weboldalak ellenőrzése vagy olyan szoftver használata, amely korlátozza a nyomkövetést.

2. KUTATÁSI MÓDSZER ÉS TERMINOLÓGIA

Dolgozatom első fejezetében röviden bemutatom a vizsgálatomhoz használt kutatási módszereket és ismertetem a vizsgálatához felhasznált fontosabb forrásokat. Ezt követően megismerkedünk a személyes adat definíciójával, annak törvényi meghatározásainak változásával, külön figyelmet fordítva a különleges adatokra, illetve tisztázzuk az adatvédelemhez szorosan kapcsolódó fogalmakat, amelyekkel a dolgozat későbbi fejezeteiben találkozni fogunk.

2.1 KUTATÁSI MÓDSZEREK

A dolgozatomban több szempontból vizsgálom a személyes adatot. Egyik célom összegezni, hogy az óriásvállalatok milyen személyes adatokat gyűjtenek be és használnak fel rólunk az alkalmazások használatával és tehetünk-e ellene. Három óriásvállalatot választottam az elemzéshez. A kutatási forrásaim az adatvédelmi dokumentumaik lesznek. Az egyik a Google, mert ez a leghíresebb keresőmotor (Johnson, 2022. b), a másik a Facebook, mert az első helyen áll a közösségi médiában (Statista.com, 2022.d), a harmadik pedig a legújabb örület, a TikTok, amely a legtöbbször letöltött „nem játék” kategóriájú mobilalkalmazás. (STH, 2022.) A kvalitatív módszertan, amit választottam a vizsgálatomhoz, az a *dokumentumelemzés*, amely egy adatgyűjtési eljárás, melynek alapja valamilyen kész produktum vizsgálata, szubjektív tanulmányozása, kritikája. (Hunkár, 2013) Főként napjaink anyagaival foglalkozik. (Kérdő, 2008.) Elemezhetünk vizuális anyagot, írott szöveget vagy rögzített előbeszédet is (Kiss et al., 2006.). Először röviden bemutatom a választott vállalatokat, majd áttekintést adok az adatvédelmi dokumentumaikról. Összefoglalom azokat a személyes adatokat, amiket begyűjtenek és használnak, majd elemzem a dokumentumokat. Megállapítom, hogy az adatvédelmi dokumentumok alapján egyszerűen tudjuk-e módosítani az adatvédelmi beállításokat.

Ezt követően megvizsgálom, hogy tartanak-e a fogyasztók attól, hogy a személyes adataik nincsenek biztonságban az interneten és hogy *melyek a személyes adatokkal kapcsolatos aggodalmak meghatározó tényezői*. Ennek kapcsán több összefüggést keresek például megvizsgálom, hogy milyen arányban fordul elő az egyes Uniós országokban, hogy a személyes információkat valamilyen sérelem éri. Ehhez a vizsgálatomhoz kvantitatív vizsgálatot, Pearson-féle korrelációs elemzést és regresszió számítást végeztem. A korreláció két ismérv közötti lineáris kapcsolat vizsgálatára használható. Az elemzésből a kapcsolat erőssége és az

iránya is kiderül. Az érték -1 és 1 közötti. Minél közelebb áll az eredmény abszolút értékben az 1-hez, annál szorosabb a kapcsolat a két tényező között. Lineáris regresszió esetén a determinációs együttható a korreláció értékének négyzete. Ez megmutatja, hogy milyen mértékű a függőség a két változó között és milyen százalékban befolyásolják egymást. Minél közelebb áll az R^2 értéke az 1-hez, annál erősebb a függőség. Ehhez a vizsgálatomhoz az Európai Unió 2019-es *Az internet használata során tapasztalt biztonsági problémák* című kutatását, a 2019-es *Az európaiak hozzáállása a kiberbiztonsághoz* című Eurobarometer (499) kutatását és a *Digitális jogok és alapelvek* című Eurobarometer (518) kutatását használok fel. Végül megvizsgálom, hogy mely tagországok a legtudatosabbak az adataik védelmével kapcsolatban. Több tényezőt veszek figyelembe, ami alapján csoportokba sorolom az országokat. Vizsgált tényezők:

- annak ellenőrzése, hogy biztonságos-e az a weboldal, ahol a felhasználó személyes adatokat közöl,
- az adatvédelmi nyilatkozatok elolvasása a személyes adatok megadása előtt,
- a saját földrajzi helyhez való hozzáférés korlátozása vagy megtagadása,
- a profilhoz vagy tartalomhoz való hozzáférés korlátozása a közösségi oldalakon vagy online tárhelyen,
- a személyes adatok reklámcélú felhasználásának megtagadása,
- internetböngésző beállításainak módosítása, hogy megakadályozza vagy korlátozza a cookie-k használatát valamely eszközén. (Eurostat, 2021.)

Megvizsgálom, hogy az egyes adatvédelemmel kapcsolatos tevékenységeket melyik országokban végzik a legnagyobb arányban, ezáltal rangsorolom őket és végül átlagolom a rangsorokat. Az Európai Unió átlag is kap egy rangsort, ehhez viszonyítva sorolom az országokat 4 csoportba: Vezetők, Követők, Felzárkózók, Lemaradók. Ehhez a vizsgálatomhoz az Európai Unió 2021-es személyes adatok védelmével kapcsolatos kutatásait használtam fel.

2.2 ALAPFOGALMAK

Ebben a fejezetben a személyes adat különböző meghatározásait és a hozzá kapcsolódó fogalmakat tekintjük át. A személyes adatot az Európai Parlament és a Tanács 95/46/EK irányelve az alábbi módon definiálja „... az azonosított vagy azonosítható természetes személyre (*"érintettre"*) vonatkozó bármely információ; az azonosítható személy olyan személy, aki közvetlen vagy közvetett módon azonosítható, különösen egy azonosító számra vagy a személy fizikai, fiziológiai, szellemi, gazdasági, kulturális vagy társadalmi identitására vonatkozó egy vagy több tényezőre történő utalás révén...” (Az Európai Parlament és a Tanács 95/46/EK irányelve, 1995.). A személyes adat tehát nem jogi személyekre vonatkozik, hanem természetes, élő személyekre, így a jogi személyekre nem terjed ki a védelem sem. A természetes személyt közvetlenül azonosíthatják pl.: a neve alapján és közvetetten pl.: a telefonszáma vagy az autójának a rendszáma alapján. Közvetett mód az is, ha olyan jellegzetes információt mondunk róla, ami alapján egyértelműen fel lehet ismerni. Pl.: Magyarország miniszterelnöke. (European Commission, 2007.). A 95/46/EK irányelvet a GDPR bevezetése során hatályon kívül helyezték. A fent említett definíció a jelenleg hatályos GDPR általános adatvédelmi rendeletben az alábbiak szerint került módosításra: „...*azonosított vagy azonosítható természetes személyre („érintett”)* vonatkozó bármely információ; *azonosítható az a természetes személy, 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.*” (Európai Parlament és Tanács, 2016.)

Láthatjuk, hogy a két definíció nem tér el egymástól, az újabb meghatározás néhány szóval került kiegészítésre. 1995 és 2016 között hatalmas változás történt a személyes adatok begyűjtését és felhasználását illetően az internet elterjedését követően. Míg 1995-ben az internetet használók száma kb. 16 millió volt, (Nurunnabi, 2010.) 2016-ban már közel 3,5 milliárd ember használta az internetet (Firdaus, 2017.). Napjainkban pedig már több, mint 5 milliárd, a teljes népesség 2/3-a. (DataReportal, 2022.) Elképesztő különbségek. A több mint 20 év alatt a technika is hatalmasat fejlődött. Például már a helyadatainkat is tudhatják az egyes alkalmazások, ami meg is jelenik a 2016-os definícióban. Az újabb meghatározásban található kiegészítés tehát főként a technológiai fejlődésnek és az emberek online térben való részvételének köszönhető. Mára a személyes adatokat már üzleti célokra is begyűjtik, amelyeket szintén a későbbiekben fogunk megvizsgálni. Ezekre a tényezőkre 1995-ben még

nem kellett külön figyelmet fordítani. A magyar adatvédelemmel kapcsolatos törvényekben is megtalálhatjuk a személyes adat fogalmát:

1. táblázat: A személyes adat magyar törvényekben található meghatározása

Törvény	Meghatározás
1992. évi LXIII. törvény	„... a meghatározott természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható...”
2003. évi XLVIII. törvény	„... bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt - közvetlenül vagy közvetve - név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet...”
2011. évi CXII. törvény	„... az érintettre vonatkozó bármely információ...”

Forrás: saját szerkesztés az (1992. évi LXIII. törvény, 1992), (2003. évi XLVIII. törvény, 2013.) (2011. évi CXII. törvény, 2011) alapján

Láthatjuk, hogy az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról magyar törvényben megtalálható definíció sem tér el nagymértékben az előzőekben vizsgált Európai Unió meghatározástól. Tartalmazza, hogy természetes személyekre vonatkozik a definíció és velük kapcsolatba hozható adatokról van szó. Különbség az előző meghatározásokhoz képest, hogy a magyar törvényi definícióban megjelenik az is, hogy meddig őrzi meg minőségét. 11 évvel később, a 2003. évi XLVIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény módosításában kiegészítésre került az előző meghatározás. A definícióban már megjelenik, a közvetlen és a közvetett azonosítás is, úgy, mint az Unió meghatározásokban. A 2011. évi CXII. törvényben -az információs önrendelkezési jogról és az információszabadságról (Infotv.)- viszont rendkívül lerövidül a személyes adat definíciója. A jogalkotó egyértelműen érezteti, hogy a személyes adatok körébe már minden információ beletartozik, amely az érintettre vonatkozik. Ez azt jelenti, hogy a jogszabály még több információra kiterjed, mint korábban.

Összefoglalva tehát, személyes adatnak tekinthető az összes olyan információ, amely az érintettre vonatkozik. Idetartozik például: a vezetéknév és utónév, lakcím, a személyazonosító iratok száma, telefonszám, az előző példához kapcsolódóan az IP-cím, ügyfélszám, a személy

egyedi azonosítását lehetővé tevő kórházi adatok, vezetéknév.utónév@vállalkozás.com típusú e-mail-címek és a Neptun kódunk is. Azok a személyes adatok, amelyek korábban már azonosításra alkalmatlanná váltak, vagy álnevesítettek, de felhasználhatók a személy újraazonosítására, szintén személyes adatnak minősülnek. Azonban azok a személyes adatok, amelyek alapján az anonimizálás következtében már nem lehet beazonosítani az egyént, többé nem tekinthető személyes adatnak. Ekkor viszont az anonimizálásnak visszafordíthatatlannak kell lennie (Európai Bizottság, 2018) . A törvényekben külön meghatározásra kerülnek a különleges adatok, amelyekre szigorúbb szabályozás vonatkozik. Az évek során ezen adatok definíciója is változott:

2. táblázat: A különleges adat magyar törvényekben található meghatározása

Törvény	Meghatározás
1992. évi LXIII. törvény	„... a faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más meggyőződésre, az egészségi állapotra, a kóros szenvedélyre, a szexuális életre, valamint a büntetett előéletre vonatkozó személyes adatok.”
2003. évi XLVIII. törvény	„... a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviselési szervezeti tagságra , az egészségi állapotra, a kóros szenvedélyre, a szexuális életre vonatkozó adat, valamint a bűnügyi személyes adat . ”
2011. évi CXII. törvény	„A személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok , az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.”

Forrás: saját szerkesztés (1992. évi LXIII. törvény, 1992) (2003. évi XLVIII. törvény, 2013.) (2011. évi CXII törvény, 2011) alapján

Az 1992. évi definíció szerint a különleges adatok közé tartozik a faji, etnikai, politikai, vallási, egészségügyi, a szexuális életre és büntetett előéletre vonatkozó személyes adat. Ahogy a 2. táblázatban láthatjuk, 2003-ra bővült a különleges adatok csoportja az érdek-képviselési szervezeti tagsággal és a 2003. évi XLVIII. törvényben már meghatározásra került a bűnügyi személyes adat fogalma is.¹2011-re a különleges adatok köre még tovább bővült, ekkor már a

¹ „A büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetőleg a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.”

definícióban szerepelnek a genetikai adatok² és a biometrikus adatok³ is. A technika fejlődése miatt manapság sokan az ujjlenyomattal vagy az arcképpel való azonosítást napi szinten használják, hiszen a telefon feloldásához szükség lehet rá. Ezen kívül online vásárlás során a telefonos jóváhagyáshoz szintén szükség lehet az ujjlenyomatunkra, de a netbankunkba való bejelentkezéshez is használhatjuk. Ezeket az adatokat tehát alapesetben nem használhatják fel a vállalatok, ám vannak kivételes helyzetek, amiket a következőkben megnézünk.

Összefoglalva tehát a különleges adatok az alábbi személyes adatok:



1. ábra: A különleges adat típusai

Forrás: saját szerkesztés (2011. évi CXII törvény, 2011) alapján

Az 1. ábra illusztrálja a különleges adat típusait, amely a jelenleg is érvényes 2011. évi CXII. törvényben található. Tilos kezelni tehát az etnikai hovatartozásra, a vallásra és a szexuális irányultságra vonatkozó adatokat, hiszen ezek mind-mind diszkriminációra adhatnak okot, amelyet az Európai Unió szeretne megakadályozni. A politikai nézetre és a szakszervezeti tagságra vonatkozó adatokat sem használhatják fel a vállalatok, így ilyen jellegű hirdetéseket sem kaphatunk az interneten.

² „genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;

³ biometrikus adat: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat (ujjlenyomat. (Britannica Inc., 1998.).” (2011. évi CXII törvény, 2011)

A telefonunkban a felsorolt adatok közül nagyon sokat tárolhatunk. A böngészési előzményeink illetve egyéb internetes tevékenységünk során sok minden kiderülhet rólunk és az érdeklődési körünkről. Az egészségügyi alkalmazásokban, -mint pl.: az EESZT-ben, megtalálható a kórtörténetünk, hogy milyen recepteket írtak fel nekünk, újabban a COVID oltással, tesztekkel kapcsolatos dokumentumaink, amiket le is tudunk tölteni. Ezen kívül egyes telefonok alkalmasak a pulzusunk, véroxigénszintünk mérésére, az újabbak már az alvásunkat is figyelik. De az okosóránk is megjegyzi a fizetési adatainkat, ha fizetünk vele, a helyadatokat, a pulzusunkat, mérheti a vérnyomásunkat, akár EKG-t is csinálhatunk a segítségével. Félelmetes belegondolni, hogy mennyi információja van rólunk az okoseszközeinknek, ám ezen egészségügyi adatok mérése sok esetben hasznos lehet, pl.: egy esetleges rosszullét esetén, hiszen a vérnyomásmérőnk nincs mindig nálunk. Egyes különleges adatokat csak kivételes esetekben használhatják fel a vállalatok, pl.: ha az érintett kifejezetten hozzájárul a kezeléshez, ha az érintett nyilvánosságra hozta ezen adatokat, ha az érintett vagy más természetes személy létfontosságú védelméhez szükséges (fizikai vagy jogi cselekvőképtelenség esetén), ha tudományos, történelmi kutatás céljából, népegészségügy területét érintő közérdekből (pl.: határon át terjedő egészségügyi veszélyek), jogi igények érvényesítéséhez, védelméhez. (GDPR, 2016.)

Ha a Facebook alkalmazásban a névjegyadatokban az alkalmazás lehetőségei ad nekünk, hogy megadjuk milyen neműek iránt érdeklődünk, milyen vallási és politikai nézeteink vannak. Ha ezeket nyilvánossá tesszük, felhasználhatják őket. A népegészségügyet érintő területre a jelenlegi járványt hozhatjuk fel példának. A COVID19 világjárvány kapcsán a mintavételt végző magánvállalatok kapcsolatban állnak az EESZT-vel és az esetleges pozitív teszteredmény esetén értesíteniük kell a rendőrséget is, hogy azok megtegyék a szükséges intézkedéseket. Külföldi helyen való hivatalos tesztelés során is értesítik a hatóságokat. A személyes adatok és a különleges adatok megismerését követően az adatvédelemhez szorosan kapcsolódó további fogalmakat is érdemes tisztáznunk, hiszen ezek meg fognak jelenni a dolgozat további részében.

A személyes adatokkal kapcsolatos műveletek elvégzését *adatkezelésnek* nevezzük. Az adatkezelő és az adatfeldolgozó meghatározása eltér. Az *adatkezelő* az, aki meghozza az adatkezelésre vonatkozó döntéseket, meghatározza az adatkezelés céljait és eszközeit. Az *adatfeldolgozó* ezeket a döntéseket az adatkezelő megbízásából végrehajtja. Az adatfeldolgozó a lényegesnek minősülő döntéseket nem hozhatja meg. A személyes adatok kezeléséről az

adatvédelmi nyilatkozat ad számunkra tájékoztatást. Ebben megtalálhatjuk például, hogy a vállalatok milyen adatokat tárolnak rólunk, meddig tárolják azokat és milyen célból. A dolgozat további fejezetében megnézzük, hogy ezeket az adatvédelmi tájékoztatókat milyen arányban olvassák el a felhasználók és mit tartalmaz a három óriásvállalat, azaz a Google a Facebook és a TikTok tájékoztatója.

Sajnos történhet olyan eset, - amitől talán kissé mindannyian tartunk -, hogy a személyes adataink elvesznek, vagy ellopják azokat. Ekkor *adatvédelmi incidensről* beszélünk. Az esetet az adatkezelő cégnek/szervezetnek jelentenie kell az adatvédelmi hatóságnak. Ha a magánélet védelmét komoly veszély fenyegeti a személyes adatok megsértése miatt, akkor az adatkezelő köteles tájékoztatni erről az egyént. Az adatkezelőnek az adatvédelmi incidenst 72 órán belül be kell jelentenie az adatvédelmi hatóságnak kivéve akkor, ha az nem jár kockázattal a természetes személy jogaira nézve. Az érintett is panaszt tehet vagy a bírósághoz keresetet nyújthat be az adott vállalat/szervezet ellen, ha úgy gondolja, hogy az adatvédelmi jogait megsértették. Ha anyagi kár keletkezik vagy nem vagyoni kárt szenved az egyén amiatt, mert a vállalat/szervezet nem tartotta be az uniós adatvédelmi szabályokat, akkor kártérítésre lehet jogosult. (Európai Unió, 2021.c) Az utóbbi években találkozhattunk a médiában néhány példával, amikor nagyvállalatokat több ezer euróra büntettek meg amiatt, mert nem kezelték megfelelően a személyes adatokat. A dolgozat 5. fejezetében, illetve a mellékletben pedig konkrét esetekről is olvashatunk (Európai Unió, 2018). De mi is az az *adatvédelmi hatóság*, ahová jelenthetjük az incidenseket? Az Európai Unió minden tagországában van a személyiségi jogok védelméért felelős hatóság. Magyarországon ez a NAIH, azaz Nemzeti Adatvédelmi és Információszabadság Hatóság. A NAIH feladata az információs jog védelme és a magyarországi adatkezelések törvényességének felügyelete (NAIH, 2021). Ahogy már korábban említettem, az utóbbi években elterjedt a személyes adatok üzleti célú gyűjtése. A *profilalkotás* segítségével a vállalatok már tudhatják rólunk, hogy milyen az érdeklődési körünk, ezáltal személyre szabott hirdetéseket jeleníthetnek meg számunkra. (Papp, 2018.). A boltokban általában a tulajdonos könnyen azonosítja a törzsvásárlókat és sokszor azt is tudhatja, hogy valaki csak nézelődni tér-e be vagy pedig valóban vásárolni szeretne. Ám a 90-es évek közepén a weboldalak még nem rendelkeztek olyan mechanizmussal, amely ezeket az információkat tudatja a weboldal üzemeltetőjével. A személyes adatok marketing célú felhasználásának témakörében az egyik legfontosabb fogalom a *cookie*, azaz a süti, hiszen a weboldalak ezeket használják fel ahhoz, hogy kövessenek minket. Bizonyára mindannyian találkoztunk már velük, hiszen a weboldal látogatásakor megjelenik egy ablak, hogy a

felhasználói élmények fokozása érdekében sűtíket használnak és a honlap használatával ezt elfogadjuk. Sok esetben választási lehetőséget kínálnak, hogy csak a weboldal működéséhez szükséges cookiekat engedjük-e telepíteni vagy a marketing cookiekat is elfogadjuk. A sűtikkel pontosan meghatározható a felhasználó honlaplátogatási története, szokásai, érdeklődési köre, hiszen a sűti képes a látogató bizonyos adatainak lekérdezésére és az internethasználatának követésére. (Origo.hu, 2020.). A felhasználók tevékenységét követik az interneten, amely alapján létre tudják hozni a felhasználói profilt és ebből adódóan célzott hirdetéseket jelenítenek meg. Amennyiben szeretnénk törölni a cookiekat, bármikor megtehetjük. (Európai Unió, 2021.c). Az általam vizsgált óriásvállalatok rengeteg adatot birtokolnak a felhasználókról, így ezek a platformok nagyon népszerűek a cégek körében, hiszen itt rengeteg embernek tudnak célzott hirdetéseket megjeleníteni a sűtik segítségével. A célzott hirdetés azt jelenti, hogy azzal, hogy követik a tevékenységeinket, a weboldalak felismerik az érdeklődési körünket és ahhoz kapcsolódó hirdetéseket jelenítenek meg. Ennek köszönhetően, a vállalatok nagyobb bevételre tehetnek szert és olyan felhasználóhoz juttathatják el a hirdetéseiket, akiket nagyobb valószínűséggel érdekelhet a termékük/szolgáltatásuk. A hirdetésekhez viszont együtt kell működni a különböző weboldalnak, hírportáloknak, közösségi oldalaknak, hiszen a sűtik csak az adott weboldalról gyűjtik be az adatokat. A későbbiekben azt is megnézzük, hogy mekkora bevételt generálnak a reklámok az óriásvállalatoknak.

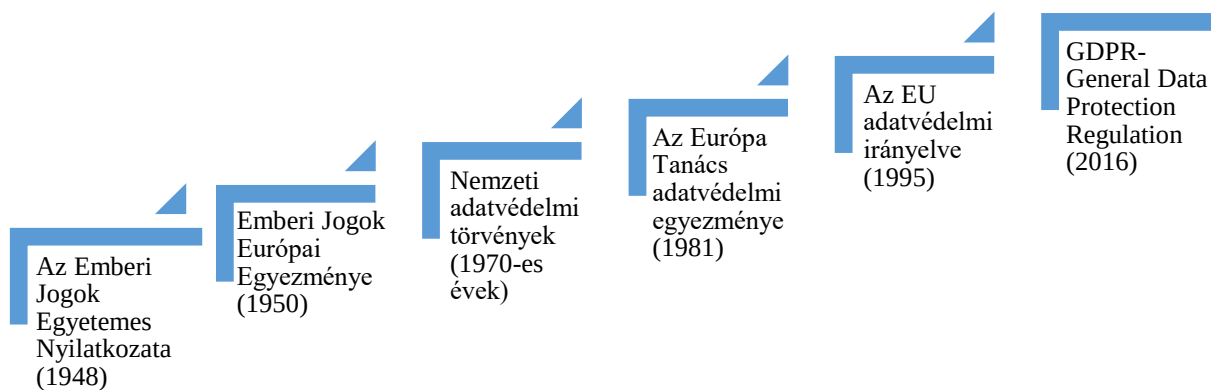
Láthatjuk, hogy az egyre elterjedtebb adatgyűjtés következtébe egyre nagyobb szükség van az adataink védelmére és arra, hogy szabályozzák azok felhasználását. A következő fejezetben megnézzük, hogy hogyan is alakult ki az adatvédelem és jelenleg milyen szabályozás vonatkozik rá.

3. A SZEMÉLYES ADATOK SZABÁLYOZÁSI KÖRNYEZETE

Ebben a fejezetben bemutatom az adatvédelem kialakulását és részletesen megnézzük a személyes adatok szabályozási környezetét az Európai Unión belül. Az Európai Unió kutatásait felhasználva szemléltetem az adatfelhasználási szabályokat és a személyiségi jogokat.

3.1 AZ ADATVÉDELEM KIALAKULÁSA EURÓPÁBAN

Hogyan kapcsolódik a személyes adat az adatvédelemhez? Az adatvédelem a személyes adatok jogszerű kezelését jelenti. Ezen kívül az érintett személyek, -azaz egy adott gazdasági társasággal kapcsolatba kerülő, bármely információ alapján azonosítható természetes személyek- védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége. (NAIH, 2021). Már a XX. század közepén megjelent a magánélet védelmének szükségessége, ám az évek során egyre indokoltabbá vált a személyes adatok gyűjtésének, tárolásának és felhasználásának szabályozása. Ebben a fejezetben megvizsgáljuk, hogyan alakult ki az adatvédelem az Európai Unióban illetve Magyarországon, és, mikor milyen szabályozás vonatkozott az adatok védelmére. Ha megnézzük az Európai Unió adatvédelmi szabályozás fejlődéstörténetét, láthatjuk, hogy a jelenleg is érvényben lévő GDPR, azaz az *általános adatvédelmi rendelet*⁴ előtt már számos törvény kapcsolódott az adatok védelméhez.



2. ábra: Európai Unió adatvédelmi szabályozás fejlődéstörténete

Forrás: saját szerkesztés (Európai Unió, 2021.) alapján

⁴ GDPR: „Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről” (GDPR, 2016.)

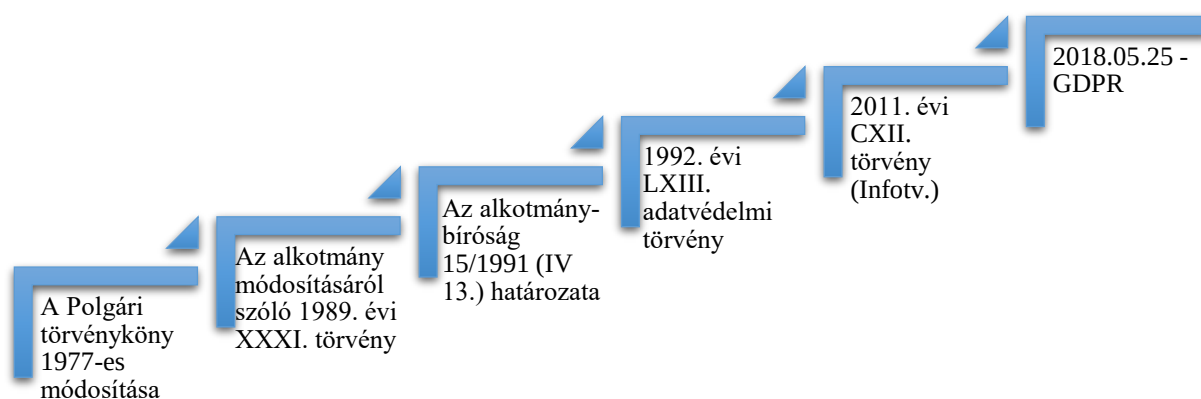
Az ENSZ által 1948-ban kiadott Emberi Jogok Egyetemes Nyilatkozata mérföldkőnek számított az adatvédelem tekintetében. A nyilatkozat 12. cikkében a magánélet védelme a következő képpen jelent meg: *„Senkinek magánéletébe, családi ügyeibe, otthonába vagy levelezésébe nem szabad önkényesen beavatkozni, sem pedig becsületében vagy jó hírnevében megsérteni. Minden személynek joga van az ilyen beavatkozásokkal vagy sértésekkel szemben a törvény védelméhez.”* (Council of Europe, 2022.). Ekkor még adatvédelmi szabályokat nem hoztak meg, de ahogyan olvashattuk, már említésre került a levelezés védelme. Az Emberi Jogok Egyetemes Nyilatkozatának mintájára hozta létre az Európai Unió az Emberi Jogok Európai Egyezményét 1950-ben. Amely ország aláírta, az kötelezettséget vállalt az emberi jogok tiszteletben tartására. Ebben a dokumentumban is említésre került az emberek levelezésének tiszteletben tartása: *„Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák.”* (Európai Tanács, 1950.). Nem véletlen, hogy az adatvédelem a XX. század közepén a levelezés védelmével kezdődött. Manapság, az online térben is azon legfontosabb dolgok közé tartozik az e-mailezésünk, amelyet nem szeretnénk, hogy nyilvánosságra kerüljön. Esetenként az üzenetekben számos személyes információ megtalálható, olyan dokumentumokat is küldhetünk/ kaphatunk, amelyek szintén csak ránk és a levelezési partnerünkre tartoznak. Példaként egy szállásfoglalást említenék, amikor előfordulhat, hogy a foglalás megerősítéséhez el kell küldenünk a bankkártya adatainkat. Ugye senki nem szeretné, hogy ez nyilvánosságra kerüljön?

Az 1960-as évek környékén eljutott a számítástechnika olyan szintre, hogy megjelent az adatok elektronikus tárolásának a lehetősége, amely egyre inkább kiteljesedett az évek során. A technológia fejlődése miatt hamar felmerült a kérdés, hogy vajon milyen hatással lesz az adatfeldolgozás és az adatok tárolása a magánszférára. Ennek következtében az 1970-es években több adatvédelmi törvény is létrejött. Az 1980-as években elterjedt a személyi számítógép és megszülettek az első nemzetközi jogi dokumentumok, amelyek a magánélet védelméről és a személyes adatok határokon átvitelő áramlásáról szólnak, ám ezeknek még nem volt kötelező erejük. 1981-ben az Európai Tanács kiadta az első kötelező erejű, nemzetközi szintű adatvédelmi dokumentumot, amelyben már külön szerepel a személyes adatok védelméhez való jog. Az egyezmény célja, hogy: *„... minden egyén számára biztosítva legyen, hogy jogait és alapvető szabadságjogait, különösen a magánélethez való jogát tiszteletben tartsák személyes adatainak gépi feldolgozása során...”* (Európai Tanács, 1981.). Ezt követően, 1995-ben egy újabb dokumentumot adtak ki, mégpedig az Európai Unió adatvédelmi irányelvét, amely megteremtette az egységes Uniós szabályozás alapjait, hiszen ezt az

irányelvet minden tagállamnak el kellett sajátítani. Mivel az évek alatt folyamatosan nőtt a feldolgozott és tárolt adatok mennyisége, valamint a határon átnyúló adatáramlás, így egy részletesebb irányelvre volt szükség. Ahogyan már említettem az utóbbi 20-25 évben megváltozott az internet használata. Sokan kezdtek el tartalmat gyártani és ezeket meg is osztották másokkal az online térben. Ezáltal, ha a felhasználók olyan adatokat osztottak meg, amelyben mások személyes adatai is nyilvánosságra kerültek, adatkezelővé váltak. Továbbá a személyes adatok kapcsán megjelent a profilozás, ami nagy üzleti lehetőség a vállalatok számára. A cégek törekednek a felhasználók személyes adatainak begyűjtésére, a tevékenységeiket követve direktmarketing eszközöket (pl.: viselkedésmarketing) alkalmaznak. (Szőke, 2013.) Az Európai Unió úgy döntött, hogy újabb szabályozást készít. 2016-ban elfogadásra került a GDPR, azaz az új általános adatvédelmi rendelet, amelyről részletesebben a későbbiekben olvashatunk.

Az adatvédelem kialakulása Magyarországon

Ahogy Európa többi részén, Magyarországon is a 20. század második felére tehető az adatvédelmi szabályozás kialakulásának kezdete.



3. ábra: Magyarország adatvédelmi szabályozás fejlődéstörténete

Forrás: saját szerkesztés. ” (1977. évi IV. törvény, 1977), (1989. évi XXXI. törvény, 1989.), (15/1991. (IV. 13.) AB határozat, 1991), (1992. évi LXIII. törvény, 1992), (2011. évi CXII törvény, 2011) alapján

Hazánkban az adatvédelem területén az egyik legfontosabb mérföldkő a Polgári Törvénykönyv 1977-es módosítása. Ebben a módosításban már konkrétan megjelenik az elektronikus adatfeldolgozással kapcsolatos személyes jogok védelme: „A számítógéppel történő adatfeldolgozás nem sértheti a személyhez fűződő jogokat.” (1977. évi IV. törvény, 1977)⁵

⁵ A 1977. évi IV. törvény 2007. július 1-jétől hatálytalan.

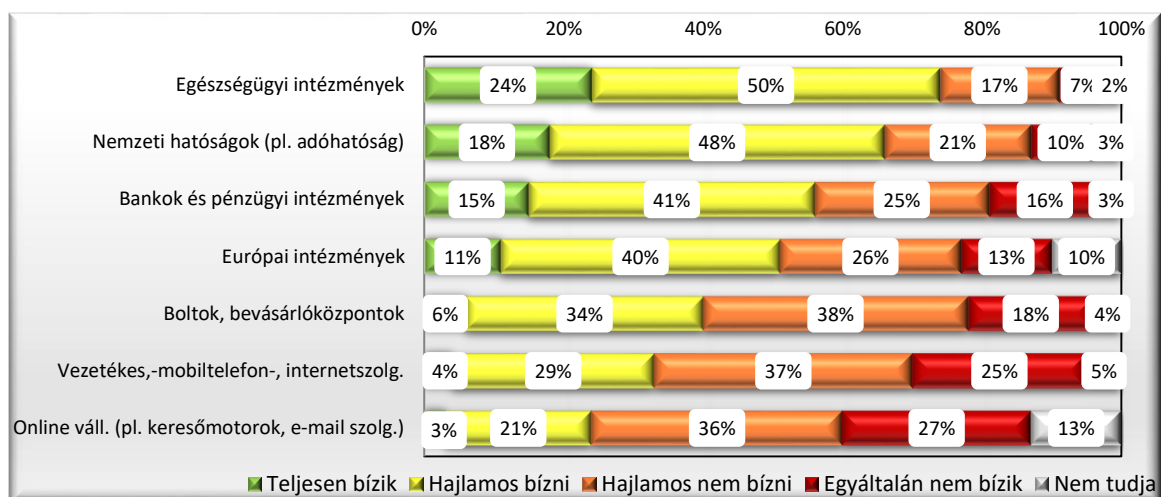
Magyarországon az Alkotmány módosításáról szóló 1989. évi XXXI. törvény⁶ határozta meg elsőként alapvető emberi jogként a személyes adatok védelmét: „*A Magyar Köztársaságban mindenkit megillet a jóhírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog.*” (1989. évi XXXI. törvény, 1989.), Mivel a korábbi rendelkezések egy része sértette a személyes adatok védelméhez való jogot, az Alkotmánybíróság 15/1991. (IV. 13.) AB határozata megsemmisítette azokat. Ez a határozat fontos mérföldkő a magyar adatvédelmi szabályozás terén, hiszen számos olyan jogintézményt teremtett meg a személyes adatok védelmével kapcsolatban, amely jelenleg is fontos alapja az adatvédelmi szabályozásnak. Ilyen például az adatkezelés célhoz kötöttsége. A határozatban a következő áll: „*Az Alkotmánybíróság megállapítja, hogy személyes adatok meghatározott cél nélküli, tetszőleges jövőbeni felhasználásra való gyűjtése és feldolgozása alkotmányellenes.*” (15/1991. (IV. 13.) AB határozat, 1991) Az 1991-es határozatban tehát már megjelenik, hogy csakis akkor gyűjthető és dolgozható fel a személyes adat, ha azt meghatározott céllal teszik. Hazánkban az első adatvédelmi törvény az 1992. évi LXIII. a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvény, amelyet a következő fejezetben részletesebben meg fogunk nézni. A törvényben már egyértelműen meg van határozva a személyes adat fogalma. (1992. évi LXIII. törvény, 1992) Ezt a törvényt a 2011. évi CXII. törvény váltotta fel, amely az információs önrendelkezési jogról és a közérdekű adatok nyilvánosságáról szól. A törvényt röviden Infotv-nek nevezzük. Az Infotv. kiegészítette és pontosította az adatvédelmi szabályokat és létrehozta a Nemzeti Adatvédelmi és Információszabadság Hatóságot (NAIH). A NAIH egy autonóm közigazgatási szerv, melynek célja a személyes adatok védelme és az információszabadság érvényesülése. (2011. évi CXII törvény, 2011) A Hatóságról a későbbiekben részletesebben olvashatunk. Magyarországon jelenleg is az Infotv. szabályozza a személyes adatok védelmét, ám ez a törvény is módosításra került a GDPR bevezetésével, amely még részletesebbé tette azt. Most pedig nézzük meg, hogy a jelenlegi GDPR hogyan szabályozza az adatvédelmet.

⁶ Az 1989. évi XXXI. törvény 2012. január 1-jétől hatálytalan.

3.2 ADATVÉDELEM AZ EURÓPAI UNIÓBAN

Ahogy már említettem, a felhasznált adatok mennyisége folyamatosan nő, emiatt pedig nő annak a kockázata is, hogy az adataink illetéktelenek kezébe kerülnek. Az Európai Parlament kiemelten fontosnak tartja, hogy legyen egy egységes általános rendelet, amely szabályozza a vállalatokat. Ahogy az előző fejezetben is láthattuk, jelenleg a GDPR, vagyis az Európai Unió általános adatvédelmi rendelete határozza meg a személyes adatok kezelését. A közel 100 oldalas rendelet a 2 éves türelmi időszakot követően 2018. május 25-én lépett hatályba.⁷ (European Union, 2018). A GDPR az Európai Unió területén működő vállalatokra vonatkozik, illetve azon EU területén kívül működő cégekre, amelyek árut értékesítenek vagy szolgáltatást nyújtanak az EU-n belül. (ProfiNet, 2019.) A rendelet védi a személyes adatokat, csökkenti a visszaélések és a magánélet megsértésének kockázatát. A szabályzat miatt a szervezeteknek nagyobb körültekintéssel kell kezelni az adatokat, ezzel csökkenti azok helytelen használatának kockázatát, amellyel erősíti a bizalmat. (Donegan, 2019.) A GDPR célja az, hogy irányítsa az adatok felhasználását, növelje a bizalmat, ösztönözze az adatok az adatvédelmi előírásoknak megfelelő megosztását, illetve újrafelhasználását, valamint biztosítsa az egyének saját személyes adatainak ellenőrzését. Nézzük meg milyen volt a bizalom a GDPR bevezetését megelőzően. Az Európai Bizottság a GDPR bevezetése előtti, 2015-ben adatvédelemmel (Data Protection) kapcsolatos felmérést végzett (Eurobarometer 431). Az EU 28 tagállamában összesen 27 980 embert kérdeztek meg, jellemzően 1000 fős mintanagysággal országonként. A kutatás szerint az Európai Unió fogyasztóinak 71%-a egyetértett azzal, hogy a személyes adatok megadása egyre inkább része a modern életnek. 58%-uk úgy vélte, hogy nincs más választása, minthogy megadja a személyes adatait annak érdekében, hogy szert tegyen az egyes ingyenes szolgáltatásokra. A válaszadók 57%-a egyáltalán nem értett egyet azzal az állítással, hogy „nem gond számára a személyes adatai megadása”. (European Commission, 2015.) Ezen eredmények alapján tehát, a fogyasztók több mint fele számára gondot jelentett a személyes adatainak közlése. A 2015-ös felmérésből az is kiderült, hogy 10 fogyasztóból 8 úgy érezte, hogy nincs teljes irányítása a személyes adatai fölött, és kétharmadukat nem is zavarta ez. Nézzük meg, hogy az egyes intézményekben/vállalatokban milyen arányban bíztak a válaszadók 3 évvel a GDPR hatálybalépését megelőzően:

⁷ Főbb fejezetei közé tartozik: *Az érintett jogai, Az adatkezelő és adatfeldolgozó, a Személyes adatok harmadik országba vagy nemzetközi szervezetek részére történő továbbítása, a Független felügyeleti hatóságok, az Együttműködés és egységesség, a Jogorvoslat felelősség és szankciók és Az adatkezelés különös eseteire vonatkozó rendelkezések* (European Union, 2018).



4. ábra: Az intézmények/vállalatok adatvédelmébe vetett bizalom (EU28; 2015)

Forrás: saját szerkesztés (European Commission, 2015.) alapján

Az Eurobarometer 431 felmérésében megkérdezték a résztvevőket, hogy milyen mértékben bíznak abban, hogy a felsorolt hatóságok és vállalatok megvédik a személyes adatait. A fogyasztók leginkább az egészségügyi intézményekben és a nemzeti hatóságokban bíztak meg a személyes adataik védelmét illetően. Kevesebb, mint a válaszadók fele bízott meg a boltok, bevásárlóközpontok és a vezetékes,- mobiltelefon, internetszolgáltatók adatvédelmében. A felmérésben résztvevők mindössze 24%-a bíz meg az online vállalatokban. A résztvevők 27%-a egyáltalán nem bízott abban, hogy ezek a vállalatok megvédik az adataikat. Láthatjuk, hogy 2015-ben az online cégeknek szolgáltatott személyes adatok védelme iránti bizalom rendkívül alacsony volt. A legtöbben, - a felmérésben résztvevők fele- attól félt, hogy az adataik megadásával csalás áldozatai lesznek. Szintén sokan (40%) tartottak attól, hogy a személyazonosságukat csalásra használják fel. A válaszadók közel 1/3 része kockázatosnak tartotta megadni a személyes adatait, mert úgy gondolták, hogy felhasználhatják a tudtuk nélkül vagy ellophatják azokat. (European Commission, 2015.)

Az Európai Unió 2019-es GDPR-ral kapcsolatos kutatásában összesen 27 524 fő vett részt az Unió különböző tagállamaiból. A válaszadók 1/3-a a felmérés időpontjában, 2019 márciusában, közel 1 évvel a hatálybalépést követően még nem is hallottak a GDPR-ról. Azok közül, akik hallottak, közel a fele nem tudta pontosan, hogy mi az. Ez az arány meglepően kevés. Hatalmas szakadék volt az egyes országok között. Olaszországban a megkérdezettek mindössze 17%-a válaszolta azt, hogy pontosan tudja mi az a GDPR, míg Svédországban 63% nyilatkozta ezt. Magyarország a 25%-os eredményével messze az Uniós (37%) átlag alatt helyezkedett el. (European Commission, 2019.)

Néhány Európai Unió kívüli ország szabályzata a *9.1 mellékletben* található.

Adatfelhasználási szabályok és személyiségi jogok

A vállalatoknak számos fontos szabályt kell betartaniuk a személyes adatok felhasználásával és tárolásával kapcsolatban, amiről az érintettnek joga van tudni, így ezeket szerepeltetni kell az adatvédelmi nyilatkozatban/általános szerződési feltételekben.



5. ábra: Adatfelhasználási szabályok

Forrás: saját szerkesztés (Európai Bizottság, 2021.b) alapján

Jogszerűen és átláthatóan kell kezelni a személyes adatokat és biztosítani kell a *tisztességes adatkezelést*. A személyes adat gyűjtésének időpontjában közölni kell az érintettel a személyes adatok kezelésének *célját*, nem lehet adatokat gyűjteni meghatározatlan célra és a személyes adatokat nem használhatják fel az eredeti adatgyűjtés céljával nem összeegyeztethető célra. A személyes adatokat csak a meghatározott cél eléréséhez szükséges ideig tárolhatják, ez a *korlátozott tárolhatóság* elve. Csakis a cél teljesítéséhez szükséges adatokat lehet gyűjteni/kezelni, ezt nevezzük *adattakarékosságnak*. A személyes adatoknak *pontosnak* és *naprakésznek* kell lenniük. Az *integritás és bizalmas jelleg* azt jelenti, hogy úgy kell kezelni a személyes adatokat, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága (Európai Bizottság, 2021.b). Az alkalmazások használatához és a weboldalak látogatásához hozzá kell járulnunk az adataink kezeléséhez. GDPR szerint az adatkezelési hozzájárulás akkor jogszerű, ha az érintett személy megfelelően tud tájékozódni adatainak kezeléséről. Az adatkezelőnek tájékoztatnia kell az adott személyeket, hogy milyen adatokat kezel, kik láthatják ezeket az adatokat, ki az adatkezelő és ki az adatfeldolgozó, mi a célja és időtartama az adatok kezelésének, és ha adattovábbításra kerül sok, akkor erről is értesíteni kell. (Reklamjog.hu, 2021.) A későbbiekben megnézzük, hogy az általam vizsgált óriásvállalatok tudatják-e ezeket az információkat az adatvédelmi dokumentumaikban. Az érintett személynek tisztában kell lennie, hogy pontosan mihez is járul hozzá. Az adatok tulajdonosainak a világos és közérthető nyelven megfogalmazott kérdésekre önkéntes, konkrét, egyértelmű hozzájárulást kell adnia. (Európai Unió, 2021.b) Amennyiben az adott cég nem kap választ arra, hogy hozzájárul-e a felhasználó a felsorolt pontokhoz, akkor az

alapesetből kell kiindulni, vagyis, hogy az adott személy nem kíván marketingüzeneteket kapni. (Európai Bizottság, 2021.b). A következő infografikán megtekinthetjük a személyiségi jogokat.



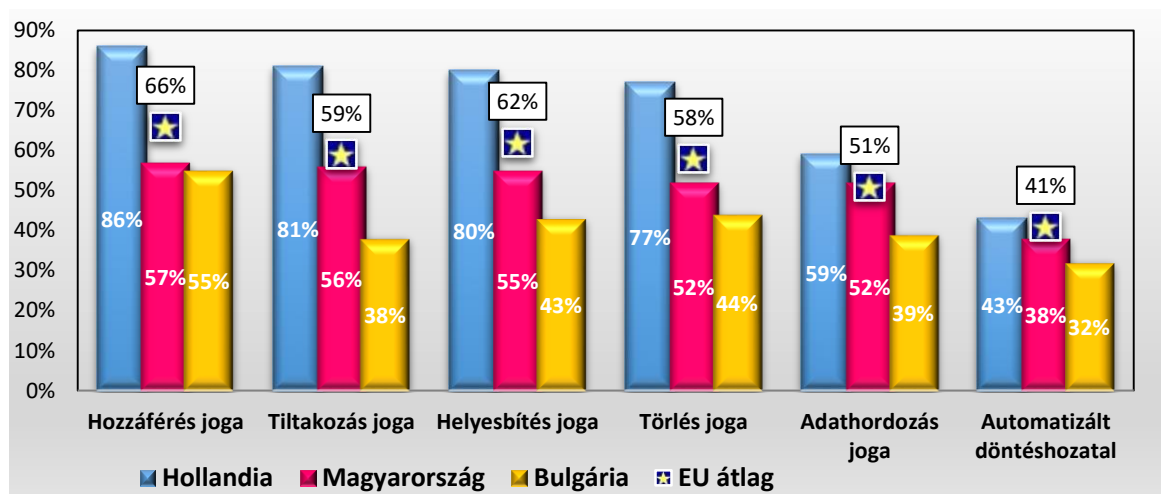
1. Infografika: Személyiségi jogok

Forrás: saját szerkesztés (DPMK, 2018.) alapján

Az egyéneknek jogában áll *hozzáférni* a saját személyes adataihoz. Ehhez fel kell vennie a kapcsolatot a céggel, amelynek 1 hónapon belül választ kell adnia és rendelkezésre kell bocsátani a személyes adatok másolatát és minden információt arról, hogy hogyan használták, illetve használják fel a megadott adatokat. Amennyiben az egyén úgy dönt, hogy habár korábban már beleegyezett a személyes adatok felhasználásába, de meggondolta magát, akkor bármikor visszavonhatja a beleegyezést, ezt követően már nem használhatják fel az adatait. Habár az adatok kezelése ellen tiltakozhat és kérheti az adatkezelés megszüntetését vagy azt, hogy ne használják fel az adatait direkt marketing célra, amennyiben a személyes adatokat tudományos kutatáshoz, statisztikai nyilvántartás céljából vagy hivatalos hatósági eljáráshoz használnák fel, akkor a tiltakozás ellenére is megtehetik. Ha az érintett észreveszi, hogy a személyes adatai helytelenül kerültek megadásra, kérheti a *helyesbítést*. Néhány esetben kérheti az adatait nyilvántartó vállalatától/szervezettől, hogy szolgáltatassa vissza vagy továbbítsa az adatait egy másik vállalatnak, ezt nevezzük *adathordozhatósághoz való jognak*. Abban az esetben kérheti az érintett az adatai törlését, ha már nincs szükség az adatokra, vagy ha azokat jogsértően használják fel. Ezt *törléshez való jognak* nevezzük. Ha egy vállalat más honlapoknak is továbbította a személyes adatokat, akkor őket is tájékoztatni kell az egyén kéréséről. (DPMK,

2018.) A *feldolgozás korlátozása* azt jelenti, hogy az adataik megmaradnak a nyilvántartásban, de az érintett kérheti, hogy ne kerüljenek feldolgozásra. A felhasználóknak lehetőséget kell biztosítani arra, hogy eldönthessék, hogy engedélyezik-e az *automatizált döntéshozatalt*. Amennyiben ez a döntéshozatal jogi előírásen alapszik, úgy a cégnek kötelessége tájékoztatni az érintettet az automatikus döntéshozatalról és biztosítani kell a lehetőséget arra, hogy tiltakozzon ezellen és emberi beavatkozást kérjen. (Európai Unió, 2021.b)

A 2019-es Eurobarometer felmérésben megnézték, hogy a résztvevők milyen aránya hallott a jogokról. Arra nem terjedt ki a vizsgálat, hogy tudják-e pontosan a jogok jelentését, csak azt kérdezték, hogy hallottak-e már azokról. A felmérésben 6 jogot vizsgáltak:



6. ábra: A GDPR által biztosított jogok ismerete (2019)

Forrás: saját szerkesztés (European Commission, 2019.) alapján

A 6. ábra Magyarország, Hollandia és Bulgária, valamint az Európai Unió (EU27) eredményeit szemlélteti. A hazai helyzet szemléltetése során azért Hollandiát és Bulgáriát emeltem ki, mert a két szélsőséges eredményeket szerettem volna bemutatni. A 6 jog közül a legismertebb a hozzáférés joga volt, ez a legtöbb országban az első helyen állt. Hollandiában az emberek 86%-a hallott már róla. Habár Bulgáriában is ezt a jogot ismerték a legtöbben, itt csak az emberek 55 %-a hallott már róla, az EU 65%-os átlaggal szemben. Az EU átlagot Magyarország csak egy jog ismeretében, az adathordozáshoz való jog esetén érte el. A legkevésbé ismert jog minden országban az automatizált döntéshozatal volt. A legismertebb jogról a válaszadók 1/3 része nem is hallott. A résztvevők 73 %-a felsoroltak közül legalább 1-ről hallott már és mindössze 30% az, aki mindegyikről. Írország kiemelkedő abban a tekintetben, hogy ott több mint a fogyasztók 50%-a hallott az összes jogról. Magyarországon ez az arány 29%.

Az Eurostat 2021-es kutatása szerint, az Unióban lakók mindössze 9%-a kérte már a weboldalak adminisztrátorát, hogy töröljék vagy frissítsék a személyes adataikat (Eurostat, 2021.c).

4. SZEMÉLYES ADATAINK NYOMÁBAN

Az előző fejezetben megnéztük a személyes adatok szabályozási környezetét, most pedig nézzük meg, hogy a konkrét vállalatok esetében ez hogyan történik. A személyes adataink megadása során fontos a bizalom, a gyanús weboldallal, e-mailekkel vigyáznunk kell, csak azokkal érdemes kapcsolatba kerülni, amelyekben megbízunk, hiszen a személyes információnk a tét. Adatainkat életünk több területén is kérhetik tőlünk. Például bevásárlás során. Amennyiben igényt tartunk rá, a nagyobb szupermarketekben igényelhetünk pontgyűjtőkártyákat, törzsvásárlói kártyát, amelyekkel akciókra tehetünk szert, a személyes adatainkért cserébe. Vannak olyan áruházak, például a TESCO, amelyek az alapján küldenek nekünk kuponokat, hogy egy adott időszakban melyik termékeket vásároltuk a leggyakrabban, így próbálnak biztosra menni, hogy legközelebb is ott bonyolítsuk le a bevásárlást. Ennek az az ára, hogy elfogadjuk, hogy tudják, hogy pontosan mikor, milyen gyakorisággal és milyen termékeket vásárolunk. Ezen kívül általában a nevünket, születési adatainkat, lakcímünket és e-mail címünket is kéri a regisztráció során. Egy másik példa: amennyiben bankkártyát használunk, a bankban dolgozók láthatják a fizetésünket és hogy mikor, hol, mennyi pénzt költünk. Hitelfelvétel esetén még több adatot vizsgálnak. Habár a titoktartás kötelező a bankban dolgozóknál is, sosem lehetünk biztosak benne, hogy valóban nem adják tovább az információkat. Ám a kényelem érdekében a legtöbben bevállaljuk ezt a kockázatot.

A személyes adatainkat egyre több helyen adjuk meg az online térben is, például egy online vásárlás kapcsán vagy a közösségi médiák használatán keresztül. Az online vásárlás és a közösségi médiában való részvétel évről évre gyakoribbá válik. Az Európai Unió 2019-es kutatása szerint, ahol a válaszadók száma 23 106 fő volt, az internetezők mindössze 18 %-a nem használt még közösségi hálót. Az internetet használók 77 %-a szokott online vásárolni.. (European Commission, 2019.) 2021-ben a kiskereskedelmi online értékesítés összege világszerte közel 5 000 milliárd dollár volt. Ez az adat 5 évvel ezelőtt, 2016-ban még a 2 milliárd dollárt sem érte el (Chevalier, 2022.). 2018-ban egy átlagos okostelefonon 60-90 db alkalmazás volt található. A legnépszerűbb Android-alkalmazások 45%-a, míg a legnépszerűbb iOS-alkalmazások 25%-a kér engedélyt például a helyadatokhoz való hozzáféréshez. Hasonló százalékban kérnek a kamerához is hozzáférést. (Cleary, 2018.) 2021-ben világszerte 230 milliárd alkalmazást töltöttek le. (Statista.com, 2022. b)



2. Infografika: Az alkalmazások által gyakran gyűjtött adatok

Forrás: saját szerkesztés

Amikor letöltünk a telefonunkra egy-egy alkalmazást, a telepítést követően, az alkalmazás használata előtt több kérdéssel is találkozhatunk. Tapasztalataim szerint az applikációk legtöbbször az infografikán felsorolt adatokhoz kérnek hozzáférést. Előfordul olyan eset, hogy ha elutasítjuk ezeket, az alkalmazás használata korlátozottá válik vagy akár meg is hiúsul. A begyűjtött adatokra legtöbbször találunk magyarázatot, hiszen például a képszerkesztőknek hozzá kell férnie a telefonon található képeinkhez annak érdekében, hogy meg tudjuk szerkeszteni azokat. A Térkép alkalmazások hozzáférést kérhetnek az egészséggel kapcsolatos adatainkhoz, hiszen a lépésszámláló segítségével meg tudják állapítani, hogy egy adott távolságot gyalogosan tettünk-e meg, a Vibernek hozzá kell férnie a névjegyekhez, hogy használni tudjuk. Sok minden összefügg. Azonban egyes applikációk sokszor olyanok adatokat szeretnének gyűjteni, amelyeket nem tudjuk összefüggésbe hozni az alkalmazás céljával. 2020-ban az Akamai kutatás szerint a résztvevők 15%-a biztosan, 54%-a pedig valószínűnek tartja, hogy eláll egy olyan üzlettől, ahol túlságosan sok személyes adatot kérnek. Sokan az összes

engedélykérést olvasás nélkül, automatikusan elfogadják és bele sem gondolnak, mi oka van az alkalmazásnak ezen adatok gyűjtésére.

Az Apple 2020 júniusában egy új adatvédelmi szakaszt jelentetett meg az App Storeban. A fejlesztő megadja azokat az információkat, amelyeket az alkalmazás begyűjt rólunk, amelyből címkéket készítenek. Célja az, hogy megkönnyítse a fogyasztók számára, hogy átlássák, milyen adatokat gyűjtenek be az egyes applikációk róluk. (Apple, 2022.) A személyes adatokat 14 kategóriába sorolták, amelyek között volt pl.: a tartózkodási hely, a böngészési előzmények, kapcsolattartási adatok, pénzügyi adatok, egészségügyi adatok. Ezen adatvédelmi címkék segítségével a pCloud felhőszolgáltató elemzést végzett a népszerű alkalmazások körében arról, hogy melyek osztanak meg adatokat harmadik felekkel hirdetési célból. Első helyen az Instagram végzett, amely a 14 kategóriából 11 kategóriában oszt meg adatokat. A második helyen a Facebook található. A Facebook az adatok 57%-át osztja meg harmadik féllel. Az Instagram a Facebookkal ellentétben a keresési és böngészési előzményeket, azonosítókat és a felhasználói adatokat is megosztja másokkal. (Felix, 2021.) A Facebook és az Instagram begyűjti a névjegyeket és a kontaktok adatait, egészségügyi adatokat, pénzügyi adatokat, helyadatokat, érzékeny információkat, felhasználói tartalmat, keresési előzményeket, böngészési előzményeket, azonosítókat, vásárlásokat, használati adatokat, diagnosztikai adatokat. Általánosságban elmondható, hogy minél népszerűbb egy alkalmazás, annál több adatot gyűjt be. (Cohen, 2022. a) Azonban vannak olyan applikációk, amelyek nem követik nyomon a személyes adatokat. Ilyen például a Signal, a Netflix, a Microsoft Teams, a Skype és a Zoom is. (Cohen, 2021. b)

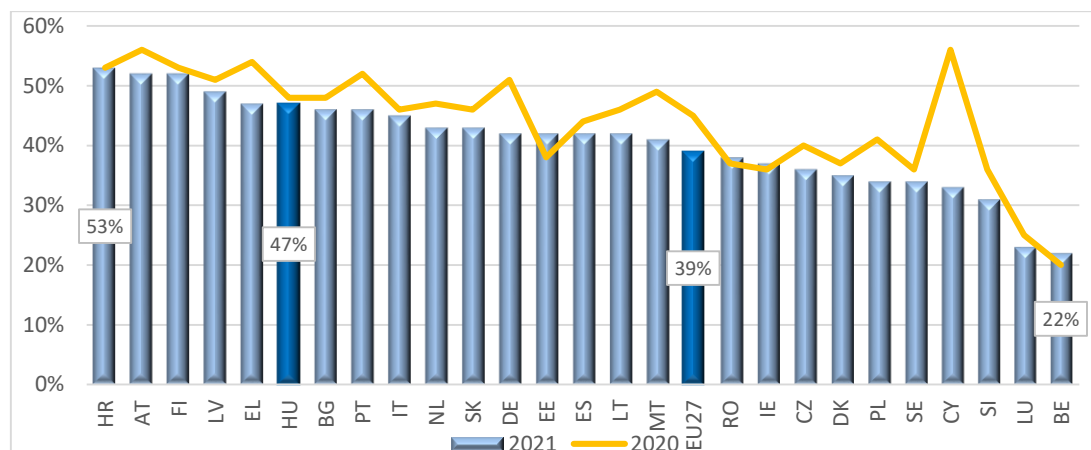
Kevés olyan embert ismerünk a környezetünkben, aki nem használja a Google keresőmotort vagy a Facebook nevű közösségi hálózatot és mára a TikTok alkalmazás is népszerű lett. A Google a leggyakrabban használt keresőmotorok között magasan az első helyen áll. A világszintű részesedése az asztali számítógépen az elmúlt 12 évben 85% és 90% közötti volt. (Johnson, 2022. b) A Facebook 2021 negyedik negyedévében a havi aktív felhasználók száma közel 3 milliárdra tehető. (Statista, 2022. c). A három vállalat a felhasználókról rengeteg adatot begyűjt, amely alapján egy úgy nevezett profilt hoznak létre rólunk. Ehhez persze mindannyian hozzájárultunk azzal, hogy regisztráltunk és elfogadtuk a felhasználási feltételeket. De valljuk be őszintén, végig olvastuk valaha azokat? A vállalatok a rólunk tárolt adatok segítségével már egyszerűen tudnak személyre szabott tartalmakat és hirdetéseket megjeleníteni. Az egyes cégek a személyes adataink felhasználásával olyanokhoz tudják eljuttatni a hirdetéseiket, akiket nagy

valószínűséggel valóban érdekelhet a termékük vagy a szolgáltatásuk, így a személyre szabott reklámokkal jóval nagyobb bevételre tehetnek szert, mint korábban. A Facebook, hasonlóan a többi népszerű alkalmazáshoz, azon dolgozik, hogy minél többen és minél gyakrabban használják az alkalmazást, ezzel minél több reakció legyen és minél több funkciót kihasználjanak. Ekkor ők egyre pontosabb profilt tudnak rólunk létrehozni, amivel egyre inkább számunkra releváns hirdetéseket tudnak megjeleníteni. (Social dilemma, 2020.) A számok azt mutatják, hogy ezt nagyon jól csinálják, hiszen a Facebook Inc.,- új nevén a Meta- 2021-ban közel 115 000 millió dollár árbevételre tett szert a reklámokból. (Statista, 2022.) A TikTok és a Google számára is a fő bevételi forrás a hirdetések. A Google például még a Metától is jóval magasabb bevételt gyűjtött a reklámokból: 2021-ben közel 210 milliárd dollárt. (Johnson, 2022.) A Netflix saját gyártású *Social dilemma*, azaz magyar címén a *Társadalmi dilemma* című dokumentumfilmjében több olyan ember megszólal, akik évekkel ezelőtt a Facebook-nál, Google-nél, Youtube-nál, Instagram-nál és egyéb hasonlóan híres és sikeres cégnél dolgoztak. A film a közösségi oldalak és a keresőmotorok árnyoldalát mutatja be. Meghökkenítő. Érdekes hallani, hogy amit csak sejtünk, valóban igaz: tényleg szinte mindent tudnak rólunk. Tudják, hogy melyik képeket nézzük meg például a Facebookon és mennyi ideig nézzük azokat, hiszen ha sokáig, akkor arra tudnak következtetni, hogy jobban érdekel minket, mint amit gyorsan átlapozunk. Tudják, hogy kikkel vagyunk kapcsolatban, milyen a jelenlegi hangulatunk. Egyre jobban képesek felismerni, hogy mit fogunk tenni, kik vagyunk. Olyan modelleket alkotnak, amelyek alapján megjósolják a viselkedésünket. Minden egyes tevékenységünket arra használják fel, hogy minél pontosabb modellt tudjanak alkotni. Ezek az alkalmazások versengenek a figyelmünkért és addiktívvá tesznek minket. A vállalatok nagyobb bevételre tesznek szert, ha több időt töltünk pl.: a Facebookon, akkor többször/hamarabb láthatjuk a célzott hirdetéseket. A filmben azt nyilatkozzák a szereplők, hogy amikor évekkel ezelőtt híressé váltak az említett weboldalak, még úgy gondolták, hogy azok fejlesztésével jót tesznek az embereknek. Ma viszont már nem tartják etikusnak. „*Ha nem fizetsz egy termékért, akkor te vagy a termék.*” hangzik el a dokumentumfilmben. A kijelentés nagyon elgondolkodtató és mióta először meghallottam, gyakran jut eszembe böngészés közben. (Social dilemma, 2020.)

A népszerűségüknek köszönhetően a három (Google, Facebook és TikTok) vállalatot keresztül fogom bemutatni, hogy milyen adatok gyűjthetnek be rólunk azok az alkalmazások, amelyeket szinte minden nap használunk. Kutatási forrásként ehhez a vállalatok adatvédelmi dokumentumait használtam illetve a saját fiókom beállítási lehetőségeit vizsgáltam.

Adatvédelmi nyilatkozat

A szabályozás témakörére visszautalva, a vállalatoknak tudatni kell a felhasználókkal a begyűjtött és felhasznált adatokat, ezeknek célját, tárolási idejét, adattovábbítási információkat, személyiségi jogokat, stb. A GDPR szerint a vállalatok nem használhatnak túl hosszú és olvashatatlan feltételeket, amikor a hozzájárulást kérik az adatkezeléshez. A feltételeknek világosnak és könnyen érthetőnek kell lenniük. (European Union, 2018)



7. ábra: Az adatvédelmi nyilatkozatokat olvasók aránya (2020, 2021)^{8 9}

Forrás: saját szerkesztés (Eurostat, 2021.c) alapján

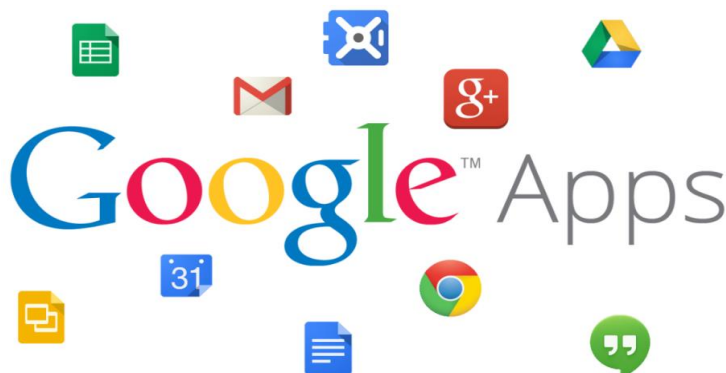
A 7. ábra azt mutatja, hogy az adatvédelmi nyilatkozatokat milyen arányban olvasták el a felhasználók 2020-ban és 2021-ben. Mindkét évben első helyen áll Horvátország, őt követi Ausztria és Finnország. Ebben a három országban a megkérdezettek több mint fele azt állította, hogy olvassa a nyilatkozatokat. Magyarország is a rangsor első harmadában helyezkedik el. A legtöbb ország esetében elmondhatjuk, hogy 2020-ban többen olvasták ezeket a dokumentumokat. Az Európai Unió 2019-es GDPR-ral kapcsolatos kutatásában megvizsgálták, hogy miért nem olvassák el az emberek ezeket. A résztvevők kb. 2/3 része amiatt nem olvassa el, mert túl hosszúak. A Spotify nyilatkozatát és az általános szerződési feltételeit közel 1 óráig tartana végig olvasni egy átlagembernek szünet nélkül. De több mint fél órán át olvashatnánk a Wikipediáét, az Apple-ét, a Tinderét, az Amazonét is, amire a mai rohanó világban kevesen szánják rá az idejüket. A második leggyakoribb ok, ami miatt nem olvassák el, az az, hogy nem elég érthetőek. A BBC felmérése szerint annak ellenére, hogy pl.: a Google-t, a Facebookot, a Youtube-ot, a Snapchatet akár 13 évesek is használják, az adatvédelmi dokumentumaik olyan bonyolultak, hogy egyetemi végzettség szükséges a teljes megértéshez. (Miller, 2018.) Nézzük meg, hogy a Google, a Facebook és a TikTok esetében igaz-e az állítás most, 2022-ben.

⁸ Franciaország esetében nem tudunk pontos adatokat, így az Uniók átlag is becslített érték.

⁹ Az országok jelölései a 9.2-es mellékletben találhatók.

4.1 GOOGLE ADATGYŰJTÉS ÉS ADATKEZELÉS

A Google óriásvállalatot 1998-ban alapították. Sikere azóta is töretlen. A népszerűségén kívül azért választottam ezt a vállalatot a személyes adataink gyűjtésének bemutatására, mert a Google fiókunkkal több alkalmazás is kapcsolatban áll. Ez azt jelenti, hogy vannak olyan adatok, amelyeket a Google összekapcsol az egyes alkalmazásokban. Például, ha használjuk a Naptárt, az megadhatja a Térképnek, hogy mikor, hová fogunk utazni egy-egy eseményre.



1. kép: Google alkalmazások

Forrás: (Finge, 2015.)

Az alkalmazások közé tartozik például a Gmail, a Google Fordító, a Google Chrome, a Google Hírek, Google Naptár, Google Play, Google Drive, Google Hirdetések, Google Segéd és a Google kapcsolatban áll a Youtube-bal is. A Google tudhatja, hogy kivel, mit levelezünk és azt is, hogy miket fordítunk le és tudja, hogy milyen események vannak beírva a naptárunkba, ismeri a dokumentumokat, amiket feltöltünk a Google Drivera, tudja, hogy milyen hirdetések érdekelnek. A Google érzékeli, ha a fiókunkba be vagyunk jelentkezve a számítógépről is és telefonról / tabletről is. Számos hasznos funkció van, például a készülékkereső segítségével, ha nem találjuk a telefonunkat, akkor a Google-t megkérhetjük a számítógépünkön keresztül, hogy keresse meg nekünk a mobilunkat, tabletünket. Ekkor azok, ha még néma módba is vannak téve, elkezdenek hangosan csörögni és a Google jelzi, hogy az eszköz hol található. Vizsgálatom során részletesen áttekintettem a Google adatvédelmi tájékoztatóját és a Google sűgót és dokumentumelemzést végeztem. A Google adatvédelmi tájékoztatója olyan hosszú, hogy nem volt elég egy délután, hogy áltassam. A vállalat szerint próbálják minél érthetőbbé tenni, rövid videókkal szemléltetni, hogy mi is történik az adatainkkal, ám véleményem szerint ez még bőven javításra szorul. A következőkben bemutatom, hogy az egyes alkalmazásokon keresztül milyen információkat gyűjtenek be rólunk.

4.1.1 Google alkalmazások vizsgálata

A **Google Drive** használata egy egyszerű és gyors módja annak, amikor nagyobb mennyiségű adatot szeretnénk megosztani valakivel anélkül, hogy romlana a minősége. Azonban tudnunk kell, hogy a feltöltött adatokat begyűjti a Google. A Drive-on keresztül számos olyan adatot osztunk meg, amelyeket semmiképp sem szeretnénk a nyilvánosság elé hozni, ilyenek lehetnek például régi családi fotók, céges vagy egészségügyi dokumentumok. Az alkalmazás természetesen funkciójából adódóan hozzáfér a galériához, a médiatartalmakhoz, dokumentumainkhoz és begyűjti azokat a kontaktokat, akikkel megosztjuk a fájlokat. A **Google Fordító**, amennyiben engedélyt adunk rá, gyűjti, hogy milyen szöveget fordítottunk le a fordító segítségével. A **Gmail** az egyik legelterjedtem e-mailezési lehetőség. Az e-mailek a fokozottan bizalmas adatok közé tartoznak, hiszen ezekben nagyon sok személyes adat megtalálható. Bármilyen üzenetet írhatunk és bármilyen fontos dokumentumot küldhetünk rajta keresztül. Ahogy sejthetjük, a Google tárolja a rajta keresztül küldött üzeneteket, így a csatolmányokat is. A Google állítása szerint a Gmail keményen dolgozik azon, hogy még a beérkező levelek közé érkezésük előtt törölje a spam jellegű és adathalász tartalmakat, valamint a rosszindulatú programokat. A spamszűréssel percenként mintegy tízmillió spam jellegű e-mailt szűrnek ki. Ezzel az adathalász próbálkozások 99,9%-át kiszűrjük, mielőtt odaérnének a felhasználóhoz. A **Google Hirdetések** gyűjtik, hogy mikor, mely hirdetésekre kattintottunk, míg a **Google Hírek** - amennyiben a híreket ott tekintjük meg -, elmenti, hogy mikor és melyik híreket néztük meg. A **Google Kereső** elmenti a kereséseinket, annak érdekében, hogy gyorsabb, relevánsabb és hasznosabb tartalomjavaslatokat biztosíthasson. A keresési előzményeinket vissza tudjuk nézni időponttal együtt. Az előzményeket lehet törölni. A Google személyre szabhatja a keresést akkor is, amikor nem vagyunk bejelentkezve a fiókba. A keresések gyűjtése miatt tudják, hogy a felhasználók ugyanazokra a kifejezésekre milyen más szavakkal keresnek rá és melyik linkekre kattintanak, ezzel segítségünkre van a keresésben. Az internetes és alkalmazástevékenységek által gyűjtött adatok törlését a rendszer automatikusan 18 hónapra állítja, ezt akármikor meg lehet változtatni. A **Google Naptárában** tárolt adatok alapján a Google tudja, hogy mikor, milyen eseményeken, programokon veszünk részt. A Gmail-lel kapcsolatban áll, így például, ha szállást vagy repülőjegyet foglaltunk és ez jelentkezik az e-mailek között, beteheti a Naptár alkalmazásba. Mivel a Naptár kapcsolatban áll a Térképpel is, amikor a repülőjegyünk megvan, és a helymeghatározás be van kapcsolva, akkor a Google figyelmeztet minket, hogy ahhoz, hogy időben a repülőtérré érjünk, mikor kell elindulnunk. A **Google Play** gyűjti, hogy milyen alkalmazásokra kerestem rá, melyeket töltöttem le.

A **hangsegéd**ek alkalmazása már régóta téma. A Review kutatása szerint 2021-ben az amerikaiak 76%-a használt már hangasszisztenst és 56%-uk napi szinten használja és a felhasználók 52%-a sosem olvasta el az adatvédelmi szabályzatot. Talán Magyarországon ez még kevésbé elterjedt. A felmérésben résztvevő intelligens asszisztens felhasználók 61%-a aggódik amiatt, hogy a hangsegéd hallgatja őket a háttérben. 45%-uk próbálta már letiltani, de 38%-ának nem sikerült. (Sandorf, 2021.) A **Google Segéd** akkor aktiválódik, amikor meghallja, hogy „Ok Google”. Ha nincs aktiválva, nem küldi el az adatokat másnak. Ám amennyiben az „Ok Google”-höz hasonló zajt hall, akkor is bekapcsolhat. Ezen a problémán még dolgoznak. Alapértelmezés szerint nem mentik a hangfelvételeket. A segéd a fióktevékenységek alapján is tud válaszolni, pl.: összekapcsolódik a naptár adataival, így tud válaszolni, ha megkérdezzük, hogy mikor indul a repülők? De akár az időjárást is meg tudja mondani a helyadatok alapján. Be lehet állítani, hogy felismerje a felhasználó hangját és csak akkor válaszoljon a személyes adataival kapcsolatban. Lezárt képernyőnél is össze lehet kapcsolni a hanggal. A Google Segéd megjegyezheti, hogy mikor mit mondtunk neki. (Google Sűgó, 2022.) (Google, 2022.) A hangsegéd gyűjti a felhasználó nevét, időzónáját, telefonszámát, a személyes érdeklődését, azokat az adatokat, amelyek a felhasználó profilban vannak tárolva, az eszköz helyadatait, a helyadatok előzményeit, az IP címet és a hangjellemzőket is. Ez kevesebb adat, mint amit a másik leghíresebb hangsegéd, az Amazon Alexa gyűjt. Amazon Alexa a fizetési információkat, a felhasználó korát és lakcímét is begyűjti. Azonban ami a kontaktjaink adatait illeti, a Google Segéd a hozzá hasonló leghíresebb hangsegéd alkalmazások közül a legtöbb adatot gyűjti be. Ilyen például a kontaktok neve, telefonszáma, címe, email címe, a tárolt kapcsolat a kontakttal. Amazon Alexa a Google Segéddel ellentétben gyűjti a képeket és videókat is. (Cohen, 2022. a)

A mai világban sokunknak be van kapcsolva a **helymeghatározás**. Habár tisztában vagyunk vele, hogy ez azt jelenti, hogy ahová a telefonunkat vagy egyéb eszközünket visszük, arról a helyről tud a Google. Azonban azt gondolom, hogy amikor szembesülünk vele, mégis egy kicsit rosszul érinthet. A dolgozatom írása közben, a kereséseim során rábukkantam, hogy mivel a helyadataim évek óta be vannak kapcsolva, a Google a Föld térképén be tudja nekem jelölni, hogy melyik tájakon jártam már. Ez egyrészt meghökkentő volt, hiszen újra szembesültem vele, hogy mindent tudnak rólam. Ekkor el is döntöttem, hogy kikapcsolom ezt a funkciót. Másrészt nagyon érdekesnek találtam és hosszú percekig töltöttem azzal, hogy megnézzem Európa melyik részein jártam már. Böngészésem során rábukkantam, hogy a leggyakrabban látogatott helyeimet is megtekinthetem. Ezeknél megtalálom, hogy mikor voltam ott utoljára és hány alkalommal látogattam meg összesen. Láthattam, hogy januárban hányszor voltam a Miskolci Egyetemen, ez hány km távolságra van az otthonomtól, a hazaúton mely bevásárló központban

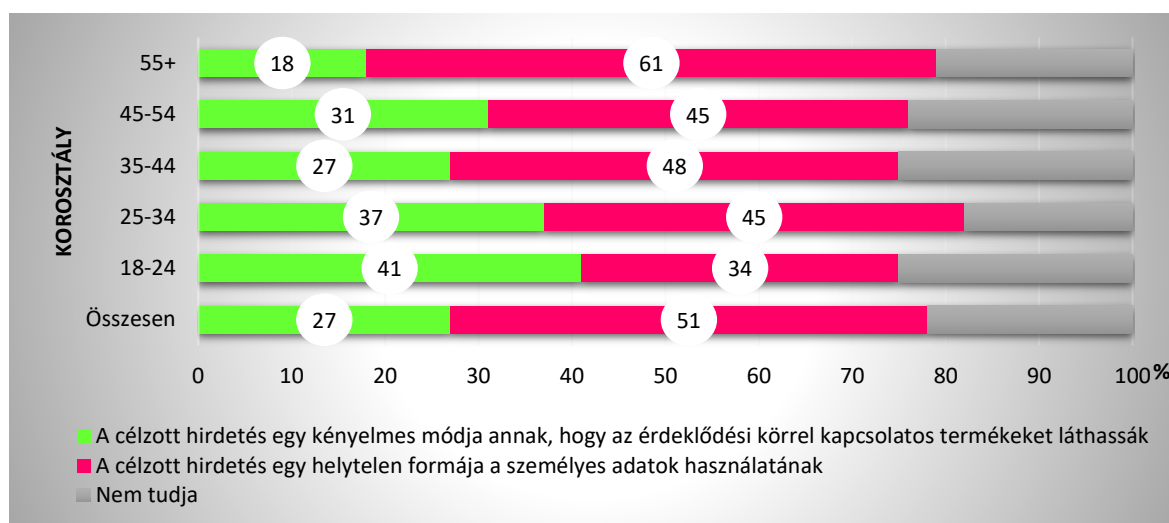
álltam meg és ott hány percet töltöttem. Tehát lekövethetem, hogy melyik nap hová mentem, hány km-t utaztam, milyen közlekedési módot választottam. A Google azt is megmutatta nekem, hogy pl.: a nyaralásom alkalmával a repülőtéren hány percet töltöttem, hány km-t és hány percet utaztam a levegőben, hány percet gyalogoltam. Ahhoz, hogy a Térkép alkalmazás meg tudja állapítani, hogy gyalogosan tettük-e meg az adott távolságot, szüksége van az egészségügyi adatainkra, így a lépésszámlálóra. Ha ez a funkció be van kapcsolva, akkor a lépések számát is tudja. Amikor használjuk a navigációt, bekapcsoljuk ezt. Nagy segítségünkre van, ha másoknak is be van kapcsolva, hiszen megtudjuk, hogy hol számíthatunk dugóra.

Összességében a helymeghatározás funkció bekapcsolásával nagyon sok adatot megtudhatnak rólunk: hol lakunk, hol dolgozunk, hová járunk vásárolni, melyik a kedvenc éttermünk, milyen gyakorisággal járunk oda és hány percet töltünk el. A Google azt is megjegyzi, hogy milyen helyekre kerestünk rá, melyik útvonalra voltunk kíváncsiak és ha a térképen csak úgy nézelődtünk, azt is látjuk, hogy megtekintettük XY város környékét. A helyadatokat még offline állapotban is elmentik, a telefonnal össze van kapcsolva. A helyelőzmények és internetes alkalmazástevékenységek alapján tudják javasolni számunkra a legmegfelelőbb éttermet. Ha jelezzük, hogy kedveljük a vegetáriánus étermeket, akkor azokat részesíti előnyben. Vagy amikor rákeresünk az éttermekre vagy benzinkútra, a helyadataink alapján, illetve az étterem szó alapján, ajánlani tudnak nekünk egyet a közelben. A helyadatok gyűjtése alapértelmezés szerint ki van kapcsolva. Amikor először engedélyezzük ezt, akkor az adatok törlését a rendszer automatikusan 18 hónapra állítja.

A Google adatvédelemmel kapcsolatos tájékoztatójában leírja azt is, hogy milyen intézkedéseket tesz az adataink megóvása érdekében. Az adatokat több biztonsági réteggel védi. Az adatok megóvása érdekében külön csoportot alakítanak ki az adathalászat ellen. Előfordult korábban, hogy például az útlevel megújítókat célozták az adathalászok, ezzel kicsalták az útlevelszámukat, bankkártya adatokat. A COVID19 járvány hatására külön munkacsoportot hoztak létre, akik éjjel nappal arra törekedtek, hogy megakadályozzák, hogy csalással kihasználják az emberek félelmeit, például, hogy áron felül és rossz minőségben adják az arcmaszkokat. A Google lehetőséget biztosít arra, hogy minden felhasználó hozzáférjen a vele megosztott tartalmakhoz bármikor, indokolás nélkül. Van egy úgynevezett *Adatok letöltése szolgáltatás*, amely segítségével le lehet tölteni a saját adatainkat, a fotókat, stb. Ez egyszerű művelet, nem kell külön kérnünk senkitől az adatokat. Amennyiben olyan személyes adatot találunk magunkról, amelyet szeretnénk letörölni, kérelmet kell benyújtani. Ilyen adat lehet például a kézzel írt aláírásunk képe, bankkártyaadatok és számlaszámok, bejelentkezési adatok, azonosító okmányok száma, képe, különleges adatok. (Google, 2022.)

4.1.2 Google hirdetések és különleges adatok

A legnagyobb bevételre a Google tesz szert a hirdetésekéből, ami a 2021-es adatok szerint közel 210 milliárd dollárt jelent. A keresések során már mindannyian találkozhattunk vele, hogy a találati listán az első pár helyen hirdetések jelennek meg. Ezek mindig meg vannak jelölve. Ha ezekre rákattintunk, akkor ebből a Google bevételre tesz szert. A hirdetőikkel csak akkor oszt meg személyazonosításra alkalmas adatokat, ha megkérjük erre. Amikor például a hirdetésre kattintva használjuk a *hívás* funkciót, akkor a hirdetővel megosztják a telefonszámunkat.



8. ábra: A célzott hirdetésekről alkotott vélemény

Forrás: saját szerkesztés (YouGov, 2019.) alapján

A fogyasztók számára aggasztó emlékeztetők lehetnek a személyre szabott hirdetések arra, hogy sosincsnek egyedül az interneten. A YouGov 2019-es felmérésében megkérdezték, hogy a résztvevőkhöz melyik állítás áll közelebb: *célzott hirdetés egy kényelmes módja annak, hogy azokat a termékeket látom, amelyek iránt érdeklődök* vagy a *célzott hirdetés egy helytelen felhasználása a személyes adatoknak*. A 3 132 fő amerikai résztvevő 51%-a úgy gondolja, hogy a célzott hirdetések a személyes adatok nem megfelelő felhasználását jelentik. 27%-uk azt mondja, hogy a célzott hirdetések kényelmes módja annak, hogy azokat a termékeket lássák, ami iránt érdeklődnek. Megfigyelhető, hogy 18 és 24 éves kor közötti válaszadók nyitottabbak az a hirdetésekre, mint az idősebbek. Közülük 41% az, aki szerint inkább kényelmes, 34% szerint nem helyén való. Az 55 év felettiek 61 %-a szerint helytelen és minősége 18% gondolja inkább kényelmesnek. (YouGov, 2019.) Ha például elmegyünk nyaralni a barátokkal a görög tengerpartra, könnyen előfordulhat, hogy valamilyen görög sör reklám jelenik meg az alkalmazásokban. Ennek oka, hogy tömérdek adatot begyűjtenek rólunk és a környezetünkben

lévőről. Láthatják, hogy nyaralás közben a barátok közelében vagyunk, akiknek tudja az alkalmazás a korát, ebből arra következtethet, hogy nagy a valószínűsége, hogy megkívánjuk a sört. (Bolcsó, 2019) A személyes adataink alapján célzott hirdetéseket tudnak megjeleníteni számunkra, ám ahogy már megnéztük, vannak olyan különleges adatok, amelyek felhasználását tiltja a törvény. A különleges adatok felhasználása a hirdetések során is túl kényesnek bizonyulna és negatívan befolyásolná a felhasználói élményt, ezért nem engedélyezett ezen kategóriák célzása. Az előző fejezetben már láthattuk, melyek a különleges adatok, amik felhasználása tilos. Nézzünk néhány példát, hogy a Google hirdetési irányelve szerint miket tilos reklámozni:

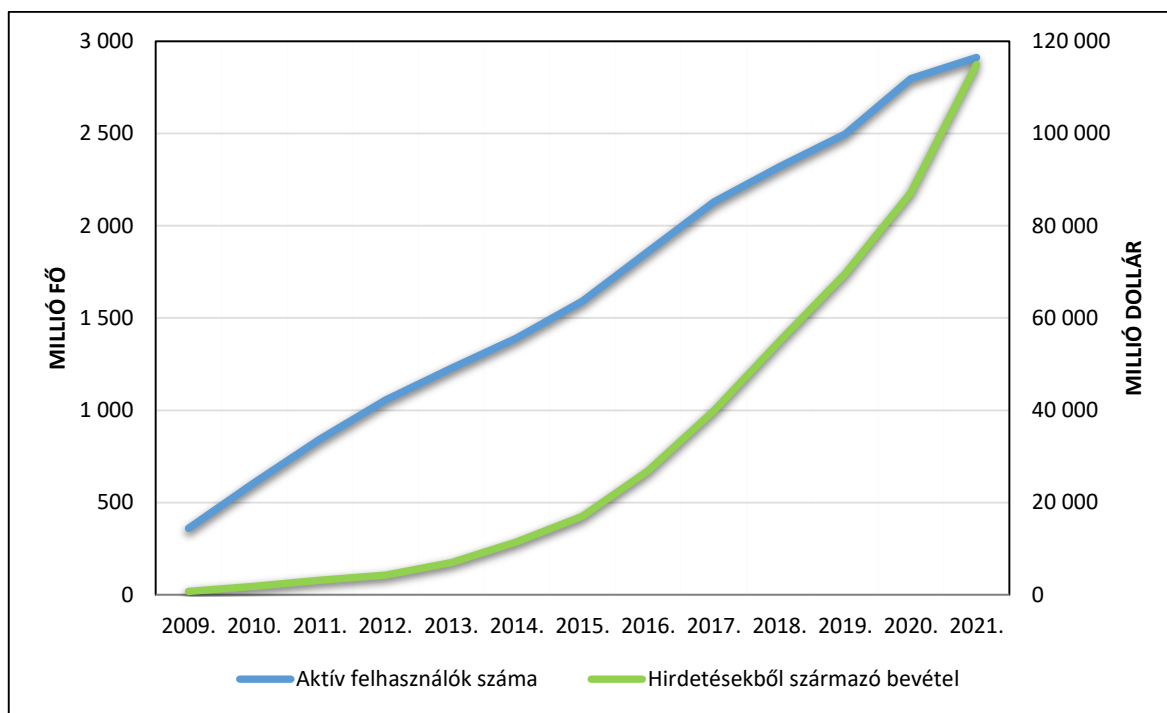
1. A 13 éven aluli gyerekek (vagy az adott országban meghatározott alsó korhatárt el nem érő gyerekek- Magyarországon 16 év) személyes adatait,
2. a vényköteles gyógyszereket, kivéve, ha csak állatgyógyászati célra használható,
3. alkoholos italokat vagy rájuk hasonlító üdítőket, a szerencsejátékot,
4. a személyes nehézségeket érintő témákat, nem lehet kihasználni a fogyasztó nehéz élethelyzeteit, traumáit, betegségeit,
5. az egészségügyi problémákat: fizikai, lelki egészség, krónikus korállapotok kezelésére szolgáló szolgáltatásokat, eljárásokat, plasztikai sebészetet, fogyatékossgot (pl.: cukorbetegség, ízületi gyulladás, szorongáshoz kapcsolódó mentális problémák, gombás fertőzések),
6. a pénzügyi problémákkal kapcsolatos hirdetéseket: pl.: hajléktalanszállók, csődszolgáltatások,
7. a párkapcsolattal kapcsolatos nehézségeket: pl.: válással kapcsolatos szolgáltatások, könyvek, gyásszal kapcsolatos szolgáltatások,
8. a bántalmazással, traumával kapcsolatos dolgokat: bűncselekmény áldozataként való besorolás, menedékek családon belüli erőszaki áldozatai,
9. tilos a testi adottságok kigúnyolása, annak sugalmazása, hogy ha nem végez el a felhasználó valamilyen cselekményt, akkor negatív dolgok fognak történni,
10. a hitvallással kapcsolatban reklámozni: beskatulyázás, hitrendszer, diszkrimináció,
11. szexuális témájú reklámok- pl.: meleg társkeresés; szexuális együttlét esetén használt termékek, terhesség vagy szexuális úton terjedő betegségek megelőzésére szolgáló eszközök,
12. politikai hovatartozással kapcsolatos reklámok- politikai kampányok, politikai vélemény,

13. szakszervezeti tagsággal kapcsolatos reklámok: amelyek a szakszervezeti tagságának ismeretét sugallják, pl.: szakszervezeti blogok,
14. etnikai hovatartozással kapcsolatos reklámok: etnikai irányultságú egyetemek, társkeresés,
15. vallással kapcsolatos reklámok: lelki vezetés, vallásos termékek,
16. tagság egy kirekesztett csoportban- bevándorlók, menekültek. Pl.: jogi szolgáltatás menekültek számára, bevándorlókat célzó szolgáltatások
17. transznemű- nemváltoztatással kapcsolatos információt. (Google, 2022. b)

Összességében a Google adatvédelmi irányelve, illetve súgója rengeteg információval szolgál. A linkek száma egy oldalon akár 15 is lehet, így habár érthetőek a leírások, nehéz követni, hogy éppen hol tartunk és könnyen elveszhetünk. A linkek egyes esetekben angol leíráshoz irányítanak, ami zavaró. Azonban pozitív, hogy nem jogi szöveget használnak, hanem egyszerű leírást, amelyet könnyen megérthet az is, akinek nincs magas szintű nyelvtudása. Ha kíváncsiak vagyunk valamire, számoljunk azzal, hogy rá kell szánni az időt a keresésre. A dolgozat írásakor végignéztem minden egyes linket és kijegyzeteltem a lényeges dolgokat. Azonban, amikor szerettem volna 1-1 témában elmélyülni és visszakanyarodni hozzá, nehezen sikerült megtalálni azt a linket, amit kerestem. Pozitívumként említem, hogy mindent leírnak érthetően, hogy milyen funkciót hogyan tudunk kikapcsolni. Beállíthatjuk, hogy az egyes adatokat hány havonta törölje automatikusan a Google. Inaktivitás esetén el lehet dönteni, hogy töröljék-e a fiókot, vagy legyen egy értesítendő személy, akivel megosztanak 1-1 adatot. (Google, 2022.) További megállapításom, hogy az adatvédelmi tájékoztató egészét megpróbálta szépíteni a Google. Arra például, hogy az alkalmazások begyűjtik és elmentik az adatokat, az *emlékszik* szót használják, ami valljuk be, valóban sokkal jobban hangzik. A tájékoztató videók kedvesek, jókedvűek, rövidek és informatívak. Bennem azt az érzést keltették, hogy a zenével és a színes videóval próbálják elvonni a figyelmet arról, amiket mondanak, néha sikerült is, ezért többször is megnéztem azokat.

4.2 FACEBOOK ADATGYŰJTÉS ÉS ADATKEZELÉS

A Facebookot 2004-ben alapította Mark Zuckerberg. Ahogy a 9. ábra is mutatja, a közösségi hálózat évről évre egyre több felhasználóval gazdagodott, ma pedig a világon közel 3 milliárd felhasználója van. (Statista, 2022. c)

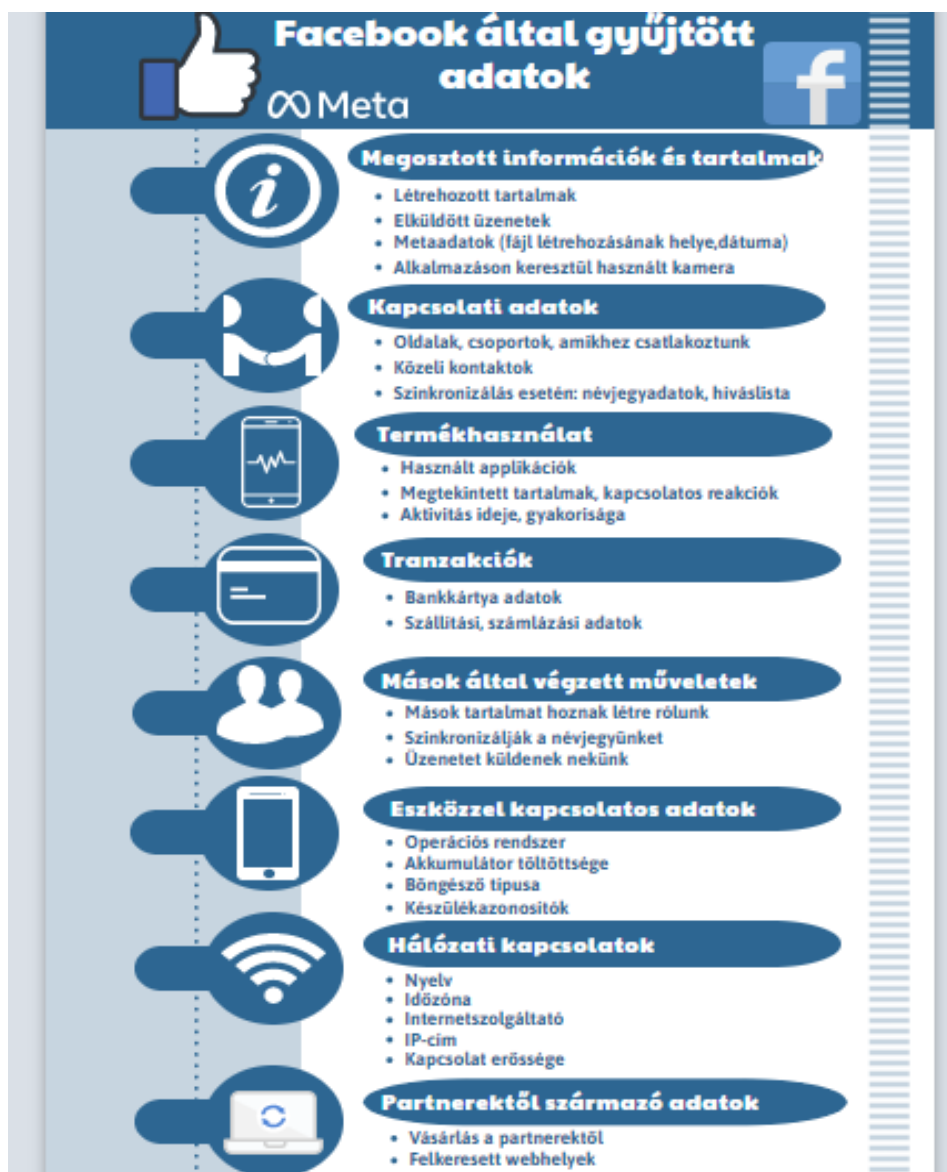


9. ábra: Facebook felhasználók számának és a hirdetésekből származó bevételének növekedése (2009-2021)

Forrás: saját szerkesztés (Statista, 2022.) és (Statista, 2022. c) alapján

Az aktív felhasználók száma nagyjából lineárisan, a hirdetésekből származó bevétel nagysága exponenciálisan nőtt. A Facebook azt nyilatkozta 2020. harmadik negyedévében, hogy egy hónapban 10 millió aktív hirdető népszerűsíti a termékét a közösségi oldalon. (Statista, 2022. b) 2021-től a Facebook Inc. helyett Meta Platforms Inc. néven fut tovább a cég. A „metaverzumba”¹⁰, tartozik az Instagram, a Messenger és a Whatsapp is. (Forbes, 2021.) A következőkben megnézzük, hogy a Facebook milyen adatokat gyűjt rólunk és mire használja fel. A legfontosabb különbség a Google és a Facebook által begyűjtött személyes adatok között, hogy a Facebook a kapcsolatainkat is nagymértékben ismeri.

¹⁰ „Magát a metaverzum szót 1992-ben alkotta meg Neal Stephenson a *Snow Crash* című cyberpunk regényében, ahol ez volt a jövőbeli virtuális valóság neve. Egy olyan, háromdimenziós virtuális teret jelölt, ahol a felhasználók avatárjai hasonlóan élhetik az életüket, mint a valóságban.” (Flachner, 2022.)



3. Infografika: A Facebook által gyűjtött adatok

Forrás: saját szerkesztés a Facebook adatkezelési szabályzata alapján

A Facebook gyűjti azokat a tartalmakat, kommunikációkat, információkat, amelyeket az applikáció használata során rendelkezésre bocsátunk. Ilyen pl.: amikor üzenetet küldünk másoknak vagy tartalmat hozunk létre. A megosztott tartalmakhoz tartozó metaadatokat is elmenti, így tudják a fájl létrehozásának dátumát és helyét. A Facebook gyűjti a kameráján keresztül látottakat, állításuk szerint abból a célból, hogy ha szeretnénk, segítsenek a megfelelő szűrők vagy maszkok kiválasztásában. A Facebook lehetőséget ad egyes különleges adataink megadására is, pl.: vallási, politikai nézetek. Ezt beállíthatjuk nyilvános adatnak is. Az alkalmazás gyűjti továbbá azt, hogy kikkel állunk kapcsolatban, kivel kommunikálunk a legtöbbet, milyen keresőcímkeket használunk, milyen csoportokhoz vagy oldalakhoz

kapcsolódunk. Ennek segítségével egy olyan hírfolyamot állítanak nekünk össze, amelyben a számunkra érdekes, fontos emberek tartalmait láthatjuk. Biztosan észrevettük már, hogy vannak olyan ismerőseink, akiknek szinte sosem látjuk a megosztásait. Ez amiatt lehet, mert semmilyen interakcióba nem léptünk velük már jó ideje, nem tekintettük meg a történeteiket, nem kerestünk rájuk, nem beszélgettünk velük. Az applikációval szinkronizáljuk pl.: a névjegyeket, ekkor felhasználják az SMS listát, híváslistát, ezzel segítenek megtalálni azokat, akiket esetleg ismerhetünk. Gyűjtik, hogy hogyan használjuk az alkalmazást, milyen tartalmakat nézünk meg és melyikkel lépünk kapcsolatba. Gyűjtik az aktivitásunk idejét, gyakoriságát, időtartamát. A folyamatos értesítések küldése (pl.: emlékek, születésnap emlékeztető, stb.) azért van, hogy vegyük a kezünkbe a telefont minél gyakrabban és töltsünk időt az alkalmazásban. Ha a Meta applikációin keresztül fizetünk, pl.: adakozunk vagy vásárolunk, a Messengeren pénzt küldünk vagy kapunk, akkor tárolják a bankkártya adatokat, a szállítási, számlázási adatokat. Ha mások rólunk osztanak meg információt, szinkronizálják az elérhetőségünket, üzenetet küldenek nekünk, azt is tárolják. Összekapcsolják azokat az eszközöket (telefon, tablet, stb.), amiken használjuk az alkalmazást és begyűjtik az eszközök adatait. Személyre szabják a tartalmakat pl.: hirdetéseket, amiket majd a másik eszközön is láthatunk, reagálhatunk rá. Az eszközök tulajdonságait is begyűjtik (pl.: operációs rendszer, akkumulátor töltöttsége, jelerősség, tárhely, böngésző típusa, stb.). És a készülékek műveleteit is, mint pl.: az egér mozgása vagy hogy milyen ablakok vannak a háttérben megnyitva. A felsoroltakon kívül tárolnak azonosítókat, pl.: játékazonosítót. Gyűjtik a Bluetooth jeleket és Wi-Fi információkat. A helymeghatározás funkciót már a Googlenél részletesen kifejtettem. Begyűjtik a nyelvet, az időzónát, a mobiltelefonszámot, az internetszolgáltató nevét, IP címet, kapcsolat sebességet, közelben lévő eszközök adatait. Utóbbit azért, hogy pl.: egy videót közvetíteni tudjunk a TV-n. A hirdetőknak és alkalmazásfejlesztőknek elküldik egyes adatainkat. Ezek a Meta partnerei. Ha a Facebook hirdetésnek köszönhetően vásárol valaki, akkor az úgynevezett Facebook-képpont aktiválódik és jelenti a műveletet a weboldal tulajdonosának, ezzel ő később is elérheti az ügyfelet.

Az adatok felhasználása:

Az adatainkat felhasználják arra, hogy a hirdetéseket, a hírfolyamokat, képfolyamatokat (az Instagramon), történeteket személyre szabják. A tevékenységünk alapján ajánlásokat tesznek olyan témákkal kapcsolatban és olyan csoportokhoz való csatlakozásra, amelyek érdekelhetnek minket. Az összes Meta applikáció kapcsolatban van egymással, így a velük kapcsolatos műveleteket összekötik, hogy minden alkalmazásban személyre szabott élményt nyújtsanak.

Pl.: javasolhatnak olyan Facebook csoportot, amelynek tagjaival kommunikálunk a Messengeren. Felhasználják továbbá a begyűjtött adatokat az applikáció fejlesztésére, tesztelésére, javítására, kutatások készítésére. Segítenek a hirdető partnereknek a hirdetés hatékonyságának mérésében és abban, hogy tudják, milyen típusú emberek veszik igénybe a szolgáltatásaikat. Adataink segítségével fel tudják venni velünk a kapcsolatot, marketinganyagokat küldhetnek és tájékoztathatnak minket a szabályzatokról. A Google-höz hasonlóan, a személyes adatainkat nem adják el 3. félnek. Talán emlékszünk rá, hogy korábban, ha feltöltöttünk egy képet a Facebookra, sok esetben tudta, hogy ki van a képen és felajánlotta az adott személy társítását a fotóhoz. Ez a funkció már nem elérhető. (Facebook, 2022.)

A Facebook is használ cookiekat, ezeket az egyes készülékeken helyezik el. A cookiek segítségével megállapítják, hogy be vagyunk-e jelentkezve, és ha szeretnénk, bejelentkezve is tudunk maradni. Megjegyzik a nyelvet, amin használjuk az alkalmazást. Felismerik, ha valaki gyorsan egymás után rossz jelszavakat ír be és jelzik, hogy gyanús esemény történt. Észlelik a kártevővel fertőzött számítógépeket és megakadályozzák a további károkozást. Lehetővé teszik, hogy olyan embereknek jelenítsenek meg hirdetéseket, akik már jártak az adott vállalkozás webhelyén, esetleg vásároltak tőlük. A cookiek segítségével korlátozzák, hogy ne mindig ugyanazt a hirdetést mutassák nekünk. Kiszámolják, hogy hányszor jelent meg a hirdetés és ennek mennyi volt a költsége, valamint hogy az emberek milyen gyakran vásárolnak egy hirdetés megtekintése után. Többféle cookie is van, ezek közül kiválaszthatjuk, hogy melyeket szeretnénk bekapcsolni. Azonban vannak olyanok, amelyek nélkülözhetetlenek az alkalmazás használatához. (Facebook, 2022.)

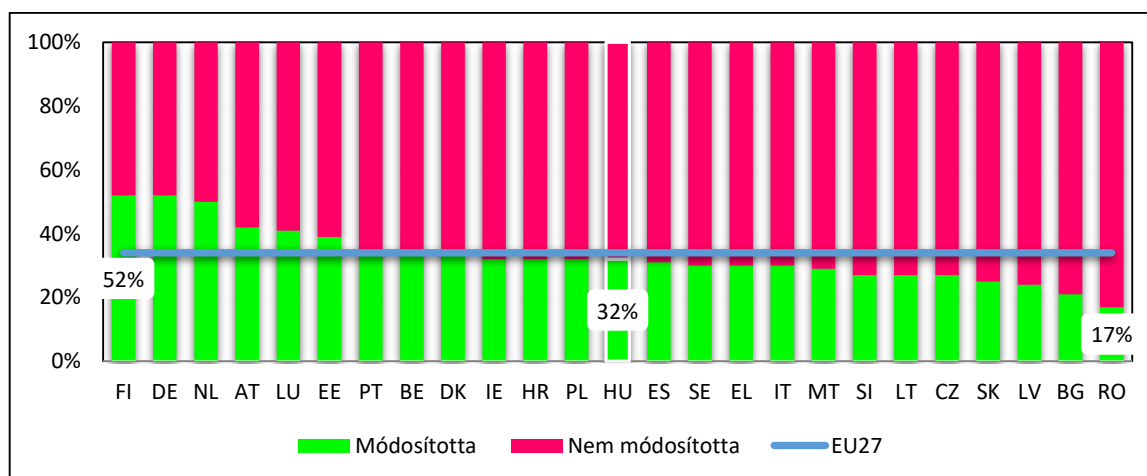
Kik azok akikkel megosztják a személyes adatainkat?

Sok adatvédelmi beállítást mi magunk is elvégezhetünk. Beállíthatjuk például, hogy az általunk megosztott tartalmakat ki láthatja, letilthatunk olyan embereket, akikkel semmilyen interakcióba nem szeretnénk kerülni. Ha azt választjuk, hogy mindenki láthatja az adatokat, akárki megoszthatja, hogy mit tettünk ki. Ám, ha korlátozzuk az adatlapunkhoz való hozzáférést, azok, akik láthatják a tartalmat, képernyőképet készíthetnek és továbbíthatják másoknak, akikkel eredetileg nem szerettük volna megosztani azokat. Ha hozzászólunk egy bejegyzéshez, akkor azt azok láthatják, akiket a bejegyzés tulajdonosa engedélyez. Előfordulhat, hogy később megváltoztatja a beállításokat és mindenki számára elérhetővé teszi a bejegyzést, aminek következtében a hozzászólásunkat is látják. Az ismerőseink láthatják, hogy éppen elérhetőek vagyunk-e vagy ha nem, akkor mikor használtuk utoljára az alkalmazást. Ezt a funkciót is kikapcsolhatjuk. Megtekinthetjük, hogy az adott napon hányszor nyitottuk meg

az alkalmazást és hány percet töltöttünk a használatával. Ha valaki adminisztrátor egy Facebook oldalon, azt tájékoztatják arról, hogy hányan tekintették meg a bejegyzéseiket, kik reagáltak rájuk. Általános demográfiai adatokat kapnak a felhasználókról (pl.: korosztály, lakóhely, érdeklődési kör). Az adatainkat addig őrzik meg, amíg nem töröljük a fiókot, vagy nem jár le a megadott idő. Pl.: a böngészési előzményeket 6 hónapig őrzik meg. (Facebook, 2022.)

Összességében a Facebook adatkezelési szabályzata jóval könnyebben kezelhető, rövidebb és átláthatóbb, mint a Google-é. A Facebook esetében egy helyen megtalálható szinte minden fontos adat. Kevés link van, amire lehet kattintani és azok is indokoltan vannak külön weblapon, nem úgy mint a Google esetében. Könnyen megtaláljuk a személyiségi jogainkat is és megfelelően ki van fejtve. Hiányosságnak azt éreztem, hogy nem volt minden adathoz leírva, hogy pontosan mire használják fel, csak néhány példát hoztak. És nem tüntették fel, hogy melyik adatot meddig tárolják pontosan. Korábban már volt szó arról, hogy azzal vádolják a Facebookot, hogy az adatvédelmi dokumentumok megértéséhez egyetemi végzettség szükséges. A 2022-es verzió esetében ezt meg tudom cáfolni. Az adatvédelmi tájékoztatóban itt is megtalálhatjuk, hogy hogyan módosíthatunk a beállításokon és azt hiszem a leírtak alapján indokolt is ezt megtennünk.

Az Európai Unió 2020-as kutatásában felmérték, hogy a tagállamok lakóinak milyen aránya változtatott már az adatvédelmi beállításokon a közösségi médiában.



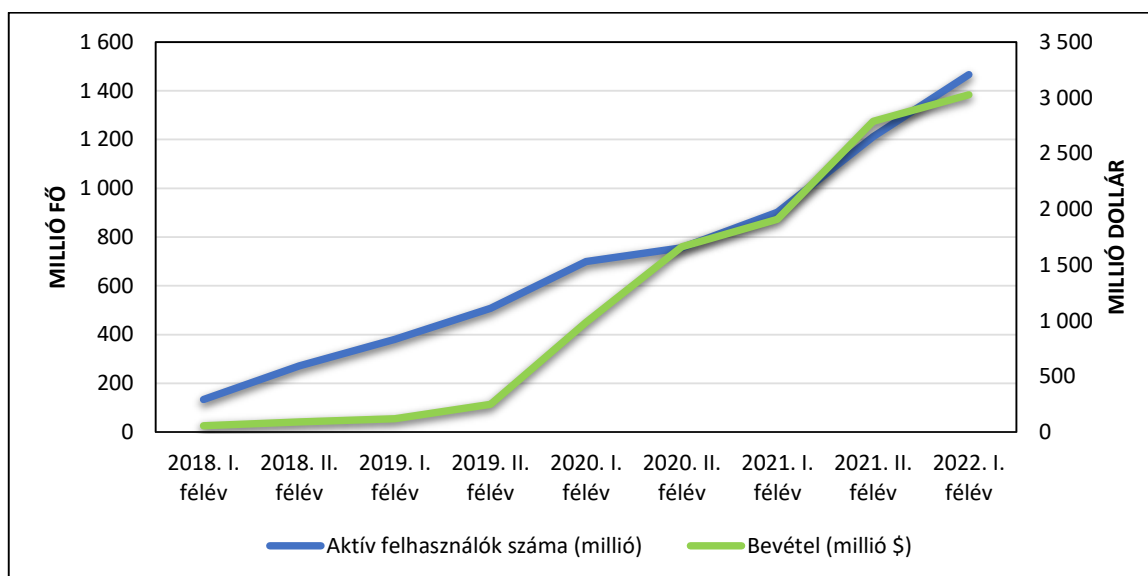
10. ábra: Az adatvédelmi beállításokat módosítók aránya (EU27,2020)

Forrás: saját szerkesztés (Eurostat, 2020.) alapján

A 10. ábrán láthatjuk, hogy a 2020-as adatok alapján Finnországban módosították a legtöbben az adatvédelmi beállításait a közösségi médiában. Ez a finn internetezők több mint felét jelenti. A válaszadók nagyjából egyharmada válaszolta azt, hogy megváltoztatta a beállításokat. Magyarország a rangsor közepén helyezkedik el 32%-kal. Romániában nem volt jellemző a felhasználókra, hogy módosítsák, a válaszadók mindössze 17%-a.

4.3 TIKTOK ADATGYŰJTÉS ÉS ADATKEZELÉS

2018-ban a kínai ByteDance cég létrehozta a TikTok rövidvideós alkalmazást, amelyet azóta több, mint 2 milliárdszor töltöttek le és melynek több mint 1 milliárd aktív felhasználója van. Az alkalmazás az első helyen áll a minden idők legtöbbet letöltött¹¹ alkalmazásai között, ezzel maga mögött hagyva az Instagramot, a Facebookot és a Whatsappot is. (STH, 2022.)



11. ábra: A TikTok bevételének és az aktív felhasználók számának alakulása 2018-2022

Forrás: saját szerkesztés (Business of Apps, 2022) alapján

Ahogy az ábrán láthatjuk, a felhasználók száma folyamatosan növekszik. A fogyasztók közel fele 16 és 24 év közötti. A 13 éven aluliak nem használhatják az alkalmazást és a 18 éven aluliak csak bizonyos tartalmakhoz férhetnek hozzá. A közvetlen üzenetküldés 16 éven aluliak számára nem elérhető. 2022 első félévében az aktív felhasználók száma már kb. 1,4 milliárd volt, a bevétel a 2021-es évben több mint 4,6 milliárd volt. 2022 első félévében pedig már meghaladta a 3 milliárd dollárt. A már eddig említett alkalmazásokhoz hasonlóan a TikTok bevételének nagyrésze is hirdetésekkel származik, kisebb része a felhasználók alkalmazások belüli vásárlásaiból. (Saxena, 2022) 2021-ben a reklámokból 4 millió dollárt generált összesen. (Statista.com, 2022.) 2022-ben várhatóan megtriplázza a hirdetésekkel származó bevételét. (Satija, 2022.) 2021-ben a felhasználók havonta átlagosan 25,7 órát töltöttek a TikTokon, míg a Facebookon 16-ot, az Instagramon és a Whatsappon pedig kevesebb mint 8 órát. (DIW, 2022.) Naponta pedig átlagosan 95 percet használják az alkalmazást. (Doyle, 2022) Az applikáció több mint 150 országban elérhető. A gyors növekedés következménye ellenőrzéseket eredményezett,

¹¹ Nem játék kategóriájú alkalmazások között

amely keretében az algoritmuson keresztül történő befolyásolást bírálták. A legtöbbször azzal vádolták a TikTokot, hogy egy kémalkalmazás, amely a kínai kormánynak szolgáltat adatokat a felhasználókról. 2020-ban az indiai kormány be is tiltotta az alkalmazás használatát és Donald Trump akkori amerikai elnök is törvényen kívül helyezte, mert azt gondolta, hogy nemzetbiztonsági kockázatot jelent. Joe Biden pedig később megváltoztatta Trump döntését. (O'Flaherty, 2021) 2019 decemberétől az amerikai katonai szervezet már nem használhatta az alkalmazást, mert kiberfenyegetésnek minősült. (Sherman, 2022.) Oroszországban a háborús helyzet miatt jelenleg -2022-ben- csak orosz tartalmakat nézhetnek a felhasználók. Egy rövid időre már betiltották Indonéziában és Bangladesben is. Mostanra elérhető, de cenzúrázott tartalmakkal. (Richardson, 2022) Ausztráliában is felmerült az alkalmazás betiltása, annak érdekében, hogy a kínai kormányhoz ne kerüljenek adatok. Felhívták az ausztrálok figyelmét, hogy az alkalmazást az üzenetek begyűjtésére is felhasználhatják. A ByteDance azt nyilatkozta, hogy az alkalmazásuk nem köthető Kínához, nem elérhető a hatóságok számára, ám az Internet 2.0 kutatása ezt cáfolja. Nem tudják, milyen adatokat küldenek, de az alkalmazás kínai szerverhez kapcsolódik. A TikTok szóvivője ezt valótlannak állítja. (Touma, 2022)

Az alkalmazásról több cikkben is olvastam, hogy azt állítják, lényegesen több engedélye van, mint amennyire szüksége lenne valójában. Hozzáfér a naptárakhoz, a névjegyekhez, a merevlemezekhez és az eszköz földrajzi helyének meghatározásához. Ha a felhasználó nem ad engedélyt az adatok gyűjtésére, a TikTok kitartóan kérdez. (Touma, 2022) Abból az adatból, hogy a felhasználó mennyi ideig nézi az adott videót, tudják, hogy mi az érdeklődési köre és arra is következtetnek, hogy milyen a kedvünk. A megosztott és kedvelt videók, a bejegyzések, a hashtagek és a fiókbeállítások alapján a hírcsatornák egyediek, személyre szabottak. Az alkalmazás célja a Facebookhoz hasonlóan, hogy a lehető legtovább maradjon a felhasználó a platformon és egyre több adatot gyűjtsön be. (O'Flaherty, 2021) Az URL Genius marketingcég kutatása szerint a fogyasztók nem tudják, hogy az adataik mely 3. félhez kerülnek és hogyan használják fel ezeket. A tanulmány szerint a nyomkövetés az alkalmazás elhagyása után is folytatódik és akkor is, ha nem engedélyezték a beállításokban. (Huddleston, 2022.) A Disconnect adatvédelmi vállalat egyik munkatársa az alkalmazás megnyitásakor kb. 210 hálózati kérést talált pár másodperc alatt, amely 125 oldalnyi gépetl adatnak megfelelő adatot küldtek az internetre. Ujjlenyomatot is lehetett venni a készülékről, akkor is, ha a felhasználó nincs bejelentkezve. 2020 márciusában fény derült arra is, hogy az alkalmazás néhány percenként hozzáfér a felhasználók iPhone vágólapjainak tartalmához, akkor is, ha az alkalmazás csak a háttérben fut. Azt nyilatkozta a TikTok, hogy ez spamellenes intézkedés és már frissítette az alkalmazást, hogy ezt leállítsa. (Fowler, 2020.) Egy német kutatás szerint az

alkalmazás böngészőkövetőket telepít, amellyel az összes tevékenységet nyomon követi. Ezt a TikTok azzal magyarázza, hogy felismerjék és megelőzzék a rosszindulatú böngésző viselkedéseket. Ha tömegesen töltik le az alkalmazást, akár az adott ország lakosságairól is következtetéseket vonhatnak le. (Sherman, 2022.)

Begyűjtött adatok:

- Profiladatok: Az alkalmazás begyűjti a profil létrehozásakor megadott adatokat. Ilyen a születési idő, felhasználónév, email cím, telefonszám, jelszó, profilkép.
- Felhasználói tartalom: Gyűjti a felhasználó által létrehozott tartalmakat, így a képeket, videókat, hangfelvételeket, hozzászólásokat, élő közvetítéseket és a metaadatokat is) Akkor is begyűjtik ezeket, ha a felhasználó csak létrehozza, de nem menti el vagy tölti fel.
- Vágólap: gyűjtik a vágólapról az adatokat, pl.: zenét, képek, videót. Ennek oka pl.: hogy videó alapján zenét találjanak
- Közvetlen üzenetek: gyűjtik az üzenetek tartalmát, résztvevőit, a küldés, fogadás és olvasás időpontját. Ennek oka: levélszemét blokkolása, bűncselekmények felderítése
- Névjegyzék: Importálás esetén. Cél: „ismerősök keresése” funkció használata.
- Vásárlási információk: gyűjtik a kártya adatokat, egyéb 3. féltől származó információkat, tranzakciós adatokat, vásárlási előzményeket.

Automatikusan gyűjtött adatok:

- Műszaki adatok: begyűjti az eszköz adatokat, a hálózati adatokat, a használt operációs rendszert, az eszköz modelljét, a billentyűleütési mintákat, az IP címet, a nyelvet, a teljesítmény információkat
- Helyadatok: begyűjti a hozzátétőleges tartózkodási helyadatokat, a SIM-kártya dataokat. Engedéllyel a pontos helymeghatározási információkat. Cél: felhasználói élmény személyre szabása, diagnosztika, hibaelhárítás
- Használati adatok: megtekintett tartalmak, alkalmazás használatának gyakorisága, ideje, kapcsolatba lépés módja a többi felhasználóval
- Tartalmi jellemzők és funkciók: begyűjti a videóval és hangfelvétellel kapcsolatos jellemzőket és funkciókat. Cél: moderálás, feliratok biztosítása
- Kikövetkeztetett információk: a tevékenységből következtetnek a felhasználói tulajdonságaira, pl.: életkor, név, érdeklődési kör. Cél: a biztonság megőrzése, a tartalom moderálása, engedély esetén személyre szabott hirdetésekre való felhasználás.
- Sütik: Cél: nyelv megjegyzése, egy-egy videó egyszeri megnézése, marketingcélok

Az alkalmazás egyéb forrásból is gyűjthet adatokat. Pl.: ha más felhasználó megemlíti minket a tartalmában vagy az üzeneteikben, vagy megadja az adatainkat az „Ismerősök keresése” funkción keresztül. Gyűjt információkat, ha TikTok fiókkal jelentkeznek be a felhasználó egy másik szolgáltatásba vagy egy harmadik fél szolgáltatásában tartalmat oszt meg a TikTok-on. Ha más platformon keresztül regisztrálnak a TikTokra, akkor a 3. fél megoszt egyes információkat, pl.: nyilvános profilt. Továbbá a hirdető és a mérési adatpartnerek információkat osztanak meg a felhasználó által végrehajtott műveletekről. (TikTok, 2021.)

Adatmegőrzés:

A megőrzés ideje az adat típusától függ. A profiladatok, a felhasználó tartalom és az üzenetek megőrzése addig tart, amíg a felhasználó rendelkezik TikTok fiókkal. Az irányelvek megsértése esetén törlik a felhasználói tartalmat a nyilvánosság elől, viszont megőrizhetik a jogsértés kezeléséhez. (TikTok, 2021.)

Tippek az alkalmazás használatával kapcsolatban:

Célszerű elkerülni, hogy összekapcsoljuk a fiókunkat más közösségi profilunkkal. Az Iphone segítségével korlátozhatjuk a nyomkövetést az Apple App Tracking Transparency funkcióval. Az ESET cég kiberbiztonsági szakértője szerint célszerű új email címet készíteni a regisztrációhoz és nem a már meglévőt használni. (O'Flaherty, 2021)

Robert Potter, az Internet 2.0 ausztrál kiberbiztonsági vállalat vezérigazgatója az alábbi javaslatot tette: *„Ha videókat szeretnél megosztani és macskákat szeretnél nézni, mindenképp tedd meg. Ha beszélgetni akarsz a barátaiddal a szexuális irányultságodról vagy az emberi jogaidról, nagyon óvatos lennék.”* (Touma, 2022)

Összességében a TikTok adatvédelmi irányelve átlátható és kellően lényegre törő, ám a megfogalmazása helyenként ködös és sokszor nem derül ki pontosan, hogy mire is használnak egy-egy adatot. Mindenképpen megkönnyítené a dolgunkat, ha lenne egy keresési mező, amelybe kulcsszavakkal rákereshetnénk arra, amiről tudni szeretnénk. A személyiségi jogainkról megfelelően tájékoztatnak. Ami rögtön feltűnik, hogy van egy úgynevezett „Automatikusan gyűjtött adatok” rész, amelyben megtaláljuk a hozzátvetőleges helyadatok begyűjtését is. Magyarázatuk szerint ezt is a felhasználói élmény javítása miatt gyűjtik, ám azt gondolom, hogy ez kevésbé magyarázható ezzel az indokkal. Ami hiányosság, hogy habár a süti törlését könnyen megtaláljuk a sütiszabályzatban, azt igencsak keresnünk kell, hogy hogyan módosíthatjuk az egyéb személyes adattal kapcsolatos beállításokat. Amikor megtaláltam és a linkre kattintottam, láttam, hogy angol nyelvű a tartalom. Véleményem szerint egy ilyen fontos témát, minden ország nyelvén elérhetővé kellene tenni.

A három vállalat bizony nagyon sok mindent tud a tevékenységeinkről. A TikTok alkalmazást nem használom, ám a Google és a Facebook alkalmazásban kiválasztottam egy tavaly augusztusi hetet, hogy megnézzem, mennyi adatot tudok visszanézni, azaz mennyi adatot tárolnak rólam még ennyi idő elteltével is. Mondanom sem kell, hogy mivel a Google elmenti a böngészési előzményeket, hamar kiderült, hogy azon a héten főként mik foglalkoztattak. Az egyik az, hogy nyaralni megyek. Többször is megtekintettem a szállást, a közelben lévő legjobb éttermeket, amibe szerettem volna vacsorázni, a közeli programlehetőségeket. Azt is visszanézhettem, hogy azon a héten COVID tesztet foglaltam valakinek. Felidézhettem, hogy milyen híreket, milyen recepteket néztem meg és azt is láthattam, hogy az egyik este probléma volt a munkahelyemen, mert azzal kapcsolatos kereséseket hajtottam végre. Emellett pedig valószínűleg mentem a műkörmöshöz, mert a keresési előzményeim tele voltak gélakkos képekkel. A Térkép alkalmazás segítségével visszanézhettem, hogy azon a héten milyen helyeken jártam és ott mennyi időt töltöttem el, milyen közlekedési eszközt használtam. A Facebookon pedig visszanézhettem az alkalmazással kapcsolatos tevékenységeimet, kinek, mikor szoltam hozzá a képéhez és mit. Kikre kerestem rá, milyen csoportokhoz csatlakoztam, milyen videókat tekintettem meg. Ha engedélyeztem volna, megjegyezte volna a hangalapú interakciókat is. Visszakereshettem, hogy milyen híreket néztem meg. Mikor jelentkeztem be az alkalmazásba. Azon a héten kik lettek az ismerőseim, esetleg kiket töröltem közülük.

Szinte minden begyűjtött adatra rámondhatjuk, hogy azokat a személye szabottabb felhasználói élmény érdekében gyűjtik be. Vajon megéri ez nekünk?

Félelmetes, hogy az alkalmazások a lájkokból, a keresésekből és abból, hogy mennyi ideig nézünk egy-egy tartalmat, következtetni tudnak a jelenlegi hangulatunkra, az érzéseinkre és arra, hogy jelenleg mi foglalkoztat.

Láthatjuk tehát, hogy mennyi mindent elmentenek rólunk az alkalmazások, ha hagyjuk. A Google és a Facebook esetében egyszerűbben megtalálhatjuk az adatkezelési tájékoztatóban, hogy hogyan kapcsolhatjuk ki az egyes funkciókat az adatok begyűjtésére. Ezzel sok adatgyűjtést megakadályozhatunk.

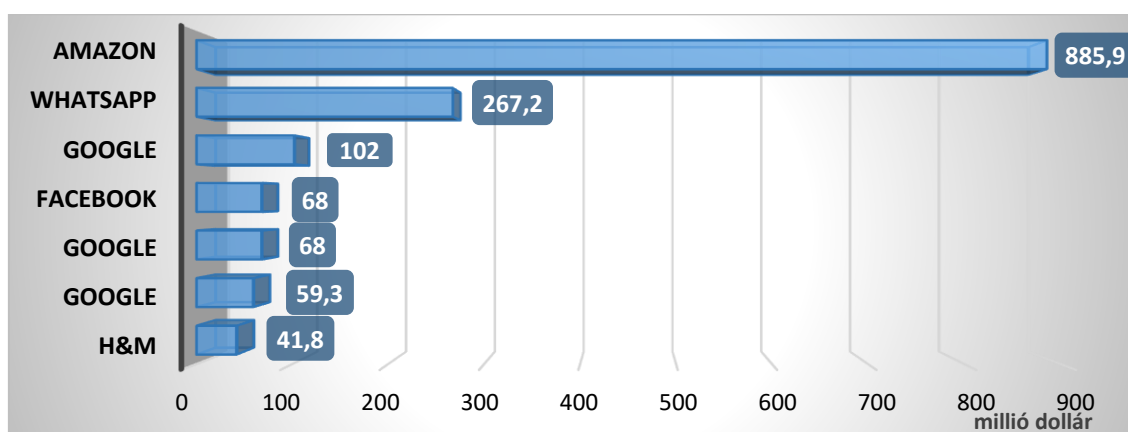
Ahogy már említettem, ha megszegik a vállalatok a GDPR-t, az árbevételük 4%-ig terjedő bírságot kaphatnak, ezért nagyon fontos, hogy odafigyeljenek a szabályok betartására. Az általános adatvédelmi rendelet bevezetését követően mind a Google mind a Facebook kapott már több millió dolláros büntetéseket. A következő fejezetben megnézzük, hogy melyek voltak az eddigi legnagyobb adatvédelmi incidensek.

5. ADATVÉDELMI INCIDENSEK

Az 5. fejezetben szemléltetem az eddigi legmagasabb büntetésekkel járó adatvédelmi incidenseket, ezt követően pedig azt, hogy mely országokban jelentették be a GDPR bevezetése óta a legtöbb incidenst. Ezután megnézzük, hogy aggódnak-e a felhasználók a kibertámadások miatt és ezt befolyásolja-e például a rossz tapasztalat. Végül bemutatom, hogy mely országokra a legjellemzőbb, hogy a lakók tesznek az adataik védelméért.

5.1 A LEGNAGYOBB BÜNTETÉSEK

2 évvel a GDPR hatálybalépése után a vállalkozások egy része még mindig nem felelt meg a rendelet elvárásainak, sokan nem vezették be a megfelelő IT-fejlesztéseket, ami nagy hiányosság. A kiberbűnözők folyamatosan az elavult szoftvereket keresik, mert azokon keresztül könnyen lophatnak adatokat. (SecureInfo, 2020.) Pedig a vállalkozásoknak komolyan kellene venni a szabályok betartását, hiszen az általános adatvédelmi rendelet megsértése súlyos büntetéseket von maga után. Egyes jogsértések esetén a vállalatot akár 20 millió euróra vagy az éves árbevételének 4%-ára is megbüntethetik. (Európai Unió, 2018) Az alábbi ábrán láthatjuk, hogy melyek voltak a legmagasabb büntetések a GDPR bevezetése óta és mely cégekre szabták ki ezeket.



12. ábra: A legmagasabb büntetések a GDPR megszegése miatt

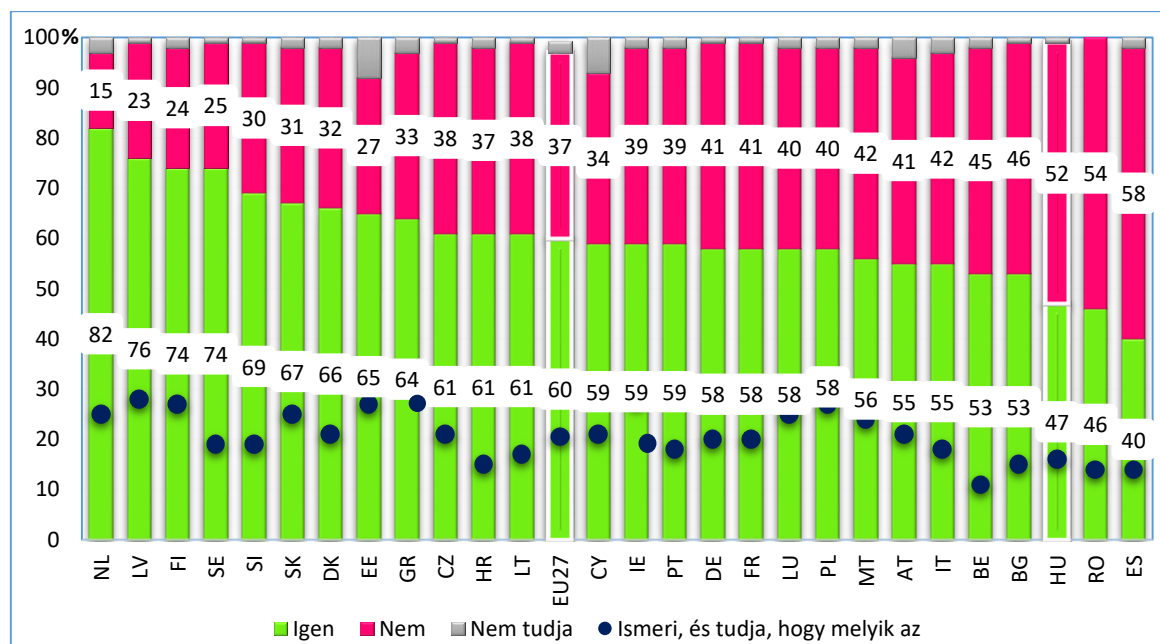
Forrás: saját szerkesztés: (CMS.Law, 2022.) alapján

A legnagyobb büntetést a GDPR megszegése miatt az Amazon kapta, ami 885,9 millió dollárt jelent. Megszegte az adatvédelemre vonatkozó irányelvet azzal, hogy a személyes adatok feldolgozása nincs összhangban a GDPR-rel. Az Amazon ezt tagadta, szerinte nem történt adatvédelmi incidens, így fellebbezést tervezett. Az összeg magában hatalmas, viszont a cég bevételéhez viszonyítva kevésbé számottevő, ami már 3 egymást követő negyedévben is

meghaladta a 100 milliárd dollárt. (Sam Shead, 2021.) A lista 2. helyén a Whatsapp bírsága áll 267,2 millió dollárral. A hatóságok azt állították, hogy a cég nem közölte a felhasználóival, hogy hogyan osztotta meg az adataikat az anyavállalatával, vagyis a Facebookkal. A Whatsapp is fellebbezett. (Portfolio.hu, 2021. c) A Google többször is magas bírságot kapott, különböző országbeli vállalatára. A legnépszerűbb keresőmotor, a GDPR több pontját is megszegte, amit már pár nappal a rendelet hatálybalépését követően elkezdtek vizsgálni. A francia adatvédelmi hivatal közel 60 millió dollár bírságot szabott ki, mert a felhasználók tájékoztatása nem volt elég átlátható és érthető. Úgy gondolom, ezt a problémát azóta sem sikerült megfelelően kiküszöbölni. Az adatfeldolgozási célok és az adattárolási időszakokat, illetve a személyre szabott hirdetésekhez felhasznált személyes adatokat csak több dokumentumból lehetett összegyűjteni. Ezen kívül, amikor valaki létre akart hozni egy fiókot, akkor a további lehetőségekre kattintva már előre be volt jelölve a személyre szabott hirdetések négyzete és automatikusan elfogadta a hangfelismerést. Ezek szintén sértették a rendeletet. (Habók, 2019). További probléma, hogy sem a Facebook, sem pedig a Google nem biztosított ugyanolyan egyszerű módot a cookiek elutasítására, mint az elfogadására. Az elutasításhoz több kattintást véghez kellett vinni az érintetteknek. (Data Privacy Manager, 2022.) A nürnbergi H&M 2014 után az alkalmazottak magánéletével kapcsolatos információit kezdte el rögzíteni. A munkavállalók szabadságai/ betegszabadságai után a csoportvezetők egy úgynevezett „Welcome back Talks”-ot folytattak, ami arról szólt, hogy hogy telt a szabadságuk. Amennyiben betegség miatt voltak távol, a tüneteiket is megkérdezték. Ezeket az információkat rögzítették és egy közös hálózati meghajtón tárolták. Nonszensz, ugye? Továbbá a dolgozók vallási meggyőződése és családi problémái is rögzítésre kerültek. 2019 októberében egy konfigurációs hiba miatt a rögzített adatok néhány órára cégszerte láthatóvá váltak. A cég azt állította, hogy ezek az adatok ahhoz szükségesek, hogy segítsék a vezetők munkavállalókkal kapcsolatos döntéseit. Ezen adatok rögzítése a munkavállalók jogainak sérelméhez vezetett. A botrányt követően a vezető kártérítést fizetett az érintetteknek. (EDPB, 2020. a) A *TikTok* is ütközött már adatvédelemmel kapcsolatos problémába. Az Egyesült Királyság Információs Biztosának hivatala szerint az alkalmazás 2018 májusa és 2020 júliusa között a 13 évnél fiatalabb gyerekek adatait feldolgozta szülői beleegyezés nélkül. Ezen kívül a cég nem adott tömör, átlátható és könnyen értelmezhető tájékoztatást az adatok feldolgozásáról. Ide tartozik pl.: a biometrikus adatok, egészségügyi adatok és a vallási adatok is. Ez sérti a GDPR-t. A TikTokot akár 25 millió fontig terjedő bírsággal is szabhatják. (Woollacott, 2022.) További adatvédelmi incidensekkel a 9.3 számú mellékletben találkozhatunk.

5.2 BEJELENTETT ADATVÉDELMI INCIDENSEK

Az adatvédelmi incidenseket a fogyasztók az adatvédelmi hivatalnak tudják bejelenteni. Ahogyan már korábban említettem, minden országban van adatvédelmi hatóság, akihez fordulhatnak az érintettek probléma esetén. Vajon az európai fogyasztók tudnak arról, hogy létezik ilyen hivatal?



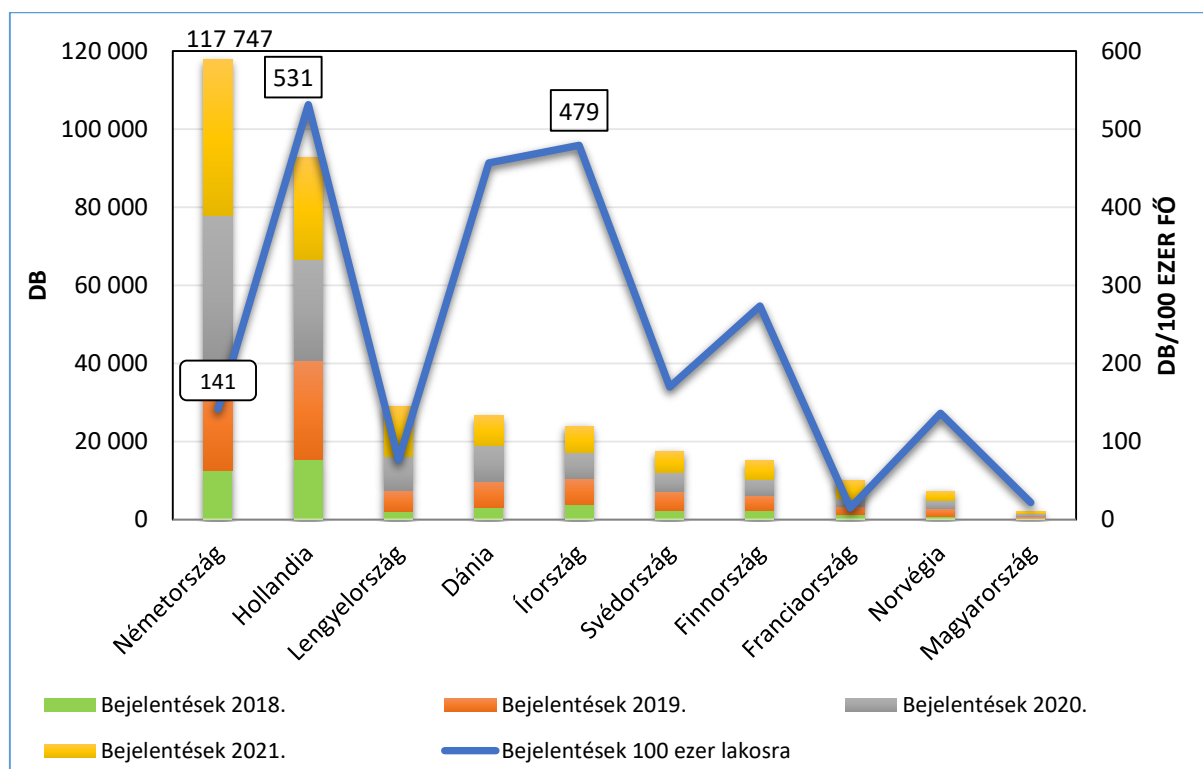
13. ábra: A személyes adatokkal kapcsolatos jogok védelméért felelős hatóság ismerete (EU27;2019)

Forrás: saját szerkesztés (European Commission, 2019.) alapján

A 13. ábra azt mutatja, hogy az Európai Unió tagországai milyen arányban tudnak arról, hogy létezik az országukban adatvédelmi hatóság és kik azok, akik tudják, hogy melyik az. Ebben a kérdéskörben is hatalmas különbség van az egyes országok között. Ahogy láthatjuk, 2019-ben Hollandiában a megkérdezettek 82%-a hallott már a hatóságról, így ő áll az első helyen. Hollandiát követi Litvánia, Finnország, Svédország, Szlovénia, és Szlovákia, ahol szintén a megkérdezettek több mint 2/3 része hallott már róla. Mindössze 3 ország van, ahol a megkérdezettek kevesebb, mint fele hallott az adatvédelmi hivatalról, sajnos ebből az egyik Magyarország. Országunkban a 2019-es felmérés szerint a válaszadók 47%-a hallott a NAIH-ról, ezzel az eredménnyel szintén jóval az EU27 átlag alatt járunk. A vizsgálatom során azokat az adatokat fogom felhasználni, amelyek arra vonatkoznak, hogy kik azok, akik tudják is, hogy melyik az országukban található adatvédelmi hivatal. Ezt figyelembe véve Hollandiában, csak a válaszadók 25%-a rendelkezik pontos ismerettel, míg Magyarországon csak 16 %-uk ismeri a NAIH-ot.

Az általános adatvédelmi rendelet hatálybalépése óta 2022 áprilisáig összesen 1 619 295 046 € büntetést szabtak ki a GDPR megszegése következményeként. (CMS.Law, 2022.) A 2. fejezetben már találkozhattunk a legnagyobb incidensekkel, most pedig megnézzük, hogy országonként hány bejelentés érkezett.

Európát tekintve az első 10 helyen álló országot (+ Magyarországot) az alábbi ábrán tekinthetjük meg. Ezekben az országokban érkezett a legtöbb szabályszegésről szóló bejelentés.



14. ábra: Bejelentett adatvédelmi incidensek (2018-2021)

Forrás: saját szerkesztés (DLA Piper, 2019.), (DLA Piper, 2020.), (DLA Piper, 2021.), (DLA Piper, 2022.c) alapján

A vizsgálatunk alapjául viszont nem az összes bejelentést vesszük alapul, hiszen az egyes országok népessége között nagy különbség van. Az adatvédelmi incidensek számát elosztottam az ország népességével és megszoroztam 100 ezerrel, így megkaptam, hogy 100 ezer főre hány bejelentés jut. Az ábrán láthatjuk, hogy ez milyen különbséget jelent, hiszen míg Németországban történt a legtöbb bejelentés, közel 120 ezer, ami jóval magasabb a többi országnál. Ha a 100 ezer főre jutó bejelentéseket nézzük, akkor Hollandiában, Dániában, Írországon és Finnországon is több bejelentés történt. Hollandiában a 100 ezer lakosra eső bejelentés közel négyszer annyi, mint Németországban. Habár Dániában ehhez a két országhoz viszonyítva kevés bejelentés érkezett, mégis ebben az országban majdnem annyi adatvédelmi incidenst jeleztek 100 ezer főre nézve, mint Hollandiában. Magyarországon a három és fél év

alatt kb. 2 150 db bejelentés érkezett, amellyel nagyjából a középmezőnyben helyezkedik el az európai országok között.

Korábban már megnéztük a legnagyobb adatvédelmi incidenseket, most pedig magyar példát is szeretnék említeni. Az egyik legfrissebb adatvédelmi incidenssel 2022 áprilisában találkozhattunk a médiában, amelynek keretében egyben a legmagasabb büntetést szabták ki az országban. Az egyik bankot (nem adják ki, hogy melyik) kb. 670 ezer euróra, azaz 250 millió forintra büntették. Az indok az volt, hogy az ügyfélszolgálati hívások hangfelvételeit automatikusan elemezték és az eredmények alapján döntöttek el, hogy kiket érdemes visszahívni. Az elemzést egy mesterséges intelligencia alapú szoftver segítségével végezték, amely képes volt a kulcsszavak alapján és a hívó érzelmi állapota alapján elemezni a hívásokat. A bank adatvédelmi nyilatkozata viszont csak általánosságban hivatkozott a minőségellenőrzésre és az ügyfélszolgálat hatékonyságának fejlesztésére, a hangelemzésről nem tartalmazott lényeges információt. Az adatkezelés céljaként a minőség-ellenőrzés és a panaszmegelőzés volt feltüntetve. A NAIH felhívta a figyelmet arra, hogy a mesterséges intelligencia használata adatvédelmi kockázattal jár, így az alkalmazása kiemelt figyelmet igényel. (Kozma-Almási, 2022.)

2020-ban a Deichmann Cipőkereskedelmi Kft. 20 millió Ft-os bírságot kapott, mert adatkezelőként nem volt tisztában az érintett jogaival és a GDPR szerinti kötelezettségeivel. Egy vásárló 20 000 Ft-os címlettel fizetett, de csak 10 000 Ft-ból kapott visszajárót. Akkor nem vette észre, ám később igen, ekkor elkérte a kamerafelvételeket az eladótól. Az eladó megtagadta a videó kiadását, pedig a vásárlónak joga volt látni. (GDPR Specialisták, 2020.)

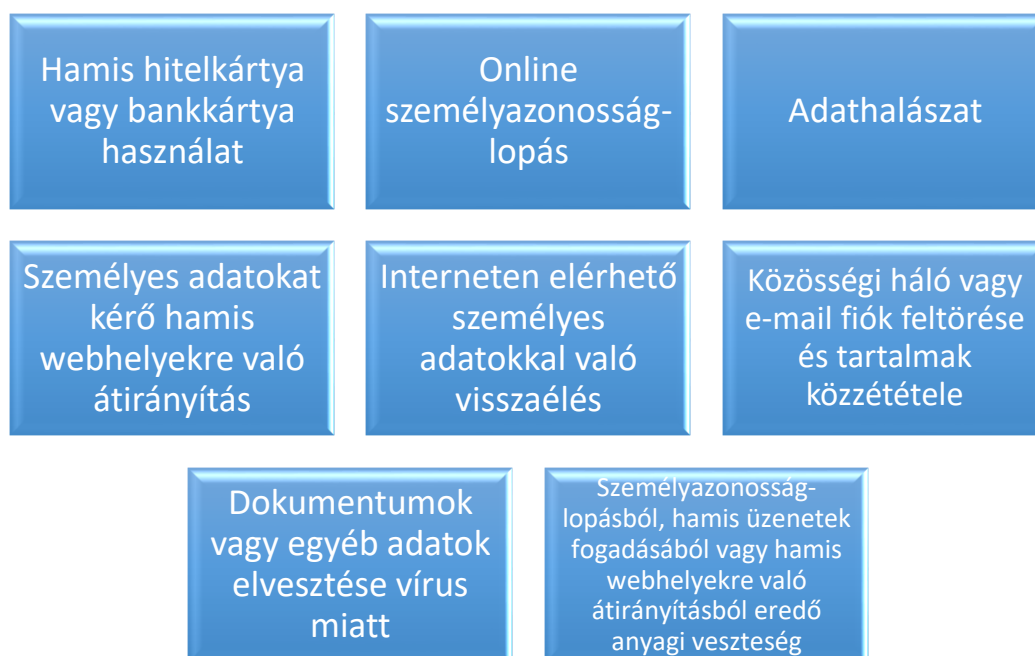
A DIGI Kft. ellen a NAIH 2019-ben indított eljárást, melynek eredményeképp 100 millió Ft bírságot szabtak ki a cégre. A GDPR célhoz kötöttség, illetve korlátozott tárolhatóság elvét megszegték. Tesztelési célból korábban létrehozta egy adatbázist, amely valószínűleg egy korábbi hiba kiküszöbölése céljából készült. Az adatbázisba feltöltötték az előfizetők elérhetőségeit. Mivel az adatbázis célját már nem lehetett meghatározni, az adatokat rég törölni kellett volna. Az adatok nem kerültek titkosításra. (Pánszky, 2022.)

Természetesen nem mindenki jelenti be az adatvédelmi incidenseket, hiszen vannak, akik nem veszik komolyan vagy nem töltik ezzel az idejüket. A következő fejezetben megnézzük, hogy az egyes országokban milyen arányban tapasztaltak már valamilyen adatbiztonsági problémát.

5.3 ADATBIZTONSÁGI PROBLÉMÁK

Az Európai Unió 2021-es Digitális jogok és alapelvek című kutatása során kiderült, hogy az Unió tagállamok lakóinak 56 %-át aggasztja a digitális eszközök növekvő szerepe miatti kibertámadások, adathalászat, személyes adatokkal való visszaélés. Azt feltételezem, hogy azokban a tagországokban, ahol nagyobb arányban tapasztaltak már valamilyen adatbiztonsági problémát, ott jobban aggódnak a kibertámadások miatt.

Vizsgálatomhoz az Európai Unió kutatásait használtam fel. Az információs és kommunikációs technológiával (IKT) kapcsolatban már 2002 óta végeznek felmérést. (Eurostat, 2019.b) 2019-ben az internet használata során tapasztalt biztonsági problémákat vizsgálták. A felmérésben azt kérdezték, hogy tapasztalták-e a résztvevők az alábbi problémákat valaha az interneten:



15. ábra: Adatbiztonsági problémák

Forrás: saját szerkesztés (Eurostat, 2019.b) alapján

A leggyakrabban tapasztalt probléma az adathalászat, ezt már az Unióban élő válaszadók 25%-a tapasztalta. A következő leggyakrabban előforduló gond 13%-os eredménnyel a *személyes adatokat kérő hamis webhelyekre való átirányítás*. Összességében a válaszadók közel egyharmada, 32%-a tapasztalta már legalább az egyik problémát. Magyarország jóval az Unió átlag alatt helyezkedik el, hazánkban ekkor a válaszadók 20%-a tapasztalta már valamelyik vizsgált tényezőt. (Eurostat, 2019.)

A feltételezésem bizonyítására szolgáló másik vizsgálat, az az Európai Unió 2019-es kutatása arról, hogy valamilyen internetes tevékenységet nem végeztek el a válaszadók egyes biztonsággal kapcsolatos aggodalmaik miatt.

Ilyen tevékenység lehet például:

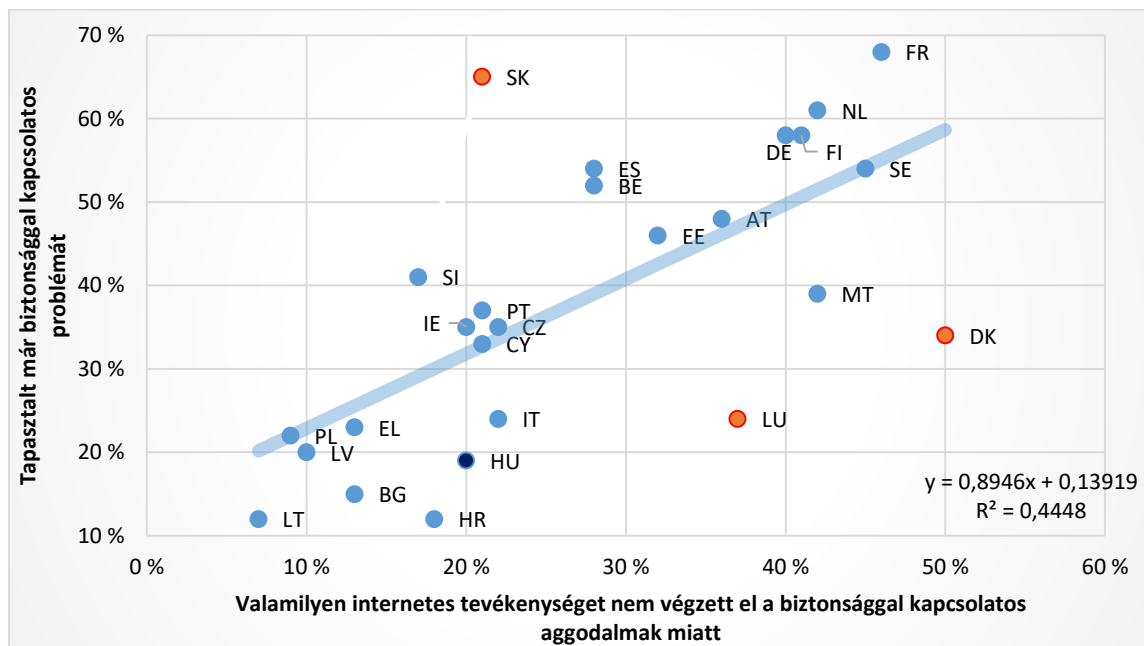


16. ábra: Internetes tevékenységek

Forrás: saját szerkesztés (Eurostat, 2019.c) alapján

A felsoroltakon kívül a megkérdezettek az „egyéb” lehetőséget is használhatták. Összességében a válaszadók 45%-ánál előfordult már, hogy nem végzett el valamilyen tevékenységet az interneten a biztonsággal kapcsolatos aggodalmi miatt. Magyarországon a válaszadók mindössze 19%-ával történt már ilyen. (Eurostat, 2019.c)

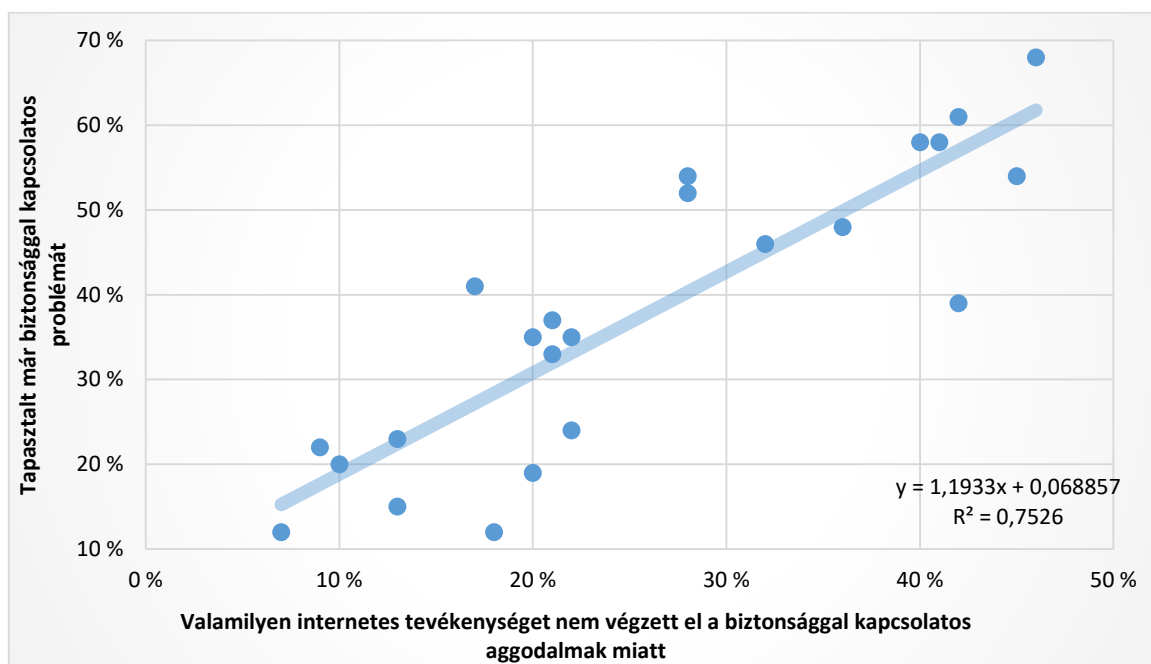
Most pedig nézzük meg, hogy van-e kapcsolat a tapasztalat és az aggodalom között.



17. ábra: Az adatbiztonsággal kapcsolatos tapasztalat és az aggodalom kapcsolata (EU27;2019)

Forrás: saját szerkesztés: (Eurostat, 2019.) és (Eurostat, 2019.c) alapján

Pearson féle korrelációs elemzést végeztem a két tényezőre nézve. Az eredmény $r = +66,69$ lett, amely pozitív irányú közepesen erős kapcsolatot feltételez a két ismerv között. A determinációs együttható értéke lineáris regresszió esetén a Pearson-féle korreláció eredményének négyzete, ahogy az ábrán is láthatjuk $R^2 = 0,4448$, amely azt jelenti, hogy 44,48%-ban befolyásolja az aggodalmat az, hogy az adott országban milyen arányban tapasztaltak már valamilyen biztonsággal kapcsolatos problémát a felhasználók. Az egyenlet $y = 0,8946x + 0,13919$, amely azt mutatja, hogy ha pl.: $x = 20\%$, akkor $y = 0,8964 \cdot 0,2 + 0,13919$ vagyis 31,847 %. Ez természetesen nem a pontos érték, akkor lenne az, ha az egyenesen helyezkedne el, de megközelítőleg ez tartozik hozzá. Pirossal jelöltem a három outliert, azaz a kiugró értékeket. Érdeemes elvégezni a vizsgálatokat úgy is, hogy ezeket nem vesszük figyelembe, hiszen torzíthatják az eredményt. A következőkben láthatjuk, hogy milyen különbségeket eredményez, ha a három ország: Dánia, Luxemburg és Szlovákia értékeit kihagyjuk az elemzésből.

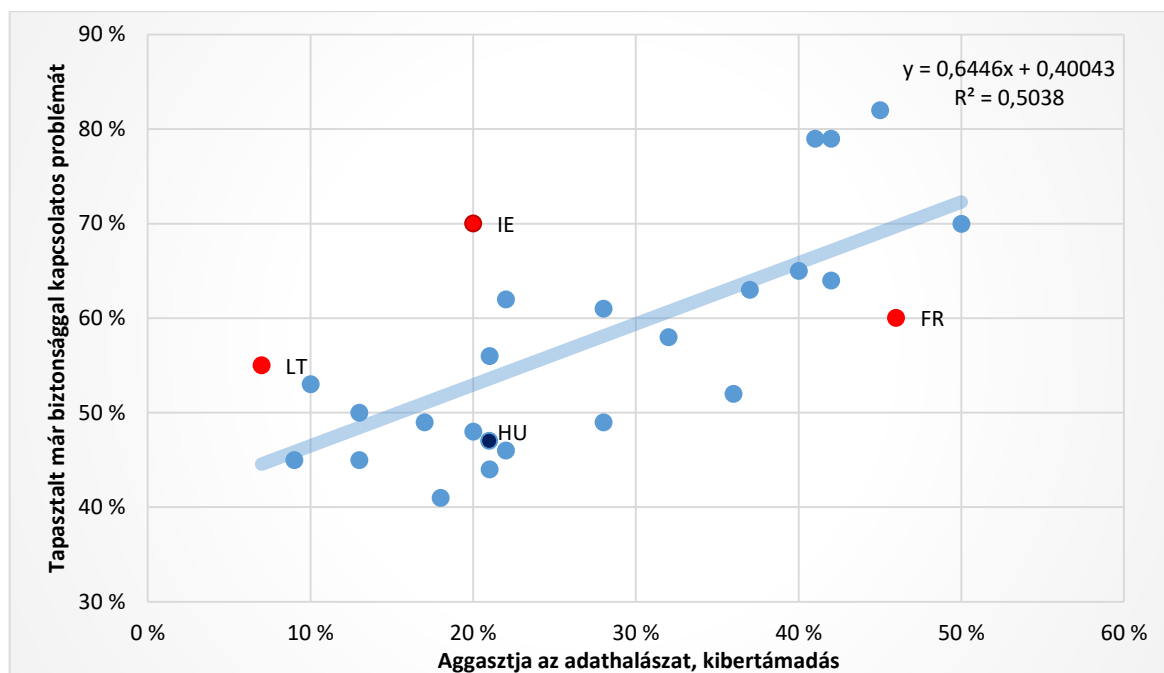


18. ábra: A tapasztalt biztonsággal kapcsolatos problémák és az aggodalom közötti kapcsolat- outlierok nélkül

Forrás: saját szerkesztés: (Eurostat, 2019.) és (Eurostat, 2019.c) alapján

A három ország eredményének figyelmen kívül hagyásával a Pearson-féle korrelációs elemzés értéke jóval magasabb lett: $r = +0,8675$, amely pozitív irányú, erős kapcsolatot mutat. A determinációs együttható értéke szintén magas, $R^2 = 0,7526$, ez szoros kapcsolatot feltételez. Vagyis az, hogy tapasztaltak-e már az országban valamilyen biztonsággal kapcsolatos problémát, 75,26%-ban befolyásolja az aggodalmat.

További vizsgálatom során az Európai Unió 518-as számú Eurobarometerének eredményeit használtam fel. Ez a kutatás 2021-es és a digitális jogokról és alapelvekről szól. Ebben a közleményben a kibertámadásokkal kapcsolatban is tettek fel kérdéseket a résztvevőktől. Összesen 26 530 fő válaszaiból készítették a statisztikákat. A felmérésből kiderült, hogy a válaszadók 56%-a aggódik a kibertámadások vagy az adathalászat miatt. (European Union, 2021.)

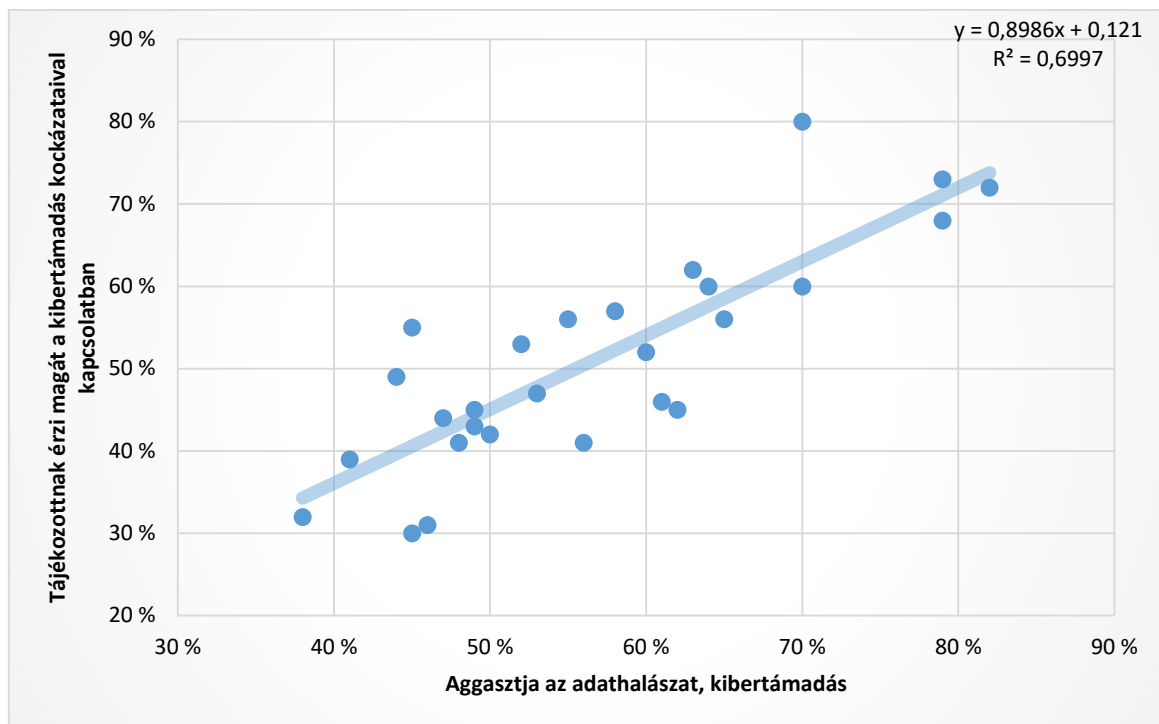


19. ábra: A tapasztalt biztonsággal kapcsolatos problémák és az aggodalom közötti kapcsolat

Forrás: saját szerkesztés: (Eurostat, 2019.) és (European Union, 2021.) alapján

Az ábrán láthatjuk, hogy a pontok nagyjából a trendvonal körül helyezkednek el. A korrelációs elemzés értéke $r=+0,7098$, amely a kiugró értékek figyelembevétele nélkül is pozitív irányú erős kapcsolatot feltételez. A kiugró értékek nélkül az eredmény $r=+0,8132$ és az R^2 értéke 0,6614-re nő.

A másik tényező, amire kiterjedt a vizsgálatom, az a kibertámadás kockázataival kapcsolatos tájékozottság. A következőkben megnézzük a kapcsolatot az aggodalom és a tájékozottság között.



20. ábra: A kibertámadással kapcsolatos tájékozottság és aggodalom kapcsolata

Forrás: saját szerkesztés: (Eurostat, 2019.) és (European Union, 2021.) alapján

Vizsgálataim során megállapítottam, hogy azokban az országokban, ahol a lakók tisztában vannak a kibertámadások okozta kockázatokkal, ott nagyobb arányban aggódnak miatta. A korreláció $r=+0,8364$, a determinációs együttható értéke pedig $0,6997$. Erős pozitív irányú kapcsolat van a két tényező között az egy kiugró érték figyelmen kívül hagyása nélkül is. A tájékozottság közel 70%-ban befolyásolja az aggodalmat.

Tehát elmondhatjuk, hogy az aggodalom egyik befolyásoló tényezője a rossz tapasztalat egy másik pedig a tájékozottság. **Azokban Európai Unió tagországokban, ahol a lakosság nagyobb aránya tapasztalt már valamilyen adatbiztonsággal kapcsolatos problémát az online térben és tájékozottabbak a kibertámadás kockázataival, ott nagyobb arányban aggódnak a kibertámadások miatt.**

5.4 SZEMÉLYES ADATOK VÉDELME

Az Európai Unió Statisztikai Hivatala által közzétett 2021-es felmérésben a Digital Skills Indicator 2.0 (DSI) azaz az egyének digitális készségi szintjét mérő mutatót vizsgálták. Az index az internet vagy szoftverhasználattal kapcsolatos tevékenységen alapul és az Európai Unió tagállamaiban mérik. A 2021-es mintanagyság az egyes tagállamokban 3 000 és 6 000 elem között volt. Célcsoport: 16-74 évesek. A mutató 5 dimenziót vesz figyelembe a vizsgálatkor, amelyen belül 30 indikátort vizsgálnak. (Eurostat, 2021.) Az 5 dimenzió a következő:

- Információ- és adatkultúra,
- Kommunikáció és együttműködés,
- Digitális tartalomkészítési ismeretek,
- Biztonsággal kapcsolatos készségek,
- Problémamegoldó készség.

A kutatásom során a témámhoz legjobban kapcsolódó dimenzióval, azaz a biztonsággal kapcsolatos készségekkel foglalkoztam. Ebben a dimenzióban a magánélet védelméért való cselekvést vizsgálják a digitális környezetben, melyek közé az alábbi tényezők tartoznak:



21. ábra: Adatvédelemmel kapcsolatos tevékenységek

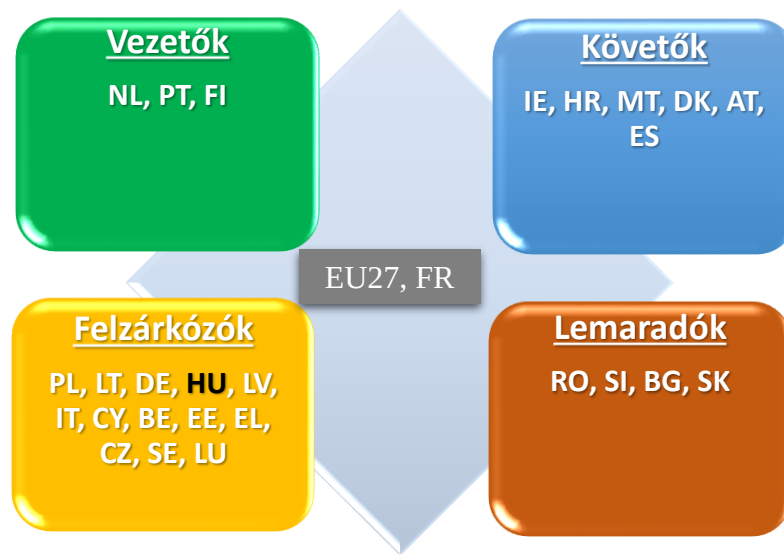
Forrás: saját szerkesztés (Eurostat, 2021.c) alapján

Kiegészítésképpen még két tevékenységet vizsgáltam, amelyekhez szintén az Eurostat 2021-es felmérésének eredményeit használtam:

- Az adatvédelmi nyilatkozat elolvasása a személyes adatok megadása előtt

- Kapcsolatfelvétel weboldalak vagy keresőmotorok adminisztrátorával az adatokhoz való hozzáférés, frissítés vagy törlés miatt. (Eurostat, 2022. d)

A vizsgálatom során azt vettem figyelembe, hogy a felsorolt tevékenységeket az egyes országban milyen arányban végzik és csoportokat alkottam az Uniós átlag függvényében. Minden tényező esetében rangsoroltam az országokat, majd átlagoltam a rangsorokat és az alapján megnéztem, hogy mely országok eredményei vannak messze az Európai Unió átlag alatt vagy fölött.



22. ábra: Országcsoporthok

Forrás: saját szerkesztés (Eurostat, 2021.c) és (Eurostat, 2022. d) alapján

Franciaországot nem tudtam besorolni egyik csoportba sem, mert az összesített eredménye megegyezik az Európai Unió átlagával. Az összesített rangsor alapján az Európai Unió a 10. helyen áll.

Ahogy a 22. ábra mutatja, a *Vezetők* közé soroltam Hollandiát, Portugáliát és Finnországot. Ez a három ország jóval az Unió átlag fölötti eredménnyel rendelkezik. Közülük mindegyik az összes figyelembe vett tényező esetében az átlag fölött teljesített.

A *Követők* csoportjába tartozik Írország, Horvátország, Málta, Dánia, Ausztria és Spanyolország. Ezek az országok habár az Unió átlag fölött helyezkednek el, eredményeik jóval a *Vezetők* alatt vannak.

A *Felzárkózók* közé soroltam Lengyelországot, Litvániát, Németországot, Magyarországot, Lettországot, Olaszországot, Ciprust, Belgiumot, Észtországot, Görögországot, Csehországot Svédországot és Luxemburgot. Ezek az országok már az Unió átlag alatt állnak.

A *Lemaradók* között van Románia, Szlovénia, Bulgária és Szlovákia. Szlovénia és Románia minden tényező esetében átlag alatti eredményt ért el.

6. KÖVETKEZTETÉSEK, JAVASLATOK

Az olvasottak alapján arra a következtetésre jutottam, hogy az Európai Unió általános adatvédelmi rendeletének hatálybalépése előtti 2 éves türelmi idő sok vállalat számára kevés volt a felkészülésre. A nagyobb vállalatoknak, akik foglalkoztatnak pl.: jogász munkatársakat, illetve nagyobb bevételi forrással rendelkeznek, azoknak egyszerűbb volt az implementálás. A kisebb cégeknek a rendelet megértése is nehézséget okozott, nem beszélve a hatalmas költségekről, amelyet be kellett fektetni például a munkatársak képzésére, új marketing eszközök alkalmazására vagy a biztonsági rendszer megerősítésére. Ráadásul az Unió tagállamok különböző fejlettségi szintje miatt is nehéz az azonos feltételeknek való megfelelés. Hosszútávon megtérülés lehet viszont az adatok tisztítása. A már szükségtelen adatok eltávolítása és a még szükséges információk rendezése hosszútávon kifizetődő lehet, hiszen egyszerűbb és gyorsabb egy rendezett és rendszerezett közegben dolgozni. Mivel a GDPR megszegésének súlyos büntetés lehet a következménye, akár 20 millió euró vagy az éves árbevétel 4%-a, ezért fontos, hogy a vállalatok betartsák a szabályokat. Az Európai Unió 2019-es Eurobarometer 478 kutatása szerint, amely közel 1 évvel a GDPR hatálybalépése után készült, 2019. elején a fogyasztók meglepően keveset tudtak a rendeletről. A válaszadók 1/3 része egyáltalán nem hallott még a GDPR-ról és a személyiségi jogokat is a résztvevők mindössze 31%-a ismerte. Az adatvédelmi nyilatkozatokat a válaszadók több mint fele 2020-ban és 2021-ben sem olvasta, főként azért, mert túl hosszúnak tartották. Javaslatom szerint mindenképp érdemes végigolvasni néhány adatvédelmi dokumentumot, hogy tudjuk, hogy pontosan miről szól, így a későbbiekben, már rá tudunk keresni a számunkra fontos részekre és nem lesz szükség az egész végig olvasására, hiszen ahogy tapasztaltam, a Google dokumentuma is nagyon hosszú.

A Google, a Facebook és a TikTok olyan weboldalak/alkalmazások, amelyet sokan napi szinten használunk. Az ingyenes használatért cserébe viszont a személyes adatainkkal fizetünk. Az adataink felhasználásával a vállalatok személyre szabhatják a tartalmakat és a hirdetéseket. A hirdetésekből származó bevételük teszi ki az árbevételük majdnem egészét, ezért mindent megtesznek annak érdekében, hogy begyűjtsék az adatainkat. A három vállalat adatvédelmi dokumentumain *dokumentumelemzést* végeztem, melynek keretében megállapítottam, hogy a Google adatvédelmi irányelve habár egyszerű szöveggel rendelkezik, teletűzdelték sok-sok linkkel, amely miatt nehezen követhetővé vált. A Google adatvédelmi irányelve jóval hosszabb, mint a Facebooké, nem volt elég egy délután, hogy mindent átolvassak. Tartalmaz jókedvű, rövid színes videókat, amellyel véleményem szerint el akarják vonni a figyelmünket a

lényegről, azaz arról, hogy mennyi adatot begyűjtenek rólunk. A Google adatvédelmi irányelve tehát egyértelműen fejlesztésre szorul.

A Facebook adatvédelmi dokumentuma könnyen értelmezhető, egyszerűen áttekinthető és logikusan felépített. Hiányosság viszont, hogy nem minden személyes adat gyűjtésére adnak magyarázatot. Egyik vállalat sem adja el az adatainkat 3. félnek. Mindkét dokumentumban tájékoztatást kapunk arról, hogy hogyan állíthatjuk le egyes személyes adataink begyűjtését. Összességében a TikTok adatvédelmi irányelve átlátható és kellően lényegre törő, ám a megfogalmazása helyenként ködös és sokszor nem derül ki pontosan, hogy mire is használnak egy-egy adatot. A személyiségi jogainkról megfelelően tájékoztatnak. Ami hiányosság, hogy habár a sütik törlését könnyen megtaláljuk a sütiszabályzatban, azt igencsak keresnünk kell, hogy hogyan módosíthatjuk az egyéb személyes adattal kapcsolatos beállításokat. Amikor megtaláltam és a linkre kattintottam, láttam, hogy angol nyelvű a tartalom. Véleményem szerint egy ilyen fontos témát, minden ország nyelvén elérhetővé kellene tenni. Továbbá mindenképpen megkönnyítené a dolgunkat, ha lenne egy keresési mező, amelybe kulcsszavakkal rákereshetnénk arra, amiről tudni szeretnénk.

Vizsgálataim során kiválasztottam egy tavaly nyári hetemet, amelynek következtében a Google és a Facebook alkalmazás esetében megvizsgáltam, hogy milyen adatokat találok elmentve magamról. A TikTok-ot nem használom. Mivel a Google összeköttetésben van a többi kapcsolódó alkalmazásával, így visszaneézhettem, hogy mikre kerestem rá, hol jártam, mennyi időt vett igénybe az odavezető út, milyen közlekedési eszközzel utaztam, hol volt szállásfoglalásom, mikor indult a repülőm. Megnézhettem, hogy azon a héten mely híreket és hirdetések néztem meg, milyen szöveget fordítottam le a Google Fordítóban, stb. A Facebookon leginkább az ismerősökkel való interakciókat találtam meg, ilyen például, hogy milyen személyekre kerestem rá, kiknek és mit kommentáltam, milyen csoportokhoz csatlakoztam. Egyrészt érdekes volt ezeket visszaneézni, másrészt pedig meghökkentő látni, hogy mennyi mindent tárolnak rólunk. Összességében arra a következtetésre jutottam, hogy ha nem teszünk ellene, akkor mindenféle információt begyűjtenek rólunk az alkalmazások. Azonban van rá lehetőségünk, hogy ezt megakadályozzuk, hiszen vannak olyan funkciók, amelyeket ki lehet kapcsolni vagy pedig megadhatjuk, hogy mennyi idő elteltével töröljék azokat. Ha pedig van lehetőségünk, éljünk vele! Továbbá érdemes odafigyelnünk, hogy a letölteni kívánt alkalmazások milyen adatokhoz kérnek hozzáférést, hiszen vannak, amelyek olyanokhoz is kérnek, amelyek nem kapcsolható össze a funkciójukkal.

2022 áprilisáig összesen 1 619 295 046 € büntetést szabtak ki a GDPR megszegése következményeként. Első helyen magasan Németország áll, ahová közel 120 ezer bejelentés

érkezett. Azonban amennyiben a 100 ezer lakosra nézzük az incidenseket, akkor Hollandia áll az első helyen 531 db bejelentéssel. Ez természetesen nem azt jelenti, hogy összesen ennyi incidens történt. 2019-ben például az Eurostat kutatása szerint az Unió állampolgárok közel 1/3 része tapasztalt már valamilyen adatbiztonsággal kapcsolatos problémát. Megvizsgáltam azt is, hogy az Európai Unió lakosok hajlandók-e tenni azért, hogy a vállalatok kevesebb adatot használjanak fel róluk. Ahogyan már említettem, sok adatgyűjtést megakadályozhatunk azzal, hogy módosítjuk az adatvédelmi beállításokat és sok esetben vissza is utasíthatjuk az adataink felhasználását. Léteznek olyan szoftverek, amelyek korlátozzák a nyomon követhetőségünket. Hollandiában, Finnországban és Portugáliában vannak a legnagyobb arányban azok, akik tesznek az adataik védelméért és Bulgáriában, Szlovákiában, Szlovéniában és Romániában tesznek a legkevesebbet. A legjellemzőbb adatvédelmi tevékenység a földrajzi helyhez való hozzáférés korlátozása, a személyes adatok reklámcélhoz való felhasználásának megtagadása és a hozzáférés korlátozása a közösségi oldalakon vagy megosztott online tárhelyeken található profilokhoz vagy tartalmakhoz. Az internetes tevékenységek korlátozására való szoftverek használata nem jellemző, mindössze a válaszadók 1/5 része használ ilyet. A felmérésben résztvevőkre a legkevésbé jellemző, hogy a keresőmotorok és a weboldalak adminisztrátoraival felveszik a kapcsolatot annak érdekében, hogy frissítsék vagy töröljék az adataikat. Vizsgálataim során arra a következtetésre jutottam, hogy azokban az országokban, ahol a felhasználók nagyobb aránya tapasztalt már valamilyen adatbiztonsági problémát, ott jobban aggódnak a kibertámadások miatt. Az aggodalmat az is befolyásolja, hogy mennyire vannak tisztában a kiberbűnözés kockázatával. Elmondhatjuk tehát, hogy amíg nem tapasztaltunk ilyet és nem is tudjuk, hogy mivel jár a kibertámadás, addig nem aggodalmaskodunk rajta.

Véleményem szerint az életünk minden területén fontos, hogy tisztában legyünk a jogainkkal és ha valami szabálytalansággal találkozunk, akkor éljük is velük. Az adatvédelem témaköre kiemelten fontossá vált az online tér bővülésével és érdemes utána járni, mi mit tehetünk adataink védelme érdekében. Sokszor egy pár perces utána járás is elég, hogy az adatvédelmi beállításokon módosítsunk és megakadályozzuk, hogy mindenféle adatot begyűjtsenek és felhasználjanak rólunk.

7. ÖSSZEGZÉS

Az évek során az online térben való részvételünknek köszönhetően a felhasznált adatok mennyisége is megnőtt. Vizsgálatom fókuszában a személyes adat és annak védelme áll. Személyes adat az, ami alapján beazonosíthatóak vagyunk. Például a nevünk, a telefonszámunk, az IP-címünk vagy a Neptun kódunk.

Az adatvédelem kialakulása Magyarországon az 1970-es évekre tehető. Országunkban jelenleg a 2011. évi CXII törvény (az információs önrendelkezési jogról és a közérdekű adatok nyilvánosságáról) van érvényben. A törvényben a személyes adatokon belül megkülönböztetik a különleges adatokat, amelyeket a vállalatoknak nem lehet felhasználni, csak kivételes esetekben. Idetartoznak például a biometrikus, az egészségügyi, a szexuális irányultsággal, a vallással és a faji hovatartozással kapcsolatos adatok.

Az Európai Parlament kiemelten fontosnak tartja, hogy legyen egy egységes, általános rendelet, amely szabályozza az Uniós vállalatokat. Jelenleg a GDPR, vagyis az Európai Unió általános adatvédelmi rendelete határozza meg a személyes adatok kezelését. A közel 100 oldalas rendelet a 2 éves türelmi időszakot követően 2018. május 25-én lépett hatályba és az Európai Unió területén működő vállalatokra, illetve azon EU területén kívül működő kívüli cégekre vonatkozik, amelyek árut értékesítenek vagy szolgáltatást nyújtanak az EU-n belül. A GDPR célja az, hogy irányítsa az adatok felhasználását, növelje a bizalmat, ösztönözze az adatok az adatvédelmi előírásoknak megfelelő megosztását, illetve újrafelhasználását, valamint biztosítsa az egyének saját személyes adatainak ellenőrzését. A rendeletnek köszönhetően a vállalatoknak számos szabályt be kell tartaniuk az adataink felhasználásával kapcsolatban. A vállalatok nehezen tudtak felkészülni az új szabályokra és azoknak, akik nem voltak a megfelelő fejlettségi szinten, magas költségekkel kellett számolni, hogy megerősítsék a biztonsági rendszereiket, ezzel megfeleljenek a kritériumoknak. Fontos, hogy betartsák a szabályokat, hiszen akár 20 millió euró vagy az éves árbevételük 4%-áig terjedő büntetést is kaphatnak, ha megszegik azokat. A GDPR bevezetése óta a legnagyobb büntetést az Amazon kapta, az adatvédelmi hatóság 855,9 millió dollárt szabott ki rájuk, mert a személyes adatok feldolgozása nem volt összhangban a rendelettel.

A vállalatoknak tájékoztatniuk kell az érintettet arról, hogy mi az adatkezelés célja és az adatokat csak addig használhatják fel, amíg nem teljesítik a célt. Az adatoknak pontosnak kell lenniük és csak annyit gyűjthetnek be, amennyi valóban szükséges a cél eléréséhez. A fogyasztók rendelkeznek személyiségi jogokkal, amelyek közé tartozik például a helyesbítés joga, így az adataink módosítását kérhetjük, ha azok nem pontosak. Továbbá a fogyasztóknak

jogukban áll hozzáférni a saját személyes adataikhoz. Tiltakozhatnak azellen, hogy direkt marketing célra használják fel az adataikat.

Az Egyesült Államokban nincs egységes adatvédelmi törvény, hanem olyan adatspecifikus törvények vannak, amelyek például az egészségügyi adatokat védik vagy a 13 éven aluli gyerekek adatainak gyűjtését tiltják. A kínai adatvédelmi törvény több ponton is hasonlít a GDPR-hez, bár rövidebb és kevésbé részletesebb. A legnagyobb különbség a két törvény között, hogy a kínai törvény nem rendelkezik a kormány személyes adatokhoz való hozzáféréséről, így a kormány korlátlanul fér hozzá az állampolgárok adataihoz. Vannak olyan országok Dél-Afrikában és Dél-Amerikában is, ahol az adatvédelmi törvények megsértéséért több évig terjedő börtönbüntetés jár.

Dolgozatomban dokumentumelemzést végeztem a Google, a Facebook és a TikTok adatvédelmi dokumentumaira vonatkozóan. A Google adatvédelmi irányelve illetve sűgőja rengeteg információval szolgál, de túl hosszú. A linkek száma egy oldalon akár 15 is lehet, így habár érthetőek a leírások, nehéz követni, könnyen elveszhetünk. A linkek egyes esetekben angol leíráshoz irányítanak, ami zavaró lehet. Azonban nem jogi szöveget használnak, hanem egyszerű leírást. További megállapításom, hogy az adatvédelmi tájékoztató egészét megpróbálják szépíteni. A tájékoztató videók kedvesek, jókedvűek, rövidek és informatívak. Bennem azt az érzést keltették, hogy a zenével és a színes videóval próbálják elvonni a figyelmet arról, amiket mondanak. A Facebook adatvédelmi dokumentumai rövidebbek, logikusan felépítettek, könnyen értelmezhetőek. A TikTok adatvédelmi irányelve átlátható és kellően lényegre törő, ám a megfogalmazása helyenként ködös és sokszor nem derül ki pontosan, hogy mire is használnak egy-egy adatot. Mindenképpen megkönnyítené a dolgunkat, ha lenne egy keresési mező, amelybe kulcsszavakkal rákereshetnénk arra, amiről tudni szeretnénk. A személyiségi jogainkról megfelelően tájékoztatnak.

Megvizsgáltam, hogy a két óriásvállalat, a Google és a Facebook milyen adatokat gyűjt be rólunk és mire használják fel azokat. Utána néztem, hogy egy tavaly nyári hetemet visszakeresve a két alkalmazás segítségével milyen adatokra bukkanok. Az előzményeim között találkozhattam azzal, hogy azon a héten mikor, hová mentem, milyen közlekedési eszközzel utaztam és azon hány percet töltöttem. Láttam, hogy a Google Hírek és Hirdetések közül melyekre kattintottam rá, milyen szöveget fordítottam le a Fordítóval. A Google emlékezett arra, hogy milyen weboldalakat nyitottam meg és mikre kerestem rá. A Facebookon láthattam például, hogy azon a héten milyen csoporthoz csatlakoztam, kik lettek az ismerőseim, kinek a képéhez kommenteltem, kire kerestem rá, mikor jelentkeztem be az alkalmazásba, milyen videókat néztem meg.

Láthatjuk tehát, hogy mennyi mindent elmentenek rólunk az alkalmazások, ha hagyjuk. Ám mindhárom vállalat esetében megtalálhatjuk az adatkezelési tájékoztatóban, hogy hogyan kapcsolhatjuk ki az egyes funkciókat, amelyekkel begyűjtik az adatokat. Ezzel sok adatgyűjtést megakadályozhatunk. Ha problémánk van, létezik adatvédelmi hatóság, ahová bejelenthetjük azt. Az Unió fogyasztók 21 %-a tudja, hogy melyik hivatal foglalkozik az adatvédelemmel az országában. A DLA Piper minden évben végez felmérést a bejelentett adatvédelmi incidensek számáról. Az általános adatvédelmi rendelet hatálybalépése óta 2022 áprilisáig összesen 1 619 295 046 € büntetést szabtak ki a GDPR megszegése következményeként. A legtöbb esetet, közel 120 ezer darabot Németországban jelentettek 2018 májusa és 2022 januárja között. Magyarországon ezalatt mindössze 2 150 db jelentés történt.

Az Eurostat kutatásai szerint a leggyakrabban tapasztalt adatbiztonsági probléma az adathalászat, ezt már az Unióban élő válaszadók 25%-a tapasztalta. A következő leggyakrabban előforduló gond 13%-os eredménnyel a személyes adatokat kérő hamis webhelyekre való átirányítás. Összességében a válaszadók közel egyharmada, 32%-a tapasztalta már adatbiztonsági problémát. A válaszadók 45%-ánál előfordult már, hogy nem végzett el valamilyen tevékenységet az interneten a biztonsággal kapcsolatos aggodalmai miatt. A vizsgálataim során arra a következtetésre jutottam, hogy az aggodalom egyik befolyásoló tényezője a rossz tapasztalat, egy másik pedig a tájékozottság. Azokban Európai Unió tagországokban, ahol a lakosság nagyobb aránya tapasztalt már valamilyen adatbiztonsággal kapcsolatos problémát az online térben és tájékozottabbak a kibertámadás kockázataival, ott nagyobb arányban aggódnak a kibertámadások miatt. Az outlierok figyelmen kívül hagyásával a Pearson-féle korrelációs elemzés és a determinációs együttható eredménye pozitív irányú szoros kapcsolatot feltételez mindkét esetben. Például az, hogy tapasztaltak-e már az országban valamilyen biztonsággal kapcsolatos, problémát, 75,26%-ban befolyásolja az aggodalmat.

További célom az volt, hogy megvizsgáljam, hogy az Unió internetfelhasználók tesznek-e annak érdekében, hogy minél kevesebb adatot gyűjtsenek be róluk a vállalatok. Ehhez az Eurostat 2021-es kutatási eredményeit használtam fel és csoportokba rendeztem az országokat. A legtöbben Hollandiában, Portugáliában és Finnországban tesznek az adataik védelme érdekében, így ők tartoznak a Vezetők csoportba. Magyarország a Felzárkózók között van, az Unió átlag alatti összesített eredménnyel.

8. IRODALOMJEGYZÉK

Jogszabályok:

1. 15/1991. (IV. 13.) AB határozat, 1991.
2. 1977. évi IV. törvény, 1977. 1977. évi IV. törvény a Magyar Népköztársaság Polgári Törvénykönyvéről szóló 1959. évi IV. törvenymódosításáról és egységes szövegéről, 83. §.
3. 1989. évi XXXI. törvény, 1989.. 1989. évi XXXI. törvény az Alkotmány módosításáról.
4. 1992. évi LXIII. törvény, 1992. 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról.
5. 2003. évi XLVIII. törvény, 2013. a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény módosításáról.
6. 2011. évi CXII törvény, 2011. 2011. évi CXII törvény az információs önrendelkezési jogról és a közérdekű adatok nyilvánosságáról. hely nélk.:ismeretlen szerző
7. 2018. évi XXXVIII. törvény, 2018. az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról
8. CCPA, 2018.. State of California Department of Justice.
9. Egyesült Nemzetek Szervezete, 1948: Emberi Jogok Egyetemes Nyilatkozata
10. Európai Parlament és Tanács, 2016.. Európai Parlament és Tanács 2016/679 rendelete.
11. Európai Parlament és a Tanács 95/46/EK irányelve, 1995.
12. Európai Tanács, 1950.. Emberi Jogok Európai Egyezménye.
13. Európai Tanács, 1981.. 1981. évi, 108. sz. egyezmény.
14. GDPR, 2016.. az Európai Unió általános adatvédelmi rendelete

Szakirodalom:

15. DLA Piper, 2019.. *Sweden.dlapiper.com*. [Online]
Available at:
<https://www.dlapiper.com/~media/files/insights/publications/2019/02/dla-piper-gdpr-data-breach-survey-february-2019.pdf>.
[Hozzáférés dátuma: 20. október 2021.].
16. DLA Piper, 2020.. *Sweden.dlapiper.com*. [Online]
Available at:
https://sweden.dlapiper.com/sites/default/files/node/field_download/DLA%20Piper_Data%20Breach%20Report%202020.pdf
[Hozzáférés dátuma: 20. október 2021.].

17. DLA Piper, 2021.. *Sweden.dlapiper.com*. [Online]
Available at:
https://sweden.dlapiper.com/sites/default/files/node/field_download/Data%20Breach%20Report%202021.pdf
[Hozzáférés dátuma: 20. október 2021.].
18. DLA Piper, 2022.c. *DLA Piper*. [Online]
Available at:
https://www.lawyerpress.com/wordpress/wp-content/uploads/2022/01/Data-Breach-Report-2022_DLAPIPER.pdf
[Hozzáférés dátuma: 7. március 2022.].
19. Európai Unió, 2021.. *Az Európai Unió ismertetése- A személyes adatok védelme*. [Online]
Available at:
https://www.europarl.europa.eu/ftu/pdf/hu/FTU_4.2.8.pdf
[Hozzáférés dátuma: 13 március 2022.].
20. European Commission, 2007.. *European Commission*. [Online]
Available at:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf
[Hozzáférés dátuma: 2. március 2022.].
21. European Commission, 2015.. *An official website of the European Union*. [Online]
Available at:
<https://docplayer.net/18497515-Special-eurobarometer-431-data-protection-report.html>
[Hozzáférés dátuma: 9. október 2021.].
22. Hunkár, M., 2013. *A kutatás módszertana*.
23. Kaszián, Á. G., 2021.. *Jogi Fórum*. [Online]
Available at:
https://www.jogiforum.hu/wp-content/uploads/2021/09/kaszian-abel_a-GDPR-kinai-unokatestvere_cimlappal-1.pdf
[Hozzáférés dátuma: 15. április 2022.].
24. Keith a Quesenberry, 2020. *Social Media Strategy*
25. Kérdő, A., 2008.. *A tartalomelemzés elmélete és gyakorlata*.
26. Kiss et al., P., 2006.. *ELTE, BTK Gépeskönyv*. [Online]
Available at:
<http://gepeskonyv.btk.elte.hu/adatok/Pszichologia/123Kiss/munkafuzet.pdf>
[Hozzáférés dátuma: 23. 10. 2022.].
27. McDermott Will & Emery LLP, 2018.. [Online]
Available at: https://iapp.org/media/pdf/resource_center/Ponemon_race-to-gdpr.pdf
[Hozzáférés dátuma: 13. április 2022.].
28. Nicholas Papagiannis, 2022. *Effective SEO and Content Marketing*
29. Szőke, G. L., 2013.. *Az adatvédelem szabályozásának történeti áttekintése. Infokommunikáció és jog*, Issue 56.,
30. NAIH, 2021. [Online]
Available at:
<https://www.naih.hu/files/ADATV-DELMI-SZ-T-R.pdf>
[Hozzáférés dátuma: 30 09 2021].

Egyéb:

31. *Social dilemma*. 2020.. [Film] Rendezte: Jeff Orlowski. Egyesül Államok: Exposure Labs, Argent Pictures, The Space Program.

Online források:

32. Adquadrant.com, 2020.. *Adquadrant.com*. [Online]
Available at:
<https://www.adquadrant.com/blog/what-is-a-tracking-pixel>
[Hozzáférés dátuma: 11. szeptember 2021.].
33. Apple, S., 2022.. *Apple Support*. [Online]
Available at:
<https://support.apple.com/hu-hu/HT211970>
[Hozzáférés dátuma: 2. április 2022.].
34. Balázs, M., 2022.. *Máté Balázs*. [Online]
Available at:
<https://matebalazs.hu/keresomotor.html>
[Hozzáférés dátuma: 1. április 2022.].
35. Balázs, M., 2022. *matebalazs.hu*. [Online]
Available at:
<https://matebalazs.hu/seo.html>
[Hozzáférés dátuma: 1. április 2022.].
36. BBC, 2020.. *BBC*. [Online]
Available at: <https://www.bbc.com/news/technology-52758787>
[Hozzáférés dátuma: 20. április 2022.].
37. Blazyte, A., 2018.. *statista.com*. [Online]
Available at:
<https://www.statista.com/chart/16317/share-of-e-commerce-apps-collecting-and-using-personal-data-in-china/>
[Hozzáférés dátuma: 15. november 2021.].
38. Bolcsó, D., 2019. *index.hu*. [Online]
Available at:
https://index.hu/techtud/2019/01/24/facebook_lehallgatas_celzott_hirdetes_reklam_ad_atvedelem_adatgyujtes/
[Hozzáférés dátuma: 1 április 2022.].
39. Britannica Inc., 1998.. *Britannica*. [Online]
Available at:
<https://www.britannica.com/topic/dactyloscopy>
[Hozzáférés dátuma: 9. április 2022.].
40. Business of Apps, 2022. *Business of Apps*. [Online]
Available at: <https://www.businessofapps.com/data/tik-tok-statistics/>
[Hozzáférés dátuma: 16. október 2022.].
41. Chevalier, S., 2022.. *Statista*. [Online]
Available at:
<https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/>
[Hozzáférés dátuma: 12. április 2022.].

42. Cisco, 2021.. *Cisco*. [Online]
Available at:
<https://blogs.cisco.com/security/maintaining-data-privacy-in-the-age-of-covid>
[Hozzáférés dátuma: 7. január 2022.].
43. Cleary, G., 2018.. *Broadcom software*. [Online]
Available at:
<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/mobile-privacy-apps>
[Hozzáférés dátuma: 18. április 2022.].
44. CMS.Law, 2022.. *GDPR Enforcement Tracker*. [Online]
Available at:
<https://www.enforcementtracker.com/?insights>
[Hozzáférés dátuma: 12. április 2022.].
45. Cohen, J., 2021. *PcMag*. [Online]
Available at:
<https://www.pcmag.com/how-to/social-media-and-food-delivery-apps-sell-the-most-personal-data>
[Hozzáférés dátuma: 23. április 2022.].
46. Cohen, J., 2022. a. *PcMag*. [Online]
Available at: <https://www.pcmag.com/news/amazons-alexa-collects-more-of-your-data-than-any-other-smart-assistant>
[Hozzáférés dátuma: 23. április 2022.].
47. Cohen, J., 2022. b. *PcMag*. [Online]
Available at:
<https://www.pcmag.com/news/sick-of-data-collection-try-these-apps-instead>
[Hozzáférés dátuma: 23- április 2022.].
48. Data Privacy Manager, 2020.. *Data Privacy Manager*.. [Online]
Available at:
<https://dataprivacymanager.net/725000e-gdpr-fine-by-dutch-dpa-for-collecting-employees-fingerprints/>
[Hozzáférés dátuma: 12. április 2022.].
49. Data Privacy Manager, 2021.. *Data Privacy Manager*. [Online]
Available at:
<https://dataprivacymanager.net/what-is-personally-identifiable-information-pii/>
[Hozzáférés dátuma: 5. november 2021.].
50. Data Privacy Manager, 2022.. *Data Privacy Manager*.. [Online]
Available at:
<https://dataprivacymanager.net/cnil-fines-google-and-facebook-a-total-of-e210-million-over-cookies/?hsCtaTracking=24b0cdc0-1a8b-4a01-8988-3864c8abb00a%7C04410248-f0a1-4005-8986-74c126691a29>
[Hozzáférés dátuma: 12. április 2022.].
51. DataReportal, 2022.. *DataReportal*. [Online]
Available at:
<https://datareportal.com/global-digital-overview>
[Hozzáférés dátuma: 29. október 2022.].

52. Digitrendi, 2020.. *digitrendi.hu*. [Online]
Available at:
<https://digitrendi.hu/a-gdpr-alaposan-felforgatja-a-cegek-eletet-biztos-allasa-van-a-dpo-knak/>
[Hozzáférés dátuma: 2. október 2021.].
53. DIW, 2022.. *Digital Information World*. [Online]
Available at: <https://www.digitalinformationworld.com/2022/04/data-reveals-tiktok-dominates-facebook.html>
[Hozzáférés dátuma: 16. október 2022.].
54. DLA Piper, 2021.. *DLA Piper*. [Online]
Available at:
<https://www.dlapiperdataprotection.com/index.html?t=law&c=VE&c2=>
[Hozzáférés dátuma: 11. április 2022.].
55. DLA Piper, 2022. b. *DLA Piper*.. [Online]
Available at: <https://www.dlapiperdataprotection.com/index.html?t=law&c=CA>
[Hozzáférés dátuma: 13. április 2022.].
56. DLA Piper, 2022.. *DLA Piper*. [Online]
Available at:
<https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=CN>
[Hozzáférés dátuma: 1. április 2022.].
57. Donegan, C., 2019.. *SalesForce*. [Online]
Available at:
<https://www.salesforce.com/news/stories/state-of-the-connected-customer-report-outlines-changing-standards-for-customer-engagement/>
[Hozzáférés dátuma: 22. szeptember 2021.].
58. Doyle, B., 2022. *Walloo*. [Online]
Available at:
<https://wallaroomedia.com/blog/social-media/tiktok-statistics/>
[Hozzáférés dátuma: 16. október 2022.].
59. DPMK, 2018.. *Digitális Pedagógiai Módszertani Központ*. [Online]
Available at:
<https://dpmk.hu/2018/08/22/mit-jelent-a-gdpr-az-oktatasi-intezmenyekre-nezve/>
60. dr. Horváth, K., 2020.. *hsw.hu*. [Online]
Available at:
<https://www.hsw.hu/hirek/61519/ai-mi-gazdasag-gdpr-adatkezeles.html>
[Hozzáférés dátuma: 23. szeptember 2021.].
61. EDPB, 2020. a. *European Data Protection Board*.. [Online]
Available at:
https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en
[Hozzáférés dátuma: 29. október 2021.].
62. EDPB, 2020. b. *European Data Protection Board*. [Online]
Available at:
https://edpb.europa.eu/news/national-news/2020/personal-data-breach-breidholt-upper-secondary-school-administrative-fine_hu
[Hozzáférés dátuma: 20. április 2022.].

63. Európai Bizottság, 2018. *Az Európai Unió hivatalos portáljához tartozó weboldal.* [Online]
Available at:
https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hu
[Hozzáférés dátuma: 2. október 2021.].
64. Európai Bizottság, 2021.b. *Az Európai Unió hivatalos portáljához tartozó weboldal.* [Online]
Available at:
https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_hu
[Hozzáférés dátuma: 29. szeptember 2021.].
65. Európai Unió, 2018. *Az Európai Unió hivatalos portáljához tartozó weboldal.* [Online]
Available at:
https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_hu.htm#shortcut-0
[Hozzáférés dátuma: 2. október 2021.].
66. Európai Unió, 2021.c. *Az Európai Unió hivatalos portáljához tartozó weboldal.* [Online]
Available at:
https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_hu.htm
[Hozzáférés dátuma: 29. szeptember 2021.].
67. European Commission, 2019.. *An official website of the European Union, Special Eurobarometer.* [Online]
Available at:
<https://europa.eu/eurobarometer/surveys/detail/2222>
[Hozzáférés dátuma: 2. október 2021.].
68. European Union, 2018. *Data Europa.* [Online]
Available at:
<https://data.europa.eu/en/highlights/protecting-data-and-opening-data>
[Hozzáférés dátuma: 3. október 2021.].
69. Eurostat, 2019.. *Eurostat.* [Online]
Available at:
https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCI_PB/default/table?lang=en&category=isoc.isoc_i.isoc_ci_sci
[Hozzáférés dátuma: 29. 10. 2022.].
70. Eurostat, 2019.b. *Eurostat.* [Online]
Available at:
https://ec.europa.eu/eurostat/cache/metadata/en/isoc_i_esms.htm
[Hozzáférés dátuma: 29 10. 2022.].
71. Eurostat, 2019.c. *Eurostat.* [Online]
Available at:
https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCI_AX/default/table?lang=en&category=isoc.isoc_i.isoc_ci_sci
[Hozzáférés dátuma: 25 10. 2022.].

72. Eurostat, 2020.. *Eurostat*. [Online]
Available at:
https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCI_PRV20_custom_1940277/bookmark/table?lang=en&bookmarkId=fe380ed5-848c-47b9-bfe7-6ce37d6441bd
[Hozzáférés dátuma: 18. április 2022.].
73. Eurostat, 2021.. *Eurostat*. [Online]
Available at:
https://ec.europa.eu/eurostat/cache/metadata/en/isoc_sk_dskl_i21_esmsip2.htm
[Hozzáférés dátuma: 24. 10. 2022.].
74. Eurostat, 2021.c. *Eurostat*. [Online]
Available at:
https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCI_PRV20_custom_3681576/default/bar?lang=en
[Hozzáférés dátuma: 21. október 2022.].
75. Eurostat, 2022. d. *Eurostat*. [Online]
Available at:
https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCI_PRV20_custom_3718378/default/table?lang=en
[Hozzáférés dátuma: 29. október 2022.].
76. Facebook, 2022.. *Facebook*. [Online]
Available at:
<https://www.facebook.com/privacy/explanation/>
[Hozzáférés dátuma: 15. április 2022.].
77. Felix, R., 2021.. *Statista.com*. [Online]
Available at:
<https://www.statista.com/chart/24495/apps-sharing-personal-information-with-third-parties/>
[Hozzáférés dátuma: 22. április 2022.].
78. Finge, 2015.. *Conversionlab*. [Online]
Available at:
<https://conversionlab.no/4-clever-tools-to-run-your-business-the-smart-way/google-apps-1024x575/>
[Hozzáférés dátuma: 23. április 2022.].
79. Finkle, J. S.-J., 2017.. *Reuters*. [Online]
Available at:
<https://www.reuters.com/article/us-yahoo-cyber-idUSKCN1C82O1>
[Hozzáférés dátuma: 12. április 2022.].
80. Firdaus, M., 2017.. *Research Gate*. [Online]
Available at:
https://www.researchgate.net/figure/Internet-Users-in-The-World_fig1_341591819
[Hozzáférés dátuma: 9. április 2022.].
81. Flachner, B., 2022.. *Telex*. [Online]
Available at:
<https://telex.hu/komplex/2022/02/10/metaverzum-nft-blokk lanc-kripto valuta-microsoft-meta-videojatek-next-earth-1>
[Hozzáférés dátuma: 23. április 2022.].

82. Florian Zandt, 2021.. *Statista.com*. [Online]
Available at:
<https://www.statista.com/chart/25691/highest-fines-for-gdpr-breaches/>
[Hozzáférés dátuma: 12. szeptember 2021.].
83. Forbes, 2021.. *Forbes*. [Online]
Available at:
<https://forbes.hu/uzlet/meta-facebook-metaverzum-video/>
[Hozzáférés dátuma: 10. április 2022.].
84. Fowler, G. A., 2020.. *The Washington Post*. [Online]
Available at:
<https://www.washingtonpost.com/technology/2020/07/13/tiktok-privacy/>
[Hozzáférés dátuma: 23. október 2022.].
85. GDPR Specialisták, 2020.. *GDPR Specialisták*. [Online]
Available at:
<https://gdprspecialistak.hu/20-millio-ft-birsag-kameras-megfigyeles-miatt>
[Hozzáférés dátuma: 13. április 2022.].
86. Google Súgó, 2022.. *Google Súgó*. [Online]
Available at:
<https://support.google.com/?hl=hu>
[Hozzáférés dátuma: 15. március 2022.].
87. Google, 2022.. *Google Általános adatvédelmi és szerződési feltételek*. [Online]
Available at:
<https://policies.google.com/privacy?hl=hu>
[Hozzáférés dátuma: 15. március 2022.].
88. Google, 2022. b. *Google Ads Súgó*. [Online]
Available at:
<https://support.google.com/google-ads/answer/6316?hl=hu>
[Hozzáférés dátuma: 15. április 2022.].
89. Grace Lau, 2021.. *business2community.com*. [Online]
Available at:
<https://www.business2community.com/strategy/why-companies-are-struggling-with-becoming-gdpr-compliant-02421083>
[Hozzáférés dátuma: 13. április 2022.].
90. Habók, L., 2018.. *hwsz.hu*. [Online]
Available at:
<https://www.hwsz.hu/hirek/59643/gdpr-joint-venture-baker-mckenzie-naih-adatvedelem.html>
[Hozzáférés dátuma: 2. október 2021.].
91. Habók, L., 2019. *HWSZ*. [Online]
Available at:
<https://www.hwsz.hu/hirek/59894/gdpr-cnll-adatvedelmi-hatosag-google-buntetes.html>
[Hozzáférés dátuma: 12. szeptember 2021.].

92. Huddleston, T., 2022.. *CNBC*. [Online]
Available at:
<https://www.cnn.com/2022/02/08/tiktok-shares-your-data-more-than-any-other-social-media-app-study.html>
[Hozzáférés dátuma: 23. október 2022.].
93. IMD, 2021.. *IMD World Competitiveness Center*. [Online]
Available at:
<https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/>
[Hozzáférés dátuma: 24. április 2022.].
94. Jennifer Lund, 2021.. *Super Office*. [Online]
Available at:
<https://www.superoffice.com/blog/gdpr/>
[Hozzáférés dátuma: 13. április 2022.].
95. Johnson, J., 2022. b. *Statista.com*. [Online]
Available at:
<https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/>
[Hozzáférés dátuma: 23. április 2022.].
96. Johnson, J., 2022.. *Statista.com*. [Online]
Available at:
<https://www.statista.com/statistics/266249/advertising-revenue-of-google/>
[Hozzáférés dátuma: 23. április 2022.].
97. Kozma-Almási, Z. M., 2022.. *Technology's Legal Edge*. [Online]
Available at:
<https://www.technologyslegaledge.com/2022/04/record-gdpr-fine-by-the-hungarian-data-protection-authority-for-the-unlawful-use-of-artificial-intelligence/#more-6503>
[Hozzáférés dátuma: 18. április 2022.].
98. Lars Coudal, 2019.. *cleverplugins.com*. [Online]
Available at:
<https://cleverplugins.com/pros-cons-gdpr/>
[Hozzáférés dátuma: 2. október 2021.].
99. Martin, J., 2021.. *Tech Advisor*. [Online]
Available at: <https://www.techadvisor.com/feature/internet/what-is-vpn-3672526/>
[Hozzáférés dátuma: 23. április 2022.].
100. Microsoft, 2022.. *Microsoft*. [Online]
Available at:
<https://www.microsoft.com/hu-hu/security/business/security-101/what-is-a-cyberattack>
[Hozzáférés dátuma: 30 október 2022.].
101. Miller, T. C.-J., 2018.. *BBC News*. [Online]
Available at:
<https://www.bbc.com/news/business-44599968>
[Hozzáférés dátuma: 1. október 2021.].
102. Morning Consult, 2019.. *Morning Consult Intelligence*. [Online]
Available at:
<https://verizon.morningconsultintelligence.com/>
[Hozzáférés dátuma: 8. november 2021.].

103. MTI, 2019.. *HVG*. [Online]
Available at:
https://hvg.hu/gazdasag/20191030_birsag_buntetes_facebook_cambridge_analytica_facebook
[Hozzáférés dátuma: 2. január 2022.].
104. New Technology, 2020.. *newtechnology.hu*. [Online]
Available at:
<https://newtechnology.hu/hogyan-valtoztatta-meg-a-gdpr-a-vallalatok-mukodeset/>
[Hozzáférés dátuma: 2. október 2021.].
105. Nurunnabi, M., 2010.. *Research Gate*. [Online]
Available at:
https://www.researchgate.net/figure/Internet-users-in-the-world-growth-1995-2010-Adapted-from-com-statshtm_fig1_281029160
[Hozzáférés dátuma: 9. április 2022.].
106. O'Flaherty, K., 2021. *Wired*. [Online]
Available at:
<https://www.wired.co.uk/article/tiktok-data-privacy>
[Hozzáférés dátuma: 17. október 2022.].
107. Origo.hu, 2020.. *Origo.hu*. [Online]
Available at:
<https://www.origo.hu/gazdasag/20200227-miert-kovetik-a-reklamok-az-interneten.html>
[Hozzáférés dátuma: 11. szeptember 2021.].
108. Origo, 2021.. *Origo.hu*. [Online]
Available at:
<https://www.origo.hu/gazdasag/20210816-adatlopas-kiberbiztonsag-hacker-gazdasag.html>
[Hozzáférés dátuma: 5. október 2021.].
109. Pánszky, G., 2022.. *Panszky.hu*. [Online]
Available at:
<https://panszky.hu/100-millio-forintra-birsagolta-a-naih-a-digi-tavkozlesi-es-szolgaltato-kft-t-adatvedelmi-jogsertes-miatt/>
[Hozzáférés dátuma: 20 április 2022.].
110. Papp, A. K., 2018.. *Jogászvilág*. [Online]
Available at:
<https://jogaszvilag.hu/szakma/a-profilalkotas-adatvedelmi-szabalyai/>
[Hozzáférés dátuma: 4. november 2021.].
111. Pew Research Center, 2019.. *Pew Research Center*. [Online]
Available at:
<https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>
[Hozzáférés dátuma: 8. november 2021.].
112. Portfolio.hu, 2021. c. *Portfolio.hu*. [Online]
Available at:
<https://www.portfolio.hu/uzlet/20210903/brutalis-gdpr-birsag-a-whatsappnak-a-felhasznalok-adataival-zsonglorkodtek-499034>
[Hozzáférés dátuma: 12. szeptember 2021.].

113. Portfolio, 2021. a. *Portfolio*. [Online]
Available at:
<https://www.portfolio.hu/uzlet/20210611/adatlopas-a-mcdonaldsnal-es-a-volkswagennel-487742#>
[Hozzáférés dátuma: 5. október 2021.].
114. Portfolio, 2021. b. *Portfolio.hu*. [Online]
Available at: <https://www.portfolio.hu/gazdasag/20210820/elfogadtak-ma-kinai-gdpr-torvenyt-de-nagyon-mas-mint-az-europai-497240>
[Hozzáférés dátuma: 9. április 2022.].
115. ProfiNet, 2019.. [Online]
Available at:
<https://elemzeskozpont.hu/vallalkozas/gdpr-osszefoglalo-gdpr-lenyege-gyakorlati-tanacsok>
[Hozzáférés dátuma: 22. szeptember 2021.].
116. Reklamjog.hu, 2021.. *Reklámjog*. [Online]
Available at:
<https://reklamjog.hu/adatvedelem>
[Hozzáférés dátuma: 25. szeptember 2021.].
117. Richardson, B., 2022. *VPV overview*. [Online]
Available at:
<https://vpnoverview.com/unblocking/censorship/access-tiktok/>
[Hozzáférés dátuma: 16. október 2022.].
118. Sam Shead, 2021.. *CNBC*. [Online]
Available at:
<https://www.cnn.com/2021/07/30/amazon-hit-with-fine-by-eu-privacy-watchdog-.html>
[Hozzáférés dátuma: 12. szeptember 2021.].
119. Sandorf, B., 2021.. *Reviews.org*. [Online]
Available at:
<https://www.reviews.org/home-security/smart-assistant-privacy-what-data-is-collected-and-how-to-protect-yourself/>
[Hozzáférés dátuma: 23. április 2022.].
120. Satija, B., 2022.. *Reuters*. [Online]
Available at:
<https://www.reuters.com/technology/tiktoks-ad-revenue-surpass-twitter-snapchat-combined-2022-report-2022-04-11/>
[Hozzáférés dátuma: 23. október 2022.].
121. Saxena, P., 2022. *Appinventiv*. [Online]
Available at:
<https://appinventiv.com/blog/top-tiktok-statistics/>
[Hozzáférés dátuma: 17. október 2022.].
122. Secureinfo, 2019.. *secureinfo.com*. [Online]
Available at:
<https://www.securinfo.hu/termek/videotechnika/9095-gdpr-es-videomegfigyeles-az-erintettek-azonositasanak-kerdesei.html>
[Hozzáférés dátuma: 18. április 2022.].

123. SecureInfo, 2020.. *secureinfo.hu*. [Online]
Available at:
<https://www.securinfo.hu/termek/piacok/adatvedelem/10672-hogy-allunk-gdpr-el-gdpr-elmult-ket-eve-europaban-es-itthon.html>
[Hozzáférés dátuma: 2. október 2021.].
124. Sherman, P., 2022.. *VPN overview*. [Online]
Available at:
<https://vpnoverview.com/privacy/social-media/tiktok-privacy/>
[Hozzáférés dátuma: 17. október 2022.].
125. skillcultur.com, 2021.. *SkillCultur*. [Online]
Available at:
<https://skillcultur.com/the-full-history-of-data-protection/>
[Hozzáférés dátuma: 2. október 2021.].
126. Statista.com, 2022. b. *Statista.com*. [Online]
Available at:
<https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/>
[Hozzáférés dátuma: 26 10. 2022.].
127. Statista.com, 2022.d. *Statista.com*. [Online]
Available at:
<https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>
[Hozzáférés dátuma: 20. október 2022.].
128. Statista.com, 2022.. *Statista.com*. [Online]
Available at:
<https://www.statista.com/statistics/1305708/tiktok-ad-revenue/>
[Hozzáférés dátuma: 23. október 2022.].
129. Statista, R. D., 2022. b. *Statista.com*. [Online]
Available at:
<https://www.statista.com/statistics/778191/active-facebook-advertisers/>
[Hozzáférés dátuma: 23 április 2022.].
130. Statista, R. D., 2022. c. *Statista.com*. [Online]
Available at:
<https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>
[Hozzáférés dátuma: 23. április 2022.].
131. Statista, R. D., 2022.. *Statista.com*. [Online]
Available at:
<https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/>
[Hozzáférés dátuma: 23. április 2022.].
132. STH, 2022.. *Software Testing Help*. [Online]
Available at:
<https://www.softwaretestinghelp.com/most-downloaded-apps/>
[Hozzáférés dátuma: 17. október 2022.].

133. Szép, Á. O., 2021. *drszep.hu*. [Online]
Available at:
<https://drszep.hu/gdpr-rendelet/>
[Hozzáférés dátuma: 15. október 2021.].
134. Szőke, G. L., 2013.. Az adatvédelem szabályozásának történeti áttekintése. *Infokommunikáció és jog*, Issue 56., pp. 107-112..
135. Taylor, D., 2022.. *Guru*. [Online]
Available at:
<https://www.guru99.com/what-is-big-data.html>
[Hozzáférés dátuma: 24. április 2022.].
136. TikTok, 2021.. *TikTok*. [Online]
Available at:
<https://www.tiktok.com/legal/page/eea/privacy-policy/hu-HU>
[Hozzáférés dátuma: 21. október 2022.].
137. Touma, R., 2022. *The Guardian*. [Online]
Available at:
<https://www.theguardian.com/technology/2022/jul/19/tiktok-has-been-accused-of-aggressive-data-harvesting-is-your-information-at-risk>
[Hozzáférés dátuma: 17. október 2022.].
138. Világgazdaság, 2021.. *Vg.hu*. [Online]
Available at:
<https://www.vg.hu/cegvilag/2021/08/hatalmas-adatlopas-miatt-vizsgalodik-a-t-mobile>
[Hozzáférés dátuma: 5- október 2021.].
139. Waitman, R., 2020.. *Cisco*. [Online]
Available at:
<https://blogs.cisco.com/security/maintaining-data-privacy-in-the-age-of-covid>
[Hozzáférés dátuma: 15. október 2021.].
140. Woollacott, E., 2022.. *Forbes*. [Online]
Available at:
<https://www.forbes.com/sites/emmawoollacott/2022/09/27/tiktok-warned-of-possible-29m-fine-for-processing-childrens-data/?sh=494164e7daac>
[Hozzáférés dátuma: 17. október 2022.].
141. YouGov, 2019.. *YouGov*. [Online]
Available at:
<https://today.yougov.com/opi/surveys/results#/survey/01894b4a-6c27-11e9-8012-358611e41108/question/73ad43ea-6c27-11e9-9bf2-ef0cdf3620c6/age>
[Hozzáférés dátuma: 8. október 2021.].

9. MELLÉKLET

9.1 ADATVÉDELEM AZ EURÓPAI UNIÓ KÍVÜL

Eddig az Európai Unió adatvédelmi szabályait ismertettem, viszont érdemes tudnunk azt is, hogy a többi, Unión kívüli országban mennyire veszik szigorúan a személyes adatok védelmét. A GDPR nemcsak az EU tagállamaira van hatással, hanem a Föld többi országára is. Azokra a nem Uniós országokra is vonatkoznak a szabályok, akik termékeket vagy szolgáltatásokat értékesítenek az Európai Unióba. Továbbá széles körben befolyásolja, hogy más országok hogyan viszonyulnak az adatvédelemhez. A következőkben az Egyesült Államok, Kanada és Kína adatvédelmét nézzük meg, emellett említést teszek néhány dél-amerikai és dél-afrikai ország adatvédelméről is.

Egyesült Államok

Az amerikai Morning Consult 2019-es felmérése eredménye alapján, amelyben 2000 amerikai fogyasztó véleményét kérdezték. A résztvevők 69%-a úgy gondolta, hogy a kormány nem tesz eleget a magánélet védelme érdekében. 86%-uk szerint az USA-nak kellene lennie a vezetőnek a fogyasztói adatvédelem terén. A résztvevők több mint 2/3-a egyetértett azzal, hogy az adatvédelmi szabályoknak egységesnek kell lenniük egész Amerika területén. A válaszadók 82%-a egyetértett azzal, hogy szükségük van egy olyan nemzeti adatvédelmi törvényre, amely a fogyasztók számára érthető és amely szerint következménye van annak, ha a cégek nem védik a személyes adatokat megfelelően. (Morning Consult, 2019.) Az amerikaiak 78%-a azt állította, hogy nagyon keveset vagy semmit sem ért abból, amit a kormány csinál az adataival. (Pew Research Center, 2019.)

Az Egyesült Államokban nincs egységes adatvédelmi törvény, viszont számos ágazatspecifikus adatvédelmi törvény létezik. Ilyen pl.: a GLBA (Gramm-Leach-Bliley Act), amely előírja a pénzintézeteknek, hogy tudatni kell az ügyfelekkel, hogy hogyan védik a személyes adataikat. Másik példa az 1996-os HIPAA (Health Insurance Portability and Accountability Act) amely az egészségügyi információkat védi. A Children's Online Privacy Protection Rule megtiltja a cégeknek, hogy a 13 év alatti gyerekek adatai gyűjtsék. Az Egyesült Államokban a személyes adat helyett a személyazonosításra alkalmas adat kifejezést használják, amely jelentése hasonló a személyes adat jelentéséhez, viszont nincs rá egységes definíció, törvényenként eltérhet. (Data Privacy Manager, 2021.)

A CCPA (California Consumer Privacy Act) kaliforniai adatvédelmi törvény a kaliforniai lakosokra érvényes. A vállalkozásoknak értesíteniük kell előzetesen a fogyasztókat arról, hogy milyen adatokat gyűjtenek és mire fogják felhasználni. Az adatvédelmi szabályzatoknak tartalmazniuk kell a begyűjtött személyes adatok kategóriáit, a nyilvánosságra hozott személyes adatok kategóriáit, illetve a vállalkozás által eladott személyes adatok kategóriáit (az elmúlt 12 hónapra vonatkozóan). Továbbá tartalmaznia kell a gyűjtés, a használat és az eladás célját, a források kategóriáit, amelyekből gyűjtik a személyes adatokat, a fogyasztók jogait és a jogok gyakorlásának módját. A törvény szerint a vállalkozás weboldalán lennie kell egy linknek, ahol az érintetteknek lehetősége van elutasítani, hogy az adataikat értékesítsék. (CCPA, 2018.) A rendelet szerint a különleges adatok közé tartozik a helymeghatározás, az emailek tartalma, személyi igazolvány száma, bankkártya adatok és a jelszavak is. (DLA Piper, 2022.d)

Minden idők legnagyobb incidense az amerikai Yahoo-hoz (az első email-szolgáltató vállalat egyike) köthető. 2017-ben derült fény, hogy a 2013-as adatlopás során 3 milliárd felhasználó fiókját törték fel. Az ellopott információk között nem voltak jelszavak vagy kártyaadatok. A szakértők szerint az információkat könnyen felhasználható titkosítással védték, amely már elavult is volt. A Yahoót éppen ekkoriban vásárolta fel a Verizon, amely az incidens után 350 millió dollárral csökkentette az ajánlatát. (Finkle, 2017.)

Kanada

Kanadában a PIPEDA (The Personal Information Protection and Electronic Documents Act), vagyis a személyes adatok védelméről és az elektronikus dokumentumokról szóló törvény hasonló a GDPR-hez abban a tekintetben, hogy mindkét törvény az átláthatóságra és az elszámoltathatóságra összpontosít. Míg a GDPR minden szervezetre vonatkozik, a PIPEDA főként a magánszektorbeli, kereskedelmi tevékenységet folytató iparágakat irányítja. Egy vállalat megfelelhet a GDPR-nek, de ez nem azt jelenti, hogy megfelel a PIPEDA-nak is. Kanada adatvédelmi törvénye jóval tágabban értelmezi a „kereskedelmi tevékenységeket”. Magába foglalja például azokat a nonprofit szervezeteket is, amelyek cserekereskedelemmel vagy bérlettel foglalkoznak. 2023-tól új, szigorúbb törvény kerül bevezetésre, amely szerint a szervezetek maximum 25 millió kanadai dolláros vagy az éves árbevételeük 4 %-áig terjedő büntetést kaphatnak. Hatalmas összeg. (DLA Piper, 2022. b)

Kína

Az Energy Research Institute 2018-as felmérése szerint akkoriban aggasztó volt a helyzet Kínában. Fény derült arra, hogy az alkalmazások többsége rengeteg adatot begyűjt a fogyasztókról. A vizsgált alkalmazások 90%-a begyűjti a tartózkodási helyet és a böngészési előzményeket. 50%-uk nem felelt meg az adatvédelmi szempontoknak, és 34%-a egyáltalán nem is rendelkezett adatvédelmi irányelvekkel. (Blazyte, 2018.)

2021. augusztus 20-án elfogadásra került Kínában az új adatvédelmi törvény (Personal Information Protection Law). Ez az első átfogó adatvédelmi szabályozás az országban az adatbiztonsági törvénnyel és a 2017. június óta hatályos kiberbiztonsági törvénnyel együtt. A jogszabály több ponton is hasonlít a GDPR-re, habár rövidebb és kevésbé részletesebb attól. A személyes adat fogalma a PIPL 4. cikke szerint: *„Bármely elektronikus vagy más módon rögzített információ, amely egy azonosított vagy azonosítható természetes személyre vonatkozik.”* A személyes adatok, az adatkezelés, az adatfeldolgozás meghatározásában nincs számottevő különbség a kínai törvény és a GDPR között, ám a kínai törvényben a különleges adatok köre szélesebb. Többek között alábbi adatok tartoznak a különleges adatok közé: *egyéni helymeghatározási adatok, pénzügyi számlákra vonatkozó adatok, stb.* A „stb.” szó a törvényben is szerepel, így nyitott végű a felsorolás és az egyéni sérelmek is idetartoznak. (Kaszián, 2021.) A legnagyobb különbség a két törvény között, hogy az új kínai törvény nem rendelkezik a kormány személyes adatokhoz való hozzáféréséről, így a kormány korlátlanul fér hozzá az állampolgárok adataihoz. (Portfolio, 2021. b)

Egyéb országok

Néhány országban nincs külön adatvédelmi törvény. Ilyen pl.: Venezuela, Irán, Namíbia, Chile, Kambodzsa, Jordánia. Ezekben az országokban más törvényeken belül térnek ki az információvédelemre. Pl.: a Venezuelai Bolívari Köztársaság olyan általános elveket állapít meg, amelyek az információvédelem keretként szolgálnak. Hasonlóképpen a GDPR-hez, a cégeknek egyértelmű és visszavonható hozzájárulást kell kérniük a személyes adatok felhasználáshoz és ugyanúgy csak előre meghatározott célra lehet felhasználni azokat. Addig lehet megőrizni, amíg a gyűjtés célját el nem éri. Az adatoknak pontosaknak kell lenni, az érintett kérheti az adatok helyesbítését. Itt az adatvédelmi incidensek bejelentése nem kötelező. Vannak olyan országok, ahol nemcsak pénzbüntetés járhat az adatvédelmi törvények megszegéséért, hanem több évig terjedő börtönbüntetés is. Ilyen például Törökország, Botswana, Madagaszkár, Argentína, vagy Dél-Afrika, ahol akár 10 év börtönbüntetést is kaphatnak. (DLA Piper, 2021.)

9.2 ORSZÁGOK JELÖLÉSE

Ország ▼	Jelölés ▼
Ausztria	AT
Belgium	BE
Bulgária	BG
Ciprus	CY
Csehország	CZ
Dánia	DK
Észtország	EE
Európai Unió tagállamai	EU27
Finnország	FI
Franciaország	FR
Görögország	GR/EL
Hollandia	NL
Horvátország	HR
Írország	IE
Lengyelország	PL
Lettország	LT
Litvánia	LV
Luxemburg	LU
Magyarország	HU
Málta	MT
Németország	DE
Olaszország	IT
Portugália	PT
Románia	RO
Spanyolország	ES
Svédország	SE
Szlovákia	SK
Szlovénia	SI

Forrás: saját szerkesztés

9.3 EGYÉB ADATVÉDELMI INCIDENSEK

Többször hallhattuk már a hírekben, hogy kirobbant egy-egy botrány a személyes adatok illetéktelen felhasználása miatt és egyiken sem szeretnénk az adathalászat áldozatai lenni. Sajnos az adatok lopása több ismert vállalatot is érintett már.

A brit információs kormánybiztosi hivatal 2018-ban 500 ezer font pénzbírságot szabott ki a Facebookra, miután napvilágra került, hogy egy londoni székhelyű brit-amerikai politikai elemző cég közel 90 millió felhasználó adatait szerezte meg annak érdekében, hogy a választópolgárok politikai beállítottságáról tudomást szerezzenek. Az adatok segítségével személyreszabott üzenetekkel próbálták befolyásolni a felhasználókat a tudtuk nélkül, a BREXIT-tel kapcsolatban. A Facebook elfogadta a büntetést. (MTI, 2019.)

A világ legnagyobb hamburgerláncja, a McDonald's is ütközött már problémába az adatvédelem tekintetében. Nemrégiben a portfolio.hu-n olvashattuk, hogy kibertámadók fértek hozzá dél-koreai és tajvani ügyfelek adataihoz. A McDonald's szerint, csak e-mail címekhez, szállítási címekhez és telefonszámokhoz fértek hozzá, fizetési adatokhoz nem. Mivel jelentős összeget fektetnek a kiberbiztonságba, így a probléma gyorsan azonosításra került. (Portfolio, 2021.)

Pár hónappal ezelőtt az Világgazdaság weboldalán olvashattuk, hogy a T-mobile átfogó vizsgálatot folytat, mert hackerek állították, hogy birtokukban van egy olyan adatbázis, ahol a T-mobile több mint 100 millió ügyfelének adatai szerepelnek (személyes adatok, társadalombiztosítási számok, címek, telefonszámok, stb.), amelyeket értékesíteni fognak. Az eladók kb. 270 000 dollárt, azaz több mint 800 millió forintot kérnek kb. 30 millió fiókért cserébe. A vizsgálat még folyamatban van. (Világgazdaság, 2021.) A Magyar Telekom szerint a magyar ügyfeleket nem érinti az adatlopás. (Origo, 2021.)

Továbbá a Volkswagen egyik adatvédelmi incidensét is felhoznám példának. Az egyik beszállítónál történt incidens során több mint 3,3 millió ügyfél személyes adatait szerezte meg egy illetéktelen harmadik fél egy olyan beszállítótól, amelyet az Audi és a Volkswagen márka kereskedő digitális értékesítéshez és marketinghez használt. Az információkat 2014 és 2019 között gyűjtötték egy elektronikus fájlba, amely nem volt biztonságban. Az ügyfelek többségének csak az e-mail címei és a telefonszámok kerültek harmadik félhez. A Volkswagen szerint 90 ezer Audi vásárló és leendő vásárló érzékeny adatait érintette az incidens, nekik a cég ingyenes hitelvédelmi szolgáltatásokat nyújt. Az érzékeny adatok 95 % jogosítványszám, kisebb része születési dátum, társadalombiztosítási szám vagy számlaszám. (Portfolio, 2021. a) Hollandiában egy nagymamát büntetett meg az adatvédelmi hatóság, mert az unokái anyja többszöri kérése ellenére sem törölte a nagymama az általa feltöltött fotókat a közösségi

oldaláról. A büntetés napi 50 EUR, legfeljebb összesen 1 000 EUR. Érdekes helyzet... Ezt sokan kihasználhatják a jövőre nézve, ha tudják, hogy emiatt is bejelentést tesznek, ami következményekkel is jár. (BBC, 2020.)

Az izlandi Adatvédelmi Hatóság egy középiskolára szabott ki 9 000 EUR bírságot, mert az egyik tanár köremailt küldött a diákoknak és szüleiknek, ám rossz fájlt csatolt. A mellékelt dokumentum a diákok egészségére, családi körülményeire, tanulmányi eredményeire vonatkozó személyes adatokat tartalmazott. (EDPB, 2020. b)

A különleges adatok kezelésének megszegésére hoztam még egy példát: 2020-ban a holland adatvédelmi hatóság az addigi legmagasabb bírságot szabta ki, azaz 790 ezer dollárt. A vállalat a munkavállalók munkába érkezését az ujjlenyomatok szkennelésével rögzítette, így megszegte a biometrikus adatok felhasználása iránti tilalmat. Az esetről a munkavállalók értesítették a hatóságot. A vizsgálat során kiderült, hogy semmilyen olyan feljegyzés nincs, amiben a munkavállalók beleegyeztek volna az érzékeny adataik felhasználására. Azonban itt felmerül, hogy amennyiben a cég kéri a munkavállaló beleegyezését, az szabad akaratból egyezik-e bele, hiszen a hierarchia miatt félhet attól, hogy, ha nem fogadja el ezt a fajta azonosítást, hátrány érheti a munkában. A cég továbbá a leszámolt dolgozók ujjlenyomatait is megtartotta. A holland törvény lehetővé teszi a biometrikus adatok biztonsági okokból történő felhasználását, de megállapították, hogy ebben az esetben más módszereket is alkalmazhattak volna az azonosításra. A cég a történetek után leállította az ujjlenyomatok szkennelését. (Data Privacy Manager, 2020.)

9.4 A COVID-19 HATÁSA A SZEMÉLYES ADATOKRA

A 2019-ben kezdődő COVID-19 névre keresztelt világjárvány életünk minden területére hatással van, így fontosnak tartom, hogy megemlítsük az adatvédelem tekintetében is. Kevesen vannak, akiknek nem volt szükségük valamilyen (PCR, antigén, antitest, stb.) teszt elvégzésére a COVID-19 vírussal kapcsolatban. A járvány miatt adatokat kellett szolgáltatnunk a kormánynak az egészségügyi állapotunkról, a teszt eredményeinkről. Amennyiben külföldre akartunk utazni, sok ország kért valamilyen regisztrációt tőlünk, amelyben meg kellett adnunk a személyes információinkat: születési adatainkat, lakcímünket, a külföldön való tartózkodási címünket és az oltottságról/ tesztről szóló információkat vagy dokumentumokat. Tudatni kellett, hogy hol jártunk, kikkel voltunk kontaktban az elmúlt napokban a járvány megfékezése érdekében. Ám ezeket az adatokat nemcsak külföldre utazás során kellett megadnunk, hanem akkor is, ha a PCR vagy antigén teszt eredményünk pozitív lett. Azonban az információk fontosak számunkra és sokan nem szívesen osztják meg az adataik védelme érdekében.

A 2020-as Cisco Consumer Privacy Survey nevű felmérésben kitért a járvánnyal kapcsolatos adatvédelemre. 2600 résztvevő válaszolt a feltett kérdésekre. A válaszadók 12 országból valók. A kutatás eredménye azt mutatja, hogy a résztvevők nagyobb része, pontosabban 57%-a támogatja azt, hogy a munkaadó ellenőrizze a munkavállalók egészségügyi állapotával kapcsolatos információkat a biztonságos munkahely érdekében. Azonban csak 37% az, aki támogatja azon információk megosztását, amely a fertőzött szomszédokkal vagy munkatársakkal kapcsolatos. (Cisco, 2021.)

A vírushelyzet következtében számos munkavállalónak otthoni munkavégzést illetve a tanulóknak online oktatást kell folytatni, ami szintén növelte a személyes adatok megadásának szükségességét. A kutatásban résztvevők közel 2/3 része aggódik az azokkal az eszközökkel kapcsolatos adatvédelem miatt, amelyeket a home office-hoz illetve az online oktatáshoz kell használniuk. (Waitman, 2020.)