SZAKDOLGOZAT

OE-NIK
2022.

Nagy Máté
T-007283/FI12904-N

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

NEUMANN JÁNOS INFORMATIKAI KAR
INFORMATIKAI KAR

SZAKDOLGOZAT

OE-NIK
2022.

Hallgató neve: **Nagy Máté**
Hallgató törzskönyvi száma: **T-007283/FI12904-N**

Óbudai Egyetem
Neumann János Informatikai Kar
Kiberfizikai Rendszerek Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: **Nagy Máté**

Törzskönyvi száma: T/007283/FI12904/N

Neptun kód: [redacted]

A dolgozat címe:

A GDPR és a user-profiling következményei
Consequences of the user-profiling and the GDPR

Intézményi konzulens: Balázsné Dr. Kail Eszter

Külső konzulens:

Beadási határidő: 2022. december 15.

A záróvizsga tárgyai: Informatikai rendszerek üzemeltetésének biztonsága
IT hálózatbiztonság

A feladat:

Korunk felgyorsult világában számos vállalat, szervezet felismerte a felhasználói kategorizálásában (user-profiling) rejlő lehetőségeket, hogy a tevékenysége ellátásához szükséges-, illetve esetenként azokon felül gyűjtött-adatokból mennyire tudja célcsoportokba sorolni a vele kapcsolatba kerülő ügyfeleket. Ez a besorolás a jellemzők alapján azután célzott stratégiák kidolgozásán keresztül jobb ügyfél-elérést, magasabb árbevételt jelent a cégeknek.

A számítástechnika fejlődésével egyre több tevékenység, és ezzel kapcsolatban egyre több adat kerül fel az internetre, illetve azon keresztül különböző adatbázisokba. A GDPR hatályba lépésével számos, korábban szabadon gyűjtött adat, információ már csak korlátozottan gyűjthető/kezelhető/tárolható.

A szakdolgozat célja annak bemutatása, hogy a user-profiling terjedésével megnyílt lehetőségek hol és hogyan kerültek kapcsolatba az adatvédelemmel, és mely területek azok, amelyek további szabályozások kidolgozását igénylik.

A dolgozatnak tartalmaznia kell:

1. Az infotörvényt, mint a GDPR-t megelőző szabályozás bemutatását,
2. A GDPR-t és hatását a hazai és európai adatkezelési eljárásokra,
3. A felhasználói profilalkotás (user-profiling) ismertetését, jelenlegi alkalmazását, lehetséges jövőbeni irányokat, módszereket,
4. A GDPR, mint szabályozás és a user-profiling mint tevékenység alkalmazásából adódó összefüggések komplex vizsgálatát,
5. A vizsgálat kiértékelését, következtetések levonását.

ÓBUDAI EGYETEM * Neumann János Informatikai Kar * Budapest 1. Ph

.....
Dr. habil. Lovas Róbert
intézetigazgató

A szakdolgozat elévülésének határideje: **2024. május 15.**
(OE TVSz 55.§ szerint)

A dolgozatot beadásra alkalmasnak tartom:

.....
külső konzulens

.....
intézményi konzulens

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

HALLGATÓI NYILATKOZAT

Alulírott Nagy Máté (neptun kód: [redacted]) hallgató kijelentem, hogy a jelen szakdolgozat saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatomban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja.

Budapest, 2022. december 15.

.....

hallgató aláírása

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

KONZULTÁCIÓS NAPLÓ

Hallgató neve: Neptun Kód: Tagozat:

Nagy Máté [redacted]

Telefon: Levelezési cím (pl.: lakcím):

[redacted]

Projektmunka címe magyarul:

A GDPR és a user-profiling komplex vizsgálata

Projektmunka címe angolul:

Complex examination of the GDPR and user-profiling

Intézményi konzulens: Külső konzulens:

Balázsné Dr. Kail Eszter ----------

Kérjük, hogy az adatokat nyomtatott nagy betűkkel írja!

Alk.	Dátum	Tartalom	Aláírás
1.	2022.04.11.	Profilalkotás eszközeinek rendszerezése	Kail
2.	2022.04.28.	GDPR elvek érvényesítési alvállalkozói szerződés során (folytatás)	Kail
3.	2022.05.02.	Internetes böngészés nyomkövetési jellemzőinek GDPR szempntú vizsgálata	Kail
4.	2022.05.09.	Véglegesítés, formázás	Kail

A Konzultációs naplót összesen 4 alkalommal, az egyes konzultációk alkalmával kell láttamoztatni bármelyik konzulenssel.

A hallgató a Projektlabor 1. / 2. / 3. / Záródolgozati projekt[1] tantárgy követelményét teljesítette, beszámolóra/védésre[2] bocsátható. A javasolt érdemjegy:

Intézményi konzulens

Kail

[1] A megfelelő bekarikázandó/aláhúzandó!

[2] A megfelelő aláhúzandó!

Tartalomjegyzék

BEVEZETÉS

Manapság már számos szervezet rájött már arra, hogy mekkora előnyöket rejt magában felhasználói adatainak gyűjtése, kategorizálása és hogy ezt a tevékenységet hogyan tudja felhasználni a nagyobb haszon elérése céljából.
Az informatika térnyerésével egyre több információ kerül fel az online térbe, ahol különféle adatbázisok szűrésével számos következtetés levonható. A GDPR ennek a szabadon felhasználásnak ment elébe és tette azokat korlátozottan hozzáférhetővé.
A felhasználói profilalkotás már az internet elterjedése előtt is ismert fogalom volt. Rendfenntartó szervek, nyomozók már a digitalizáció megjelenése előtt alkalmaztak olyan technikákat, amelyek segítségével különböző jellemzők gyűjtése alapján a bűnözőket, megfigyelt személyeket be tudták különböző kategóriákba sorolni. A besorolás eredményeképpen pedig célzott stratégiákat lehetett bevetni a kézre kerítésükhöz.
A digitalizáció és az online adatok megjelenésével a technikák nem, mindössze a fellelhető eszközök száma és fajtája sokasodott meg, valamint határozottan nehezebbé vált annak megállapítása, hogy kiről milyen adatok kerülnek begyűjtésre mely pillanatban. Így gyakorlatilag bárki, bármikor a jogosulatlan adatgyűjtés áldozata lehet.
A szakdolgozat azt hivatott feltárni, hogy a user-profiling megjelenésével a digitális térben milyen új lehetőségek nyíltak, amelyek esetlegesen az időközben létrehozott szabályozás kiegészítését igénylik
A dolgozatban bemutatásra kerül néhány gyakorlati példán keresztül, hogy milyen interakciók adnak lehetőséget az adatgyűjtésre.
Ezúton szeretném köszönetem kifejezni Balázsné Dr. Kail Eszternek a szakmai útmutatásért és az érdekes témáért.

1 AZ ADATVÉDELMI SZABÁLYOZÁSI KÖRNYEZET KIALAKULÁSA

Az adatvédelmi szabályozás kialakulása során felmérésre kerültek azon kockázatok, melyek veszélyt jelentenek a XXI. században jelen lévő eszközök és digitális adatok kontroll nélküli felhasználása illetve feldolgozása miatt. A szabályozások és törvények megalkotása létrehozta az elfogadható és biztonságos kereteket.
A XX. század második szakaszában kezdett kialakulni az adtavédelmi szabályozás, mivel a személyes jellegű információk gyűjtésére a számítástechnika ekkor vált alkalmassá. A nagy mennyiségű személyes adat miatt szabályozni kellett a személyes adatok fokozott védelmét. [15]
Az adatvédelemmel kapcsolatos szabályozás a fejlődés rövid időszakában jól elkülöníthetőek generációkra. Nincs egységes vélemény a generációk számát illetően, azonban három generáció különböztethető meg az adatvédelmi jogban.
Az 1970-es évekhez köthető az első generáció, amikor a széles körben alkalmazott számítógépes nyilvántartások miatt kellett adatbiztonsági előírásokat hozni.
Az 1980-1990-es évekhez köthető a második generáció, amikor a jogi szabályozás már a papír alapú nyilvántartásokra is vonatkozott, és kitért a nemzetközi adatáramlás szabályozására is.
Az azt követő harmadik generáció már az európai integráció jellemzőit és az egyes iparágakra, szektorokra jellemző szabályokat is tartalmazta.
Az adatvédelmi generációk a technológiai és társadalmi változásokat lekövetve fejlődött ki az európai adatvédelmi szabályozás is. Ahogy levezetésre került az adatvédelmi szabályozás története jól látható, hogy már a XX. század közepétől megjelent a nemzetközi jogrendszerben. [15]
A személyes adatok védelméhez köthető első jogszabályok a gyors technológiai fejlődéshez köthetőek. A technológia és a számítástechnika fejlődése révén a nagy mennyiségű, különböző, jórészt állami jellegű nyilvántartások ekkor tájt kezdték az adattömegeket elektronikusan rögzíteni és tárolni. Ezzel egyidőben a társadalom képviselői és a jogalkotók a digitalizált adatok és az elektronikus adatfeldolgozás magánszférára történő hatásaival is foglalkozni kezdtek. Így született meg az 1970-es években az első, nemzeti szintű adatvédelmi törvény. [15]
1981-ben került kiadásra az első európai szintű, kizárólag az adatvédelemre fókuszáló, jogilag kötelező erejű nemzetközi jogirat. A 108. számú egyezményt az Európa Tanács ekkor fogadta el. Az egyezmény a számítógépes, automatizált nyilvántartások védelmére fókuszált. Az egyezmény jelentősége abban rejlett, hogy ebben került rögzítésre a személyes adatok védelméhez való jog önállóan, mint a magánélethez való jog egyik formájaként. [15]
Közel másfél évtizedig a 108. számú egyezmény, mint adatvédelmi szabályozás volt az egyetlen kötelező érvényű nemzetközi szintű jogforrás. Az informatikai fejlődés, a személyi számítógépek egyre szélesebb körben történő elterjedése, a határon átnyúló adat-

áramlás folyamatos növekedése, valamint az adatok szabad áramlását nehezítő, egymástól eltérő nemzeti szabályozások vezettek oda, hogy 1995-ben a 95/46/EK számú adatvédelmi irányelvet az Európai Parlament és a Tanács kiadta. [15]
Az adatvédelmi irányelv érdekessége, hogy a nemzetközi jogi gyakorlatban eddig nem megszokott módon, kiterjesztő hatályú rendelet, azaz nem EGT-tagállamban működő szervezetekre is kötelező lehet.
A 95/46/EK számú adatvédelmi irányelv igazi áttörést jelentett az Európai Unióban a személyes adatok védelmére. Az irányelv kidolgozása során kettős cél volt, egyrészről harmonizálja az adatkezelési tevékenységek tekintetében a természetes személyek alapvető jogainak és szabadságainak védelmét, másrészről biztosítsa a tagállamok közötti személyes adatok szabad áramlását. Ezen kettős célt az irányelv a személyes adatok magas szintű védelme mellett kívánta elérni az adatok szabad áramlását az Európai Unión kívüli, harmadik országokban is. Az irányelv az adatvédelmi szabályozás területén nagy előrelépést jelentett, kiemelve néhány szempontot, ugyanis kiterjedt a kézi és automatizált adatfeldolgozásra, meghatározta az adatfeldolgozásra vonatkozó szabályokat, az érzékeny adatok kezelésére vonatkozó szabályokat, az érintettek jogait, a határon átnyúló adattovábbítás szabályait, valamint szigorított az adatkezelés és –feldolgozásra vonatkozóan. [15]
Az irányelvet 1998-ig kellett minden Európai Uniós tagállamnak a saját jogrendjébe ültetni, ezzel létrejött az Union belüli egységes szabályozás.
2016-ban felváltotta 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 szóló 2016/679 rendelet, másnéven az általános adatvédelmi rendelet. A rendeletről részleteiben a 1.3. fejezetben lesz szó.

1.1 A személyes adatok védelmének története Magyarországon

Az adatvédelemmel kapcsolatos szabályozás hazánkban a XX. század második felén indult azzal, hogy módosult 1977-ben a Polgári Törvénykönyv, miszerint „A *számítógéppel történő adatfeldolgozás nem sértheti a személyhez fűződő jogokat*". A törvény megszabta, hogy a nyilvántartott adatokról az érintett személyen kívül csak az arra jogosult szervnek vagy személynek lehet információt adni. Továbbá az érintett személynek helyesbítési jogot adott, ha a nyilvántartásban szereplő adatok nem feleltek meg a valóságnak, úgy kérheti az adat kijavítását vagy korrigálását. [15]
Az Alkotmány módosításáról szóló 1989. évi XXXI. törvénnyel kapott alkotmányos védelmet a személyes adat: [15]
„*59. § A Magyar Köztársaságban mindenkit megillet a jó hírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog*."
A személyes adatok védelmének megjelenése az Alkotmányban nagy előrelépést jelentett, azonban annak alkalmazására vonatkozóan nem adott iránymutatást. Emiatt az értelmezésére vonatkozóan az Alkotmánybíróság állásfoglalása kellett több alkalommal is. A

15/1991. (IV.13.) AB határozatával törölte a népesség-nyilvántartásra és a személyes adatok kezelésére vonatkozó szabályozások bizonyos részét, a személyes adatok védelme miatt. Az Alkotmánybíróság ezzel létrehozta a mai adatvédelmi szabályozási rendszer alapjait. [15]
A nagy tömegű információkezelésre, az adatok feldolgozására és nyilvántartására nem állt rendelkezésre átfogó szabályozás, ami jogbizonytalanságot jelentett. Az Országgyűlés megalkotta az alkotmányos kötelezettségeként a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvényt, másnéven adatvédelmi törvényt (Avtv.) A törvény hatálya a magában foglalta a számítógéppel, illetve kézzel történő adatkezelést is. A törvény szabályozta a közérdekű adatok nyilvánosságra hozatalát és az adatvédelmi biztos létrehozását. [17]

Az információs önrendelkezési jogról és a közérdekű adatok nyilvánosságáról szóló 2011. évi CXII. törvény („Infotörvény") váltotta az Adatvédelmi törvényt. Az Infotörvény megtartotta az adatvédelmi törvény rendszerét, némi kiegészítéssel élve. Az Infotörvényhez fűződik a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) megalakulása. Az adatvédelmi biztosi intézményt a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) váltotta fel és további jogkörökkel is felruházta. A hazai személyes adatokkal kapcsolatos védelmet jelenleg is az Infotörvény szabályozza, kiegészülve a GDPR jogharmonizációs kötelezettséggel. [15] [4]

1.2 Infotörvény

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, másnéven „Infotörvény", meghatározza azt, hogy természetes személyek magánszférája tiszteletbe legyen tartva, a keletkező adatok illetve információk kiknek rendelkeznek vagy kinek van rendelkezési joga. Továbbá meghatározza a közügyek átláthatóságát és a közérdekből nyilvános adatokhoz való hozzáférés és a terjesztés módját.
Az Infotörvényben szereplő néhány kiemelendő értelmezendő definíció, ami a Szakdolgozat szempontjából releváns [9]:

- „*érintett: bármely információ alapján azonosított vagy azonosítható természetes személy,*
- *személyes adat: az érintettre vonatkozó bármely információ,*
- *különleges adat: 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,*
- *közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben*

keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat,

- *közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli,*
- *hozzájárulás: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez,*
- *adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajttatja,*
- *adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése,*
- *adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele,*
- *nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele,*
- *adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges,*
- *adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége,*
- *adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel - az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel,*
- *adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett,*

- *adatvédelmi incidens: az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi,"*

A törvény hatálya alá tartozik minden személyes adattal, közérdekű adattal, illetve közérdekből nyilvános adattal kapcsolatos adatkezelés. [9]

A törvény 4 § tartalmazza a személyes adat kezelésének alapelveit: [9]

- a személyes adatot csak a meghatározott, jogszerű célból, a jog gyakorlása és a jogi kötelezettség érdekében lehetséges. Tisztességesnek és törvényesnek kell lennie az adatkezelés céljának, az adatok gyűjtésének és kezelésének az adatkezelésnek.
- Olyan személyes adatot lehet kezelni, ami az adatkezelés céljának megvalósulásához elengedhetetlen, illetve alkalmas a cél elérésére. A személyes adat a cél megvalósulásához szükséges mértékig és ideig kezelhető.
- A személyes adat az adatkezelés során addig marad személyes adat, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor hozható létre a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a kapcsolat helyreállításához szükségesek.
- Az adatkezeléskor az adatok pontosságát, teljességét, naprakészségét garantálni kell. Az adatot biztosítani kell, hogy az adatkezelés céljához szükséges ideig lehessen azonosítani.
- Garantálni kell az adatkezelés során a személyes adatok megfelelő biztonságát, műszaki vagy szervezési intézkedésekkel az adatkezelés alkalmával.
- A személyes adatok kezelése akkor tisztességes és törvényes, amennyiben az érintett véleménynyilvánítási szabadságának biztosítása érdekében, az érintett véleményét megismerni kívánó személy, az érintett lakóhelyén vagy tartózkodási helyén felkeresheti.

A profilalkotás során tulajdonképpen a személyes adatok és azoknak a kezelésével foglalkozunk. A dolgozatban nem kezeljük külön a személyes adatot, illetve a különleges adatot.

Az Infotörvény szerint, a személyes adatot a következőkben lehet kezelni: [9]

- ha a törvény vagy ha a helyi önkormányzat rendelete közérdek miatt úgy rendelkezik, amennyiben a törvény felhatalmazása, abban meghatározott körben, különleges vagy bűnügyi személyes adatnak nem minősülő adat,
- ha az adatkezelő törvényben meghatározott feladatainak elvégzéséhez feltétlen szükséges és az érintett a személyes adatok kezeléséhez kimondottan beleegyezik,
- ha az érintett vagy más személy nélkülözhetetlen érdekeinek védelméhez, továbbá a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez elengedhetetlen és azzal arányos,
- vagy ha az érintett a személyes adatot kimondottan nyilvánosságra hozta és elengedhetetlen az az adatkezelés céljának megvalósulásához és azzal arányos.

Az adatkezelőn kívül azzal azonos külön működő adatfeldolgozó (közös adatfeldolgozó) a begyűjtött adatokat kezelheti. Az Infotörvényben az adatkezelő és az adatfeldolgozó definiálása kevésbé precíz, a GDPR-ban meghatározotthoz képest. Ugyanakkor meghatározta azt az irányvonalat, hogy a feldolgozandó adatokat kiemelve a személyes vagy érzékeny adatokat adekvát okkal, adott intézkedés és adott módon lehessen kezelni.
Az Infotörvény meghatározza azokat a feltételeket, amik az adatok továbbítására vonatkozik a jogosultak között: [9]

- A továbbítandó személyes adatok pontosságát, hiánytalan és naprakészségét az adattovábbítás előtt az adatkezelő, illetőleg a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó megvizsgálja.
- Ha a vizsgálat eredményeképpen a továbbítandó adatok pontatlanok, hiányosak vagy már nem naprakészek, ekkor abban az esetben továbbíthatók, amennyiben
    - szükségszerű az adattovábbítás céljának megvalósulásához,
    - értesíti a címzettet az adattovábbítással azonos időben, az adatok pontosságával, teljességével és naprakészségével kapcsolatos információkról.

Abban az esetben, ha az adatkezelő vagy az adatfeldolgozó személyes adatot ebben a formában kap kézhez, úgy az adattovábbítással egyidőben tájékoztatni kell az alábbiakról:

- felhasználás előreláthető időintervallumáról,
- továbbításának lehetséges átvevőiről,
- érintett-e törvényben biztosított jogainak korlátozásáról, vagy
- egyéb feltételeiről kezelésének.

Az adatátvevő, az adatkezelő és az adatfeldolgozó, az adatkezelési feltételeknek megfelelő terjedelemben és módon kezeli a személyes adatot és az adatkezelési feltételeknek megfelelően biztosítja az érintett jogait. [9]
Az érintetteket megillető jogosultságok, a következők: [9]

- előzetes tájékozódáshoz való jog, ennek értelmében az adatkezelés megkezdését megelőzően tájékoztatást kapjon az adatkezeléssel összefüggő tényekről,
- hozzáféréshez való jog, az adatkezelő rendelkezésére bocsássa, kérésére a személyes adatait és az azok kezelésével összefüggő információkat,
- helyesbítéshez való jog, azaz kérelmére, adatkezelő helyesbítse, illetve kiegészítse személyes adatait,
- adatkezelés korlátozásához való jog, azaz kérelmére korlátozza az adatkezelő személyes adatai kezelését,
- törléshez való jog, azaz kérelmére az adatkezelő törölje a személyes adatait.

Az érintett jogainak érvényesüléséhez a következők szükségesek:

- egyszerűen hozzáférhető és olvasható formátumban lévő értesítések,
- gyors kiszolgálása az érintettek kérelmeinek,
- a fentiek díjtalan biztosítása. [9]

Az adatkezelőnek a következőkről is tájékoztatást kell adnia az adatok kezelésekor az érintettel:

- az eredetét a kezelt személyes adatoknak,
- célját és jogalapját az adatkezelésnek,
- a kezelt személyes adatok típusát,
- a kezelt személyes adatok továbbításakor az adattovábbítás címzettjeit, beleértve a harmadik országbeli címzetteket és nemzetközi szervezeteket is,
- a kezelt személyes adatok megőrzésének idejét, és az időtartam meghatározásának módját,
- a megillető jogok, illetve azok érvényesítésének módját,
- annak tényét, hogy profilalkotás alkalmazásra kerül sor,
- az érintett személyes adatainak kezelésével kapcsolatosan felmerült adatvédelmi incidensek bekövetkezésének körülményeit, azok hatásait és az azok kezelésére tett intézkedéseket,
- az adatkezelő az érintett hozzáféréshez való jogát az elérni kívánt céllal arányosan korlátozhatja vagy megtagadhatja, értesíteni szükséges erről az érintettet. [9]

Ha az érintettet az adatkezelő a meghatározott jogaiban korlátozza vagy megalapozott gyanú áll fenn a személyes adatai nem megfelelően kerülnek kezelésére az adatkezelő által, az adatkezelő és megbízottja ellen az adatvédelmi hatóság vizsgálatát kezdeményezheti.

Az adatkezelő vagy a megbízásában eljáró adatkezelő csakis az érintett jogos érdekének érvényesítése vagy törvényben meghatározott indokból végezheti az adatkezelési műveletet.

Az Infotörvény rögzíti a profilalkotás fogalmát, miszerint *„személyes adat bármely olyan - automatizált módon történő - kezelése, amely az érintett személyes jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul*”. [9]

1.3 GDPR

Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete szól a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet).

Az általános adatvédelmi rendelet angol neve General Data Protection Regulation, melyet GDPR-nak hívnak röviden.

A rendelet az Európai Gazdasági Térség (EGT) területén lévő természetes személyek személyes adatait óvja és megszabja a tagállamok közötti szabad információáramlást.

A GDPR 2016. május 24-én lépett hatályba, alkalmazni 2 éves türelmi időszakot követően 2018. május 25-től kell. A GDPR megjelenésével nem tér el a korábban hatályos irányelvtől.

A GDPR kiterjesztő hatályú, ezzel eltér a nemzetközi jogi gyakorlatban megszokottól, azaz a nem EGT-tagállamban működő szervezetekre is kiterjesztett lehet.
Így a GDPR területi hatálya alapján, megkülönböztethető az érintett állampolgársága, az érintett tartózkodási helye, az adatkezelő/adatfeldolgozó tevékenységi helye és hogy a GDPR hatálya alá tartozik-e, melyet az 1. táblázat foglal össze. [15]

Érintett tartózkodási helye	**Érintett állampolgársága**	**Adatkezelő/adatfeldolgozó tevékenységi helye***	**GDPR hatálya alá tartozik?**	
			Igen / Nem	**Ha igen, akkor melyik pont alapján**
EU	EU	EU	**I**	3. cikk / 1. pont
EU	EU	Nem EU	**I**	3. cikk / 2. pont**
Nem EU	EU	EU	**I**	3. cikk / 1. pont
Nem EU	EU	Nem EU	**N**	-
EU	Nem EU	EU	**I**	3. cikk / 1. pont
EU	Nem EU	Nem EU	**I**	3. cikk / 2. pont**
Nem EU	Nem EU	EU	**I**	3. cikk / 1. pont
Nem EU	Nem EU	Nem EU	**N**	-

1. táblázat GDPR területi hatálya [15]

Megjegyzés:
*Az Adatkezelő/adatfeldolgozó EU-n belül tevékenykedik.
**Itt azon feltevéssel lett figyelembe véve, hogy az adatkezelési tevékenység az áruhoz vagy szolgáltatáshoz köthető, illetve az érintett Unión belül tanúsított viselkedésének megfigyelésére irányul.

A fenti 1. táblázatból kiolvasható, hogy a GDPR nézőpontjából éppúgy elhanyagolható az érintett állampolgársága, az adatkezelő/adatfeldolgozó tevékenységi helye, illetve az adatkezelési tevékenység tényleges helyszíne is. Ezzel a rendelet hatálya lefedi azt, ha az EU-ban tevékenységi hellyel rendelkező cég harmadik országbeli állampolgárok személyes adatait kezeli. Ugyanakkor nem vonatkozik a GDPR előírása azon EU-ban tevékenységet nem folytató vállalat adatkezelési tevékenységére, ha Union túl lévő uniós állampolgárról személyes adatokat rögzít az érintett ott tartózkodása során. [15]
A GDPR 2. cikke szerint többek között nem alkalmazandó, ha a természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik a tevékenységüket. Ha az adatokat ezen túlmutatóan használnák, üzleti, kereskedelmi stb. céllal akkor már a GDPR szabályait kell alkalmazni. [10]
A GDPR rendelet alapelveket fogalmaz meg a személyes adatok kezelésére vonatkozóan. [15]
A GDPR 7 alapelve az alábbi: [15]

„Jogszerűség, tisztességes eljárás és átláthatóság elve”: a személyes adatok kezelését jogszabályi előírásoknak megfelelően és tisztességesen, az érintett számára átlátható és mindenre kiterjedő tájékoztatása mellett végzi.

„Célhoz kötöttség elve”: a személyes adatok gyűjtése, kezelése, kizárólag konkrét és jogszerű célból lehet.

„Adattakarékosság elve”: a személyes adatokat csakis az adatkezelés céljainak eléréséhez elengedhetetlen mértékben és ideig kezelhető.

„Pontosság elve”: a személyes adatoknak helyesnek és szükség szerint aktuálisnak kell lenniük, a téves személyes adatokat törölni vagy helyreigazítani szükségszerű.

„Korlátozott tárolhatóság elve”: a személyes adatok tárolása úgy történhet, hogy az érintettek azonosítását mindössze a személyes adatok kezelése céljainak eléréséhez elengedhetetlen ideig.

„Integritás és bizalmas jelleg elve”: a személyes adatok kezelése során alkalmas műszaki vagy szervezési megoldással kell a személyes adatok biztonságáról gondoskodni.

„Elszámoltathatóság”: az adatkezelőnek teljesen meg kell felelnie az alapelveknek, azokat maradéktalanul be kell tartania, amit igazolnia is kell.

A GDPR-ban az érintettek jogai az alábbiként sorolható fel: [9, 15]

- Hozzáféréshez való jog,
- Helyesbítéshez való jog,
- Törléshez való jog,
- Elfeledtetéshez való jog,
- Adatkezelés korlátozásához jog,
- Adathordozhatósághoz való jog,
- Tiltakozáshoz való jog,
- Átlátható tájékoztatáshoz való jog.

2 A GDPR HATÁSA A MAGYARORSZÁGI ÉS EURÓPAI ADATKEZELÉSI ELJÁRÁSOKRA

2.1 Hatályba lépés körüli állapot

Az Európai Unió általános adatvédelmi rendelete (General Data Protection Regulation, röviden: GDPR) 2018. május 25-től kell minden EU tagországnak, így Magyarországnak is alkalmaznia.

A rendelet fő célja, a személyes adatoknak az egységes adatvédelme. Akik személyes adatokat kezelnek vagy azokkal kereskednek, biztonságosan és áttekinthetően végezzék. Átlátható tájékoztatáshoz való jog alapján, magánszemélyek (EU-s állampolgárok) az adatkezelőt információ nyújtásra szólíthatják fel, hogy az érintett magánszeméllyel kapcsolatban kezel-e személyes adatot, milyeneket, miért és meddig. [15]

A GDPR egzakt módon rögzíti, hogy az adatait kikérő magánszemély a hozzáférési jogát hogyan tudja gyakorolni.

A GDPR előírásainak megfelelően, benyújtott kérés esetén az adatkezelőnek az alább felsorolt adatokat kell megadnia: [9, 15]

- milyen céllal kezelik a vonatkozó adatokat (kategorizálva),
- adat átadás vagy közvetítés esetén ki felé végzik,
- külföldre továbbított adat esetén, milyen biztosíték van a megfelelő adatkezelésre vonatkozólag abban a külhoni államban,

- meddig tárolják a vonatkozó adatokat (ugyancsak kategorizálva),
- informálni kell az adattulajdonost a jogairól (lásd korábban az érintettek jogai felsorolás szerint),
- közölni kell a panaszbenyújtás módját,
- meg kell adni azon rendelkezésre álló adatokra vonatkozó forrásokat is, melyek más adatállományból vagy forrásból erednek,
- tájékoztatni kell az adatkérőt, hogy igénybe vesznek-e bármiféle automatizált adatkezelésen alapuló döntéshozatalt, ami profilalkotással jár. (A profilalkotás során ilyen pl.: célzott reklámokkal bombázás, vagy a késedelmes fizetés esetén az automatikus szerződés felbontás.) Ha profilalkotást alkalmaznak arról teljeskörű felvilágosítást kell adni.

Kézenfekvő példázat erre az, ha bizonyos szervezet Facebook pixeleket alkalmaz (ez egy reklámos nyomkövető, ismertetése a 3. fejezetben található) arra, hogy testre szabott promotálást alkalmazzon, amihez különféle kategorizálást végez (szegmentálás), melyről szintén felvilágosítást kell igény esetén adnia. [5, 15]

A GDPR érvénybelépésének elején, különleges tévhitet okozott idehaza, legfőképp félreértelmezés folytán. Ugyanis számtalan szervezet törölte e-mailes adatállományát, mert úgy tartották, ha nem tudják bebizonyítani, hogy a felhasználóktól engedélyt kaptak az adatok kezelésére, akkor jogellenesen kezelik és szankció vár rájuk.

Ezzel szemben a GDPR preambuluma rögzíti a rendelet megjelenése előtti állapotot, hogy azt hogyan kell kezelni. E szerint, a korábbi adatbázisokat nem kell törölni akkor, ha kizárólag azért nem tesz eleget a rendeletnek, mert az új tájékoztatási kötelezettségeket a megelőző jogszabály szerint nem tudta az adatkezelő végrehajtani.

Abban az esetben viszont, ha nem volt megfelelő jog szerinti felhatalmazása az adatkezelésre, vagyis ha nem kért engedélyt a reklám célú üzenetek küldéséhez, azaz spam-elt, azt az adatbázist viszont törölni kényszerült. [15]

A magyarországi szabályozás korábban és jelenleg is szigorúbb, mint a GDPR, hisz régóta a reklámok küldéséhez idehaza hozzájárulás kell.

Ha valaki GDPR következtében törölte az adatállományát, az vagy porul járt, mert szabályosan végezte az adatok kezelését vagy ezidáig is jogtalanul kezelt adatokat. [6]

A magyar domén-adatbázist kezelő testület a GDPR miatt úgy határozott, hogy nem nevesíti a domén-tulajdonos nevét, mindössze „természetes személy” fog szerepelni rákeresés esetén. Ennek a testületi döntésnek hátulütője, ha védjegybitorlás vagy szerzői jogsértés okán peres eljárásban, nehezen beazonosítható hogy kit kell milyen elérhetőségen keresni kiváltképp, ha az elengedhetetlen impresszum sem található meg az internetes oldalon. [6, 15]

A TMSI Kft., aki informatikai rendszerekkel, illetve a GDPR-ra történő felkészítéssel foglalkozó cég, megvizsgálta, hogy az itthoni cégek, mennyire felkészültek a GDPR alkalmazására.

A vizsgálatuk eredménye alapján megállapítható volt, hogy a cégek internetes oldalán az előírt adatkezelési nyilatkozat a cégek durván kétharmadánál volt megtalálható, a maradék arányban viszont nem volt fellelhető, ezen szervezetek javarészt állami tulajdonúak.
A szervezetek 90 %-ban válaszoltak a megkeresésre, a maradék 10 % pedig egyáltalán nem jelzett vissza.
Az adatkérők hitelesítését mindössze 14,3 %-uk hajtotta végre, amivel elkerülhető a személyes adat kikérés utáni jogosulatlan felhasználása. Emellett 83 %-ban pedig rossz visszajelzés érkezett az adatkérésre. [6, 15]

2.2 A személyes adatok védelme a GDPR tükrében – hatósági feladatok

A GDPR az érintettek és az adatkezelők mellett a felügyeleti hatóságok működésére is megállapít komoly előírást.
Az adatvédelmi irányelv előírja az EU tagországainak a felügyeleti hatóságok létrehozását. Az EU tagországaiban történő adatvédelmi irányelv beültetése eltérő jogértelmezéssel párosult bizonyos hatóságoknál.
Az adatvédelmi irányelv azzal, hogy közvetlenül alkalmazandó az EU tagországaiban, nagymértékben redukálta a tagországok felügyeleti hatóságainak lehetőségeit. Ezzel az Unióban egységesítésre került az adatvédelmi szabályok alkalmazása és ellenőrzése. [10, 15]
Az irányelv egyetemesen szabályozza a nemzeti felügyeleti hatóságok jogállását, ide értve a feladat- és hatáskörüket és a hatóságok egymás közötti együttműködési keretrendszerét.
A felügyeleti hatóság önálló közhatalmi szerv, melynek legfontosabb feladata a természetes személyek jogainak védelme a személyes adataik kezelésében.
A GDPR 58. cikke Hatáskörök alatt a (1) felügyeleti hatóság vizsgálati hatáskörét, a (2) a felügyeleti hatóság korrekciós hatáskörét, a (3) a felügyeleti hatóság engedélyezési és tanácsadási hatáskörét sorolja fel.
A felügyeleti hatóság vizsgálati hatásköre között szerepel b) vizsgálatot folytat adatvédelmi auditok formájában, ezzel az adatkezelő jogszerű működését megvizsgálja.
A felügyeleti hatóság korrekciós hatáskörében eljárva felhívja a figyelmét az adatkezelőnek vagy az adatfeldolgozónak, ha az adatkezelési tevékenységei feltételezhetően megsértik a rendeletet. Megbünteti az adatkezelőt vagy az adatfeldolgozót, ha az adatkezelési tevékenysége megszegte a rendelet előírásait. Elrendeli az adatkezelőt vagy az adatfeldolgozót, hogy hajtsa végre és tegye lehetővé az érintettek a rendelet szerinti jogai szerint megillető kérelem gyakorlását. Bizonyos esetben a felügyeleti hatóság ideiglenesen avagy végérvényesen korlátozza az adatkezelést, beleértve az adatkezeléstől való eltiltást is. A felügyeleti hatóság közigazgatási bírságot is meghatározhat a rendeletben foglaltak szerint.

A felügyeleti hatóság rendelet szerinti hatáskörében eljár a személyes adatok kezeléséhez köthető engedélyek és az adatvédelmi auditokat követő tanúsítványok kiadásában. Emellett ajánlásokat tesz az adatkezelőnek és egyéni kezdeményezésre vagy kérelemre álláspontot kiad a jogalkotó felé. [10, 15]
A GDPR rendelet szerint a felügyeleti hatóságok kétoldalú segítséget nyújtanak az egységességre való tekintettel egymásnak a határon átnyúló estekben, ahol együttesen rendelkeznek. Több érintett felügyeleti hatóság esetében kinevezésre kerül a fő felügyeleti hatóság, aki az ügymenetben a kapcsolattartó szereplő.
A rendelet úgy rögzíti, hogy „*Az adatkezelőt és az adatfeldolgozót egyaránt érintő esetekben továbbra is annak a tagállamnak a felügyeleti hatósága az illetékes fő felügyeleti hatóság, amelynek területén az adatkezelő tevékenységi központja található, azonban az adatfeldolgozó felügyeleti hatósága érintett felügyeleti hatóságnak tekintendő, ennek a felügyeleti hatóságnak részt kell vennie az e rendeletben meghatározott együttműködési eljárásban.*”
A fő felügyeleti hatóság irányítja az érintett hatóságokkal való közös együttműködést. A fő felügyeleti hatóság az érintett felügyeleti hatóságokkal együtt az összes fontos információt megosszák egymással.
A fő felügyeleti hatóság a határozat tervezetét azonnal továbbítja a másik érintett felügyeleti hatóságnak véleményezés céljából, aki álláspontját elégséges módon tekintetbe veszi. [10, 15]
A nemzeti felügyeleti hatóságok mellett az Európai Adatvédelmi Testület ugyancsak részt vesz a személyes adatok védelméhez való jog, valamint a GPDR-ban foglalt rendelkezések kontrolljában.
Az Európai Adatvédelmi Testület (European Data Protection Board - EDPB) önálló európai szerv, aki az Unió területén elősegíti az adatvédelmi szabályok következetes felhasználását, ezenfelül támogatja az uniós adatvédelmi hatóságok kooperációját.
Az Európai Adatvédelmi Testület tagjai a nemzeti adatvédelmi hatóságok képviselői valamint az európai adatvédelmi biztos. Az általános adatvédelmi rendeletet tartalmazó kérdésekben úgyszintén a testület tagjai az EFTA–EGT-tagállamok felügyeleti hatóságai. [10]
A GDPR bevezetését követő félévben csaknem 95 000 adatvédelmi kifogást kaptak a felügyeleti hatóságok az érintettektől, ezek zöme a reklám célú (telefonos vagy e-mailes) megkeresés, ezenkívül kamerával történő megfigyelés volt.
Az adatkezelők 41 502 adatvédelmi incidenst jeleztek ugyanezen időszakban a hatóságoknak, ez tagállamonként átlagban 185 db/hó/incidens. [7]
A legsúlyosabb eset ezek közül a Google-nak tulajdonítható, az ügyfelek nem kielégítő, elégtelen tájékoztatása révén, ezt a francia adatvédelmi hatóság (Commission Nationale Informatique & Libertés - CNIL) 2019 elején 50 millió euróra büntette.
A hatóság nyilatkozata alapján, a Google adatvédelmi tájékoztatója túl messze volt egymástól (5-6 vagy több kattintásra, illetve több dokumentumban). Emellett a Google-nál be volt jelölve a személyre szabott hirdetésekhez való hozzájárulás választási lehetőség

alapértelmezetten, ami ellentmond a GDPR előírásának, miszerint az érintett jóváhagyásának egzakt, vitathatatlan beleegyező lépéssel kell megvalósulnia.
A francia adatvédelmi hatóság a fent bemutatottak miatti magas büntetést azzal magyarázta, hogy számottevő érintett személy volt kitéve a folyamatos és állandó jogellenes magatartásnak.
Megjegyezzük, hogy ez a metódus a MediaWorks csoporthoz tartozó honlapok (Origo és az Index) süti-kezelésére is fennáll, ugyanis a jóváhagyás nagyon gyorsan egyetlen gombnyomással lehetséges, azonban az elutasítás már több macerával jár, hosszas scrollozást követő átkapcsolással van rá mód, ami a felhasználót a „könnyebbik megoldás" felé tereli.
A NAIH 2018 évi közleménye alapján, 414 adatvédelmi eljárás volt itthon, ami tetemes az azt megelőző évhez viszonyítva.
Az adatvédelmi eljárások zöme a szigorúbb GDPR hatályba lépését követően volt. Ugyanakkor megjelent a szabályozással kapcsolatos aggály is, amit a kétszeresére nőtt konzultációs kérelem is bizonyít. [15]
A rendelet hatályba lépése után idehaza 50 hatósági eljárás iránti bejelentést rögzített a NAIH, mely legtöbbje munkahelyi, egészségügyi, banki adatkezeléssel volt kapcsolatos, emellett az érintett jogait nem tudta gyakorolni a teljesítés megtagadásával vagy elmulasztásával, ezenfelül a kamerás megfigyeléshez volt köthető.
A rendelet hatályba lépésével megjelent a felügyeleti hatóság általi hatósági kontroll az adatvédelmi incidensek során.
A NAIH-hoz 244 db adatvédelmi incidenssel kapcsolatos bejelentés érkezett 2018-ban az adatkezelők részéről. A bejelentett incidensek száma csekély, amivel arra lehet következtetni, hogy az adatvédelmi incidens ismerete, az ezzel járó bejelentési kötelezettség még nem volt ismert. [15]
Az adatvédelmi incidensek a felügyelet általi nyilvántartás alapján, a lenti rendelet elleni vétségekből származott:

- papír alapú továbbá digitális levelek fals címre küldése miatt,
- elektronikus levelezési címek helytelenül kerültek felhasználásra, merthogy másolatként és nem titkos másolatként lettek elküldve, így másolatként mindenki láthatta a másik címét,
- az adatkezelőtől incidens miatt kikerült személyes adatok,
- eltulajdonított vagy elhagyott informatikai eszközök és telefonkészülék miatt.

A NAIH weboldalának közzététele alapján, itthon a GDPR előírásaink nem teljesítésért 2018.12.21.-ével szabott ki először büntetést. A NAIH által kivetett legtetemesebb szabályszegés, ami hatalmas hírt is gerjesztett egyben a Demokratikus Koalíció párt (DK) szabálytalanságához köthető.
A NAIH által hozott határozat alapján, a DK által üzemeltetett portál hackertámadása során személyes adatok, úgymint az elektronikus levelezési címek, felhasználói nevek amellett jelszavak kitudódtak és a weben szabadon hozzáférhetővé váltak. Ennek az inci-

densnek a jogszabály szerint előírt hatósági bejelentésének a DK nem tett eleget, mindezek mellett az érintettek részére sem jelezte. A DK, jókora 11 millió Ft összegű büntetést kapott, mivel a hatóság rendkívül nagy kockázatúnak minősítette az incidenst, tekintve hogy olyan rendkívül érzékeny közéleti nézethez társuló információ került ki, amivel több ezernyi (6000-nél is nagyobb számú) felhasználó vált érintetté. [15]
A 2018-ban bevezetett GDPR a NAIH intézményében jókora átalakulást hozott. A rendelet szerinti hatósági feladatok ellátására a szervezetnek bővülésre és átalakulásra volt szüksége, ennek keretében új osztály, részleg, pl: Engedélyezési és Incidensbejelentési Főosztály, alatta Incidensbejelentési Osztály és Engedélyezési Osztály, vagy Tanúsítási és Társadalmi Kapcsolatok Főosztálya, alatta Társadalmi Kapcsolatok Osztály és a Tanúsítási Osztály jött létre. Ennek következményeként a hatósági dolgozók létszáma is majd kétszeresére növekedett. [15]
A hatósági ügymenetben a GDPR szigorúan és egzakt módon meghatározza az eljárásokat, az Infotv. ezzel szemben szabadabban kezeli a választható eljárás típusát. Mivel a GDPR szigorúbb rendelet, az életbe lépésével megnövekedett a hatóság felé érkező bejelentések mennyisége, ami megnövekedett ügyintézési idővel jár.

3 A FELHASZNÁLÓI PROFILALKOTÁS (USER PROFILING) BEMUTATÁSA, JELENLEGI ALKALMAZÁSA, JÖVŐBENI IRÁNYOK, MÓDSZEREK

A user-profiling definíció szerint: „…az adatbázisokban szereplő adatok és információk közötti viszonyok „felfedezésének" azon folyamata, amely emberi vagy nem-emberi alanyok (egyének vagy csoportok) azonosítására, ábrázolására használható és/vagy az egymással kölcsönös viszonyban lévő adatok csoportjainak alkalmazásával alkalmas egy megfigyelt alany azonosítására és ábrázolására, esetleg arra, hogy egy adatalanyt egy csoport vagy kategória tagjaként azonosítson".
Felhasználói profilalkotási csoportok az alábbiak (csoportosítás a létrehozás szerint) [1, 2, 8]:

- *explicit*: a felhasználók direkt megkérdezésén alapul, pontosságát tekintve magas, jelentős ráfordítás árán szerzett,
- *implicit*: automatizált módon megszerzett, a user keresési előzményein alapuló, ráfordítását tekintve jelentéktelen erőfeszítéssel összeszedett adat. A pontosításához jelentős mennyiségű további információt/adatot kell feldolgozni,
- *hibrid*: az előbbi két mód kombinációja.

A user profiling-al legtöbbször a személyes adatok fizetőeszközként való felhasználása során kerülünk kapcsolatba: vagyis amikor látszólag térítésmentes szolgáltatást vesz valaki az interneten igénybe, ekkor számos alkalmazás a személyes adataik megadása után enged csak tovább lépni, kvázi azok felhasználásával és tovább értékesítésével fizetik meg a felhasználók a szolgáltatást, sokszor nem is tudva erről. Minél nagyobb valakinek az ún. „digitális lábnyoma" az interneten, annál több információ áll rendelkezésre róla, így

azokat kombinálva lehetőleg minél több további következtetésre alkalmas információt lehessen az egyénről kinyerni.
A felhasználói profilalkotás másik gyakorlati példája, mikor nagyvállalati rendszerekben a különböző felhasználók egyéni beállításai, felhasználásra kerülő szoftverei és egyéb alkalmazások egyedileg kerülnek beállításra és azok központilag letárolásra.
A felhasználói profilozás céljai:

- személyre szabott tartalmak előállítása,
- szűrőbuborék létrehozása a célcsoportok számára,
- megfigyelés és befolyásolás (szűrőbuborékon keresztül, illetve a kapott információk módosításával),

A felhasználói profilozás jelentősége az egyénekről rendelkezésre álló egyre több adat tükrében és az egyre hatékonyabb eszközök megjelenése következtében egyre nagyobb.
A leggyakoribb, az átlagos felhasználóknak jelenleg a legkevésbé ismert és felismert profilozási lehetőséget az online keresések és vásárlások jelentik.
Internetes keresés során a felhasználói, és a szerver oldalon is történik adattárolás, amely lehetővé teszi, hogy a felhasználók szokásai, földrajzi helye és a megtekintett weboldalak szerint egyéb jellemzőit meg lehessen határozni és ezáltal lehetővé tegye a profilalkotást. [4]

A profilalkotás felhasználó oldali eszközei és folyamatai

A felhasználók az eszközeiken lévő böngészők segítségével jelenítik meg a tartalmakat.

Böngészők

Az interneten lévő adatok és információk megjelenítésére a felhasználói oldalon különféle HW eszközök állnak rendelkezésre, amelyek sok esetben egymástól nagyobb mértékben el is térhetnek. Ez a szoftveres oldalon okozhat jelentősebb módosításokat, amelyek miatt a honlapokat eszközcsoportokra optimalizált változatban szokás elkészíteni. Mivel minden eszközre külön-külön elképzelhetetlenül sok változatban kellene a tartalmakat legyártani, ezért az ún. „responsive design” terjedt el, amely a gyakorlatban az adott kijelzőre optimalizált tartalom megjelenítést jelenti.[14]
A korábbi internetes böngészők a tartalmat a szerveren generálták le, külön domain alá helyezve a mobil (m) tartalmakat és a különböző változatokat, napjainkban ez a kijelző szélességének függvényében dinamikusan változik.

A böngészőkben alkalmazott programozási nyelv a JavaScript, amely lehetővé teszi a dinamikus változtathatóságot, ugyanakkor sebezhetővé is teszi a felhasználó oldalt. [14]
A gyakorlat azt mutatja, hogy egy-egy felhasználó rendszerint több eszközt – értjük ez alatt, hogy többféle böngészőt – alkalmaz, legtöbbször ugyanazon fizikai eszközön kü-

lönböző alkalmazások formájában. Ezek a különböző alkalmazások ugyanakkor nem képesek egymás kliens-oldali adataihoz hozzáférni, így a felhasználó követését sem tudják alkalmazásokon keresztül biztosítani. Amennyiben a felhasználók böngészési előzményeinek felderítése a cél, akkor mindenképpen az eszközön lévő összes kliens oldali eszköz adatait figyelembe kell venni [3, 14]
A szakirodalom a felhasználó oldali tartalom megjelenítő eszközöket „user agent"-nek is nevezi, a későbbiekben böngészőként hivatkozunk rájuk. A gyakorlatban 5-6 böngésző tarolja le a piacot, amelyek piaci részesedése a 2. táblázatban került összefoglalásra.

	Microsoft Internet Explorer/Edge	Mozilla Firefox	Google Chrome	Apple Safari	Opera
2022. március	9,65%	7,57%	67,29%	9,56%	2,81%

2. táblázat. Az 5 leggyakoribb kliens oldali kereső piaci részesedése [13]

A böngészőkben használt megjelenítő motorok – amelyek végső soron a Javasript utasításokat végrehajtják felkereséskor – a 3. táblázatban kerültek összefoglalásra.[14]

Böngésző	**Megjelenítő motor**
Microsoft Edge	Edge HTML
Microsoft Internet Explorer	Trident
Mozilla Firefox	Gecko
Google Chrome	Blink
Apple Safari	WebKit
Opera	Presto

3. táblázat: Néhány ismertebb kliens oldali eszköz és megjelenítő motorja [14]

A felhasználó oldali eszközökben hozzávetőlegesen 2008-2010 környékén került bevezetésre az **inkognitó mód**. Az inkognitó mód lehetővé teszi, hogy a normál böngészéshez képest kevesebb adatot mentsenek le a felhasználó oldali eszközök, így csökkentve az adatok strukturált gyűjtését. Normál módban ugyanis legalább az alábbi adatok lementésre kerülnek:

- weblapok tartalma
- lapok látogatási időpontja
- cookie-k, localStorage és sessionStorage

A tartalom lementése a netes forgalmat tudja ugyan csökkenteni, hiszen csak a megváltozott részeket kell frissíteni, azonban a mentések lehetővé teszik, hogy a felhasználó keresési előzményei visszanyerhetők legyenek. Az inkognitó mód ennek megy elébe – a böngészés után nem hagy adatot az eszköz háttértárolóján, így mind a sütik, mind a LocalSession tartalma törlődik és az előzmények nem kereshetőek vissza. A honlapok szerver oldali nyomonkövetésétől azonban az inkognitó mód sem tud megóvni senkit. [14, 2, 5]

http header

Az internetre csatlakozó böngészők a „HyperText Transfer Protocol“-t (azaz HTTP-t) alkalmazzák kommunikációs nyelvként, amely lehetővé teszi az adatcserét paraméterek, parancsok alkalmazásával. A felhasználói oldal (számítógép böngészője) és a kiszolgálói (a honlap szerverén lévő program) oldal közötti adatcsere tulajdonképpen kéréseket („requests“) foglal magában, amelyeket a felhasználó a böngészés kezdetekor a kiszolgáló felé küldd. Valamennyi kliens-szerver interakciónak 3 fő része van:

1. Egy sor az igény vagy válasz típusának megjelölésére
2. Header információk
3. A kapcsolat tartalma

A fenti részekből a kapcsolat tartalmi részén felül a Header rész tartalmaz a nyomon követés kapcsán értékelendő információkat.
A kliens oldalon lekérdezés fejléc tartalma a 4. táblázatban szereplő adatokat tartalmazza

Operating system	Windows 10
IP address	176.63.9.232
Javascript enabled	Yes
Cookies enabled	Yes
Flash version	Not installed
Java version	Not installed
Websockets supported	Yes
WebGL supported	Yes
Language	hu-HU
Browser size	2543 x 1339
Screen size	2560 x 1440
Color depth	24 bit

Your full user agent string is:

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

4. táblázat, www.whatismybrowser.org által kiadott eredmények (saját felvétel)

A HTTP fejléc tulajdonképpen több adatcsomag egymás utáni felsorolása, ahol minden rész a felhasználói oldal egy-egy különleges részletét tartalmazza.
A „DNT” Do-Not-Track, vagyis hogy ne kövessenek egybites kapcsolója.
Az „ACCEPT“ adja meg azokat a file-okat, amiket a felhasználói oldal fogadni tud.
A „REFERER“ adja meg azt a visszahivatkozást, hogy honnan keletkezett az igénylés.
A „USER_AGENT“ adja meg a kliens oldali eszköz típusát, verziószámát.

A fentiekből igazából a User-Agent mező tartalmaz a nyomon követéshez használható információkat:

- Mozilla böngészővel való kompatibilitás
- A kliens oldali operációs rendszer főbb adatai
- A kliens oldali eszköz megjelenítő motorjának neve és verziója
- Kliens oldali eszköz neve és verziója
- Aktív szolgáltatások, egyéb jellemzők

Do Not Track (DNT)

A fejlécben látható adatcsomagok közül a kliens oldalról elküldött DNT paraméter a HTTP fejlécben fontos jelentőséggel bír a nyomon követés szempontjából. A DNT a **Do-Not-Track** rövid változata, ami magyarul annyit jelent: "ne kövess". Amennyiben a kliens úgy tartja jónak, hogy a felkeresett oldal vagy harmadik fél ne gyűjtsön adatokat róla, akkor, a kliens oldali eszköz a HTTP kérés fejlécben bejelöli ezt az adatot a kiszolgáló oldali eszköz számára. Napjaink felhasználó oldali eszközei szinte kivétel nélkül tudják a DNT funkciót, azonban a felhasználóknak csak elenyésző száma használja. Példaként érdemes megemlíteni, hogy a Firefox használók 90%-a nem használta ezt a rendelkezésre álló funkciót 2012 év végén. A funkció alkalmazásáról nem kapnak a user-ek visszajelzést. Maga a funkció hasznos lenne, ugyanakkor a jövőbeni alkalmazása igencsak kétséges, hiszen egyrészről pont létezése révén lehet bizonyos kliens oldali eszközök alkalmazásáról meggyőződni, másrészről pont az a Yahoo! függesztette fel az alkalmazását 2014-ben, amely legelőször használni kezdte.
[14, 5, 2]

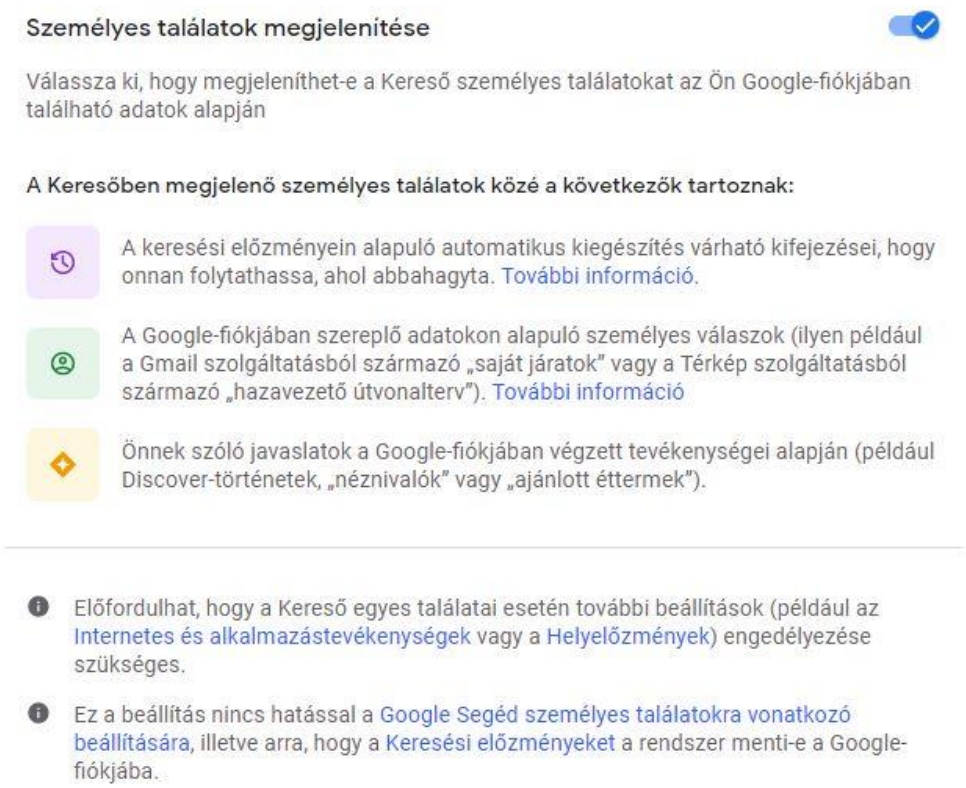
A letöltött és megőrzött adatok - munkamenet a http kapcsolatban

A HTTP kapcsolatokon alapuló felhasználói és kiszolgáló oldali kommunikációnak azt a formáját, amikor a felek egymásról átmenetileg adatokat tárolnak – bár állapotmentes protokollon keresztül történik a kommunikáció - munkamenetnek nevezzük. A legegyszerűbb és legkönnyebb megoldása a munkamenet kialakításának az ún „session cookie”-k alkalmazása, amelyek a kliens oldali eszköz bezárásakor törlődnek.. Működése úgy történik, hogy kiszolgáló az első kapcsolatfelvétel alkalmával elküld egy azonosítót a kliens oldali eszköznek, a saját adatbázisában pedig adatokat tárol ehhez az azonosítóhoz kapcsolódóan (bejelentkezés, IP cím, NAT, proxy, stb.). Mivel a kliens oldali eszköz ezt az azonosítót minden lekérdezés alkalmával visszaküldi, ezért a kiszolgáló tisztában van a felhasználó állapotával.

Nem megfelelően kezet vagy előállított munkamenet azonosító megszerzésével lehetőség nyílik az ún „session-hijacking” támadás. [14, 5, 2]

Abban az esetben, ha a felhasználó oldalán a sütik letiltásra kerülnek, és a weblap nem megfelelően felkészített, akkor a felhasználók nem fognak tudni belépni, mert a munkamenet fejlécében nem jelennek meg a munkamenet azonosítók.

A google a böngészőjében biztosítja, hogy a user-ek a munkamenetekben gyűjtött adatok alapján készült google ajánlásokat kikapcsolhassák. A funkció az adatvédelmi beállításokban érhető el (lásd. 1. ábra), ugyanakkor fontos megjegyezni, hogy ez csak az ajánlásokat kapcsolja ki, magát az adatgyűjtést nem.

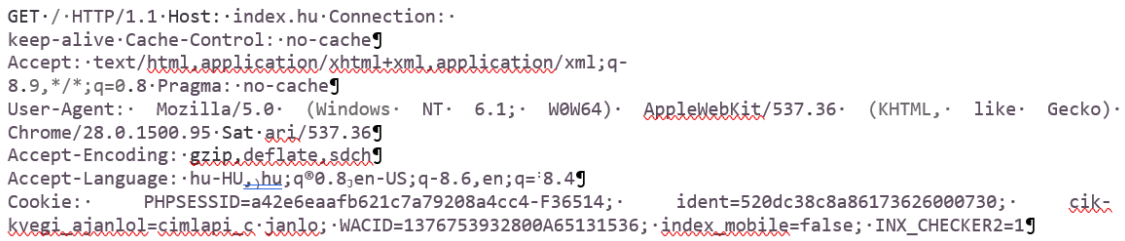


1. ábra A Google Account Adatok és Adatvédelem beállításai (saját mentés)

Azon honlapok esetén, amelyeknek a cookie-kat nem támogató böngészőkben is futniuk–kell - ilyenek például a banki rendszerek is – más módon történik a munkamenet azonosító átküldése (p. query string felhasználásával). [3, 14]

Felhasználó oldali adattárolás a HTML fejlődésével

A HyperText Markup Language, röviden HTML az a megjelenítő nyelv, amely a megjelenése óta már általánosan elterjedt szabvánnyá vált.



2. ábra, HTTP fejléc (archive.org az index.hu-ról 2017-ből) [18]

A 2. ábrán egy HTTP lekérdezés fejléce található. Az első sor a metódust adja meg (GET), protokoll a HTTP 1.1. A második sor a host, ez tartalmazza a lekérdezés adatait.
2014 óta a HTML5 az aktuális verziója, amelyben a korábbi verziókkal való kompatibilitás is megoldott.
A HTML5-ben az adattárolási – és ezáltal a profilozási lehetőségek is – kiszélesedtek, hiszen nem csupán cookie-ek, hanem Web Storage tárolásra (localStorage és sessionStorage) is mód nyílik, amely a sütik méretét jóval meg is haladja. [14]
A megadott WebStorage technológiák (localStorage és sessionStorage) a sütik analógiájához hasonlóan a kiszolgáló és a felhasználó oldali technológiákat takarják azzal a különbséggel, hogy a localStorage tartalma a felhasználó oldali eszköz bezárása után is hozzáférhető marad. [8]
A http://panopticlick.eff.org honlap megmutatja, hogy a felhasználó böngészője milyen specifikus jellemzőkkel bír, így adott esetben egyedi azonosításra is felhasználható. [14, 5, 20]
A saját böngészőn futtatva igazolásra került, hogy annak jellemzői, az elmúlt 45 napban vizsgált böngészőkhöz képest (176 357 db számszakilag) egyedi vonásokat tartalmaz, így beazonosítható.
A honlap által vizsgált jellemzők az alábbiak:
Fejléc információk:

- User agent információk: ez a vizsgált böngésző esetén az alábbi: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36. A honlap szerint ezen jellemzők alapján az alkalmazott böngésző és a felhasználó egyértelműen beazonosítható.
- HTTP_ACCEPT HEADERS: értéke: text/html, */*; q=0.01 gzip, deflate, br hu-HU,hu;q=0.9,en-US;q=0.8,en;q=0.7,ar;q=0.6. Ezen adatok annak megadására szolgálnak, hogy jelezzék a kiszolgáló felé, hogy a felhasználó oldali eszköz milyen tartalmat képes fogadni.

Böngésző információk:

- BROWSER PLUGIN DETAILS: azon külsős fejlesztésből származó böngésző bővítményeket listázza, amelyek a sérülékenységük révén akár támadási felületek is lehetnek.

- TIME ZONE OFFSET: mivel időzónákra vonatkozó információkat nem küldenek a kiszolgáló és a felhasználó oldali kommunikáció során a header részben, így a GMT zónához képesti eltérést kerül csak kommunikálásra.
- TIME ZONE: olyan adat, amely a tartózkodási helyre vonatkozóan ad információt (Pl. America/San Antonio).
- SCREEN SIZE AND COLOR DEPTH: kevésbé használt információ a nyomon követéshez, hiszen a felhasználók oldaláról ezek a beállítások könnyen megváltoztathatók.

Ujjlenyomat információk:

- SYSTEM FONTS: telepített karakterkészletre vonatkozó adatok. Hasznosságuk abban rejlik, hogy amennyiben akár egyetlen olyan betűkészlet is telepítésre kerül a böngészőben, amely alapértelmezésben nincs benne, akkor egyedivé teszi azt a felhasználó oldaláról.
- ARE COOKIES ENABLED: a sütik engedélyezésére vonatkozó információ. Jellemzően nem önmagában, hanem más jellemzőkkel kombinálva van jelentősége.
- LIMITED SUPERCOOKIE TEST: Ezek igazából nem a hagyományos értelemben vett sütik, hanem olyan paraméterek, amelyekkel a különféle honlapokon eltöltött böngészési időtartamok, bejelentkezési információk stb. Fontos jellemzőjük, hogy még a hagyományos sütik törlésre kerülnek, ezek a jellemzők viszont nem.
- HASH OF CANVAS FINGERPRINT: A nyomon követésre igen jól használható ujjlenyomat-mintát ad ez a jellemző. A videokártya, annak drivere, az operációs rendszer, valamint a telepített betűtípusok következtében különféle képek megjelenítése különféle jellemzőket generál ezen jellemzők eltérései alapján.
- HASH OF WEBGL FINGERPRINT: Az előzőhöz hasonló működéssel bíró jellemző.
- DNT HEADER ENABLED: A Ne Kövessenek jellemzőt napjainkban már egyre kevesebben használják önmagában, ugyanakkor más jellemzőkkel kombinálva a felhasználók profilozására alkalmas lehet.
- LANGUAGE: Ez a jellemző akkor lehet alkalmas a felhasználó beazonosítására, amennyiben az adott időzónában nem túl gyakori nyelvről van szó.

HW jellemzők:

- PLATFORM: A számítógép konfigurációjától függően (CPU, operációs rendszer) alkalmas a felhasználók azonosítására.
- TOUCH SUPPORT: Az adott eszközön lévő érintés érzékelők számát jelöli (képernyő, touch pad).
- AD BLOCKER USED: Ez a jellemző azt figyeli, hogy van-e az adott eszközön hirdetés-blokkoló installálva.
- AUDIOCONTEXT FINGERPRINT: Hasonló elven működik, mint a CANVAS FINGERPRINT, azonban a grafikus jellemzők helyett az eszköz audio eszközei alapján állít elő egyedi azonosítót.

- CPU CLASS: Ez a jellemző csak azt figyeli, hogy ki a CPU gyártója.
- HARDWARE CONCURRENCY: Ez a jellemző a CPU magok alapján állít elő azonosítót.
- DEVICE MEMORY: Ez a jellemző az eszközön hozzáférhető memória egészre kerekített értékét adja meg GB-ban.

A felhasználók online-tevékenységén alapuló nyomon követési módszerek fejlődését az alábbi egyszerű 3. ábra is összefoglalja.

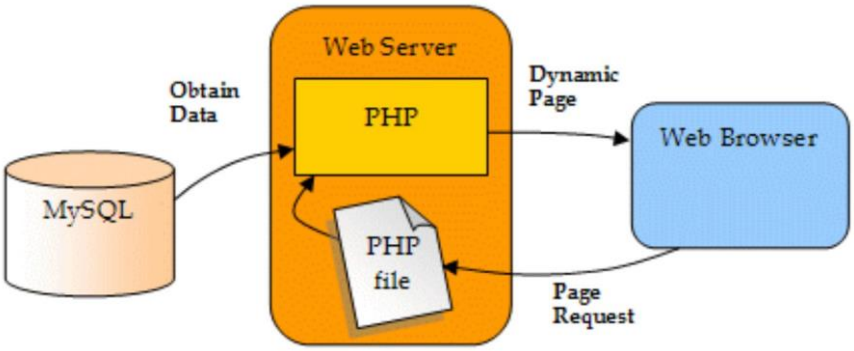
3. ábra, Nyomonkövetésre alkalmas technológiák alakulása [14]

A profilalkotás kiszolgálói oldal eszközei és folyamatai

A felhasználó oldali adattárolással szemben a kiszolgáló oldali munkamenet-tárolás az alábbi okokból kedvezőbb:

- adatok a kiszolgáló oldalon tárolódnak, a felhasználó oldalán nem is jelennek meg,
- adatok, jellemző paraméterek nem kerülnek továbbításra feleslegesen a kiszolgáló és a felhasználó között,
- a kiszolgáló oldalon tárolt és azonosított adatok a munkamenet-azonosítóval (sütiben vagy URL-ben tárolva) a szerver oldali adatbázisból lekérhetők és felhasználhatók,

A működését tekintve a 4. ábrán feltűntetett lépések során a felhasználó oldali eszköz a kiszolgálóval beszélget, amely a lekérdezés eredményeképpen kiszolgáló oldalon előállítja a megjelenítendő weblapot.. A PHP kód az adatbázisban tárolt munkamenet-azonosítót felhasználva további paraméter-beállítások sorozatán keresztül előállítja a megjelenítendő HTML tartalmat, ami visszaküldésre kerül a felhasználó számára. , [14]



4. ábra: Kiszolgáló oldal kapcsolata annak adatbázisával és a felhasználó oldali megjelenítővel [14]

Profilozásra alkalmas technológiák

FLoC:

A sütik körül kialakult ellenszenv miatt, valamint az anonim kategorizálás biztosítására jelent meg a FLoC (Federated Learning of Cohorts) technológia, amely az érdeklődési köreik alapján a nagyszámú felhasználók mennyiségét homogén kategóriákba sorolja. Elméletileg a technológia nem alkalmas az egyének azonosítására, hiszen legalább 1000 felhasználóból álló csoportokat hoz létre, azonban a kliens oldali eszköz egyéb adattárolási metódusaiból további személyes adatok nyerhetők ki. [11]
Hátránya pont ezekkel a másodlagos technológiákkal való összekötési lehetőségből adódik: egyéb adatok gyűjtésével (pl. header adatok), akár az IP címmel is összekapcsolhatóvá válik az adott személy kliens oldali eszköze, ezáltal egyértelműen beazonosíthatóvá válik. Jó hír, hogy létezik olyan honlap, ahol a FLoC adott felhasználón történő alkalmazásáról meggyőződhetünk (https://amifloced.org/ [11, 12].
A Chrome-on kívül (aki a fejlesztője a technológiának) számos más kliens oldali eszköz fejlesztő elzárkózott a FLoC alkalmazásától, hiszen felismerték annak a veszélyét benne, hogy a csoportok képzésén keresztül akár a sütikénél is pontosabb profilozás válik alkalmazásával lehetővé. [11].
Facebook képpont vagy Facebook pixel:
A Facebook-pixel a személyes hirdetések hatékony elemzésére jött létre, gyakorlatilag a felhasználó tevékenységeit elemzi és azok alapján vonja le következtetését.
A Facebook pixel felhasználása az alábbiakra terjed ki:[8]

- Célzott hirdetések megjelenítése, új ügyfelek szerzése meghatározott lépések alapján.
- Új ügyfelek szerzésén keresztül az értékesítés növelése.
- A célzott hirdetésekkel azok eredményességének növelése és egyben mérhetőségük javítása.

A Facebook-pixel meghatározott tevékenység végrehajtása után aktiválódik és elkezdi az adatokat, lépéseket gyűjteni. Egyre több információ és az azok közötti összefüggések fényében a Facebook egyre hatékonyabban tudja megcélozni az elérni kívánt célcsoportot, ezt hívja a szakirodalom konverzióoptimalizálásnak. [8]
Az Apple szerencsére azonban az iOS 14 megjelenésével lehetővé tette ügyfelei számára, hogy az AppTrackingTransparency keretrendszer alapelvei alapján a Facebook pixelhez hasonló eszközök adatgyűjtésétől el lehessen zárkózni. [7].
TweetPsych: a Twitterre alkotott olyan elemző eszköz, amely gyakorlatilag a bejegyzések 140 karakteres láncának (ebből is kb. 1000 db bejegyezés szükséges egy személytől) elemzése alapján képes meghatározni az adott személy tudatos és tudat alatti szándékait.

Rep'nUp: egy olyan szolgáltatás, amely adott felhasználó esetén annak Facebook, Twitter és Instagramm fiókjai elemzése alapján megállapítja, hogy potenciálisan történt-e a múltban olyan bejegyzés, amely később gondot okozhat. Gyakorlatilag SWOT elemzést végez az adott felhasználón.
Apple Magic Sauce: az előző eszközhöz teljesen hasonló működésű és célú eszköz, amellyel lehetővé válik annak bemutatása egy adott felhasználó számára, hogy a Facebook, Twitter és Instagram fiókjai alapján hogy látja őt a külvilág. .
Data Selfie: egy olyan bővítmény – Google Chrome-hoz és Firefox-hoz– amely elsősorban a Facebook-on végzett tevékenységeket monitorozva képes feltárni, hogy milyen gépi tanulási algoritmusok jöhetnek szóba egy adott személy személyiségének meghatározásakor. A projekt 2018-ban elvileg befejeződött.

Maltego

A Maltego egy nyílt adatforrásból dolgozó, vagyis publikus adatokból dolgozó program (OSINT), fejlesztője a Paterva. A program arra a célra került kifejlesztésre, hogy egy olyan összekapcsolt adatbázist nyújtson a felhasználójának, ahol valamennyi szabadon hozzáférhető adatot össze lehet rendelni egy közös cél érdekében (kapcsolatok elemzése, adatvizualizáció). [16]

A Maltego használatával objektum orientáltan lehet vizualizálni a különböző szintű kapcsolatokat és jellemzőket, így nem csupán emberek, telefonszámok weblapok, hálózatok és azok részei, hanem közösségi hálózatokhoz való kapcsolódások is megjeleníthetők, egészen új szintre emelve az egymással való kapcsolatok feltárását. A Maltego-ban nem csupán saját fejlesztésű, hanem külső alkalmazások is rendelkezésre állnak, illetve a rendszer különböző harmadik féltől származó adatforrásokkal is összeköthető.

A jövő adatvédelmi kihívásai az okos városok és hálózatok tükrében

Az egyre gyorsabb kommunikációs hálózatok – vezetékes és vezeték nélküli - elterjedésével az ún „smart city - smart grid" is egyre inkább elterjedőben vannak, hiszen ezek teszik lehetővé az okos városok kialakulását.
Az okos rendszerek alapvető eleme az okos mérők, amelyek új adatgyűjtési pontként üzemelve újabb adatokat gyűjtenek a felhasználókról és alapvetően az alábbi funkciókkal jellemezhetők: [6, 8]

- oda-vissza adatkapcsolat a szolgáltató és a fogyasztó között;
- aa felhasználások folyamatos (de legalább 15 percenként) meghatározása;
- a helyi hálózat beépítése a kommunikációs kapcsolatba (HAN: Home Appliance Network) ;
- az energiafelhasználás mennyiségi és minőségi jellemzőinek detektálása;

- az adatkapcsolat minőségi jellemzőinek és biztonságának fenntartása.

Az okos fogyasztásmérők alkalmazásával lehetőség nyílik a korábbi eszközök hiányosságainak pótlására: vagyis a pontatlanság, manipulációra való alkalmasság, a távoli hozzáférés hiánya mind-mind elkerülhetővé válnak. Az okos fogyasztásmérők a korszerű infrastruktúrából adódó előnyöket is képesek kihasználni és az alábbi főbb részekből állnak:[6, 8]

- adatkapcsolati részek (interfészek),
- felhasználó oldali kijelző és vezérlő,
- alkalmazások (user-kiszolgáló részek, adatfeldolgozás, user profilok),
- mérések adatainak gyűjtése és az üzleti terület felé történő feladása.

Az okos hálózatok olyan adatok és információk gyűjtését teszik lehetővé, amelyekkel a fogyasztók egészen más dimenzióba tartozó adatai (energiafelhasználási szokások, otthoni jelenlét stb.) válnak elérhetővé és gyűjthetővé.
Az okos hálózatok alkalmazásával begyűjtésre kerülő adatok és az azokra épülő adatbázisok védelme ezek fényében a jövő kiemelt feladata lesz.

A 3. fejezetben bemutatott profilalkotásra szolgáló felhasználó és kiszolgáló oldali alkalmazások és eszközök bemutatása a 5. táblázatban látható.

S.Sz.	Név	Típus	Mire szolgál	Megjegyzés
1	http fejléc a kliens oldalon és azok különféle paraméterei, illetve azok kombinációja	Szükséges elem	Beállítások, beazonosítás	A különböző paraméterek lehetővé teszik a profilozást
2	DNT	Szükséges elem	Ne kövessenek kapcsoló	Elméletileg a nyomon követés kikapcsolására szolgál, azonban számos esetben ez a paraméter nem kerül figyelembevételre
3	Cookie	Beépített plusz elem	Információ gyűjtés, fogyasztói szokások rögzítése	Felhasználói jellemzők mérésére létrejött eszköz

4	http munkamenet	Szükséges elem	User azonosítás, paraméterek kezelésén keresztül	Kiszolgáló és felhasználó oldali adattárolások révén van lehetőség profilalkotásra
5	HTML5	Szükséges elem	User azonosítás, paraméterek kezelésén keresztül	Kiszolgáló és felhasználó oldali adattárolások révén van lehetőség profilalkotásra
6	FLoC	Új külső elem	Információ gyűjtés, fogyasztói szokások rögzítése	Homogén csoportok létrehozásán keresztüli profilalkotásra alkalmas eszköz
7	Facebook pixel	Új külső elem	Információ gyűjtés, fogyasztói szokások rögzítése	Hirdetési elérés és hatékonyság mérése válik ezzel lehetővé
8	TweetPsych	Külső eszköz	Profil alkotás a Twitter bejegyzések alapján	Twitter fiók bejegyzései alapján személyiségjegyek elemzése alkalmas eszköz
9	Rep'nUp	Külső eszköz	SWOT elemzés a személyiségjegyek alapján	Többféle felhasználói fiók adatai alapján személyiségjegyek megállapítására alkalmas eszköz
10	Apple Magic Sauce	Külső eszköz	Profil alkotás	Többféle felhasználói fiók adatai alapján személyiségjegyek megállapítására alkalmas eszköz
11	Data Selfie	Külső eszköz	Profil alkotás	Chrome és Firefox külön bővítmény, a Facebook tevékenység adatait elemzi, azokból von le következtetéseket
12	Maltego	OSINT keretrendszer külső bővítményekkel	Vizualizáció, kapcsolatok feltárása	Publikus adatbázisok alapján kapcsolatok feltárása

5 táblázat Profiling tools

4 A GDPR, MINT SZABÁLYOZÁS ÉS A USER-PROFILING MINT TEVÉKENYSÉG ALKALMAZÁSÁBÓL ADÓDÓ ÖSSZEFÜGGÉSEK KOMPLEX VIZSGÁLATA WEBÁRUHÁZBAN TÖRTÉNŐ VÁSÁRLÁS ÉS INTERNETES BÖNGÉSZÉS VALAMINT ALVÁLLALKOZÓI SZERZŐDÉS PÉLDÁJÁN

A 4. fejezetben egyedi eseteken keresztül bemutatásra kerülnek a személyes adatok gyűjtéséhez és kezeléséhez kapcsolódó gyakorlati példák, illetve számos esetben az azok kezelésére szolgáló lehetőségek is.

4.1 Profilozás és adatvédelem online vásárlás során

Webáruház

Az első esettanulmány egy online áruházban végzett rendelésen alapul, ahol az áruház adatkezelési szabályzata az 1. mellékletben található.
Az áruház bőrből, kézzel készített termékeket értékesít, az áruház honlapjának címe: www.boreger.hu.
Az online áruház közel 35-féle süti alkalmazásával igyekszik a felhasználói élményt fokozni , egyben kiszolgálja a Google Analitics és a Facebook alkalmazásához szükséges bemenő adatok körét. Azáruház sütikre vonatkozó tájékoztatója megadta, hogy melyik süti mennyi ideig érvényes, illetve a tájékoztató arra is felhívta a figyelmet, hogy bizonyos sütik el nem fogadása esetén az áruház miért nem fog működni.
Az online áruház szabályzatában a legfontosabb rész a szerződés létrejötte és a fizikai teljesítés érdekében kezelt adatokról adott tájékoztató.
Az adatkezelés a webáruház és a vásárló magánszemélyek (vagy cégek) között az alábbi esetekben jön létre:

- Kapcsolat kialakítása,
- Online bejelentkezés,
- Rendelés feladás,
- Számlázás,
- Áruszállítás adatainak kezelése,
- Áruszállítás adatkezelésének adatfeldolgozói,
- Szavatossághoz kapcsolódó adatkezelés,
- Fogyasztóvédelmi adatkezelés,
- Kezelt adatokhoz való hozzájárulás,

A fizikai teljesítés a szerződéskötéssel (rendelés) és a kiszállítással, valamint adott esetben a panaszkezeléssel befejeződik.
A webáruház az alábbi célok megjelölése mellett hivatkozik az adatkezelés szükségességére:

- Hírlevelek küldése,
- Személyre szabott reklámok,

- Remarketing,
- Nyereményjáték,
- Nem definiált további adatkezelések,

Az adatkezelés marketing célokra történő felhasználása a személyre szóló reklámokra, remarketingre, hírlevelekre terjed ki.
A gyűjtött személyes adatokkal az alábbi adatkezelők kerülnek kapcsolatba:

- Tárhely szolgáltató: adattárolásra jogosult, megismerésre nem.
- Hírlevél küldő: személyes adatként a vevők nevét, címét kezeli a hírlevél küldéshez.
- Könyvelő: a számviteli bizonylatok elkészítése miatt a vevők nevét, címét kezeli a szükséges mértékben, a Sztv. 169. § (2) bekezdésének megfelelő időtartam, után azokat törli.
- CRM működtető: a megrendelés nyilvántartásán keresztül a vevők nevét, címét kezeli, melyet adott idő után ugyancsak töröl.

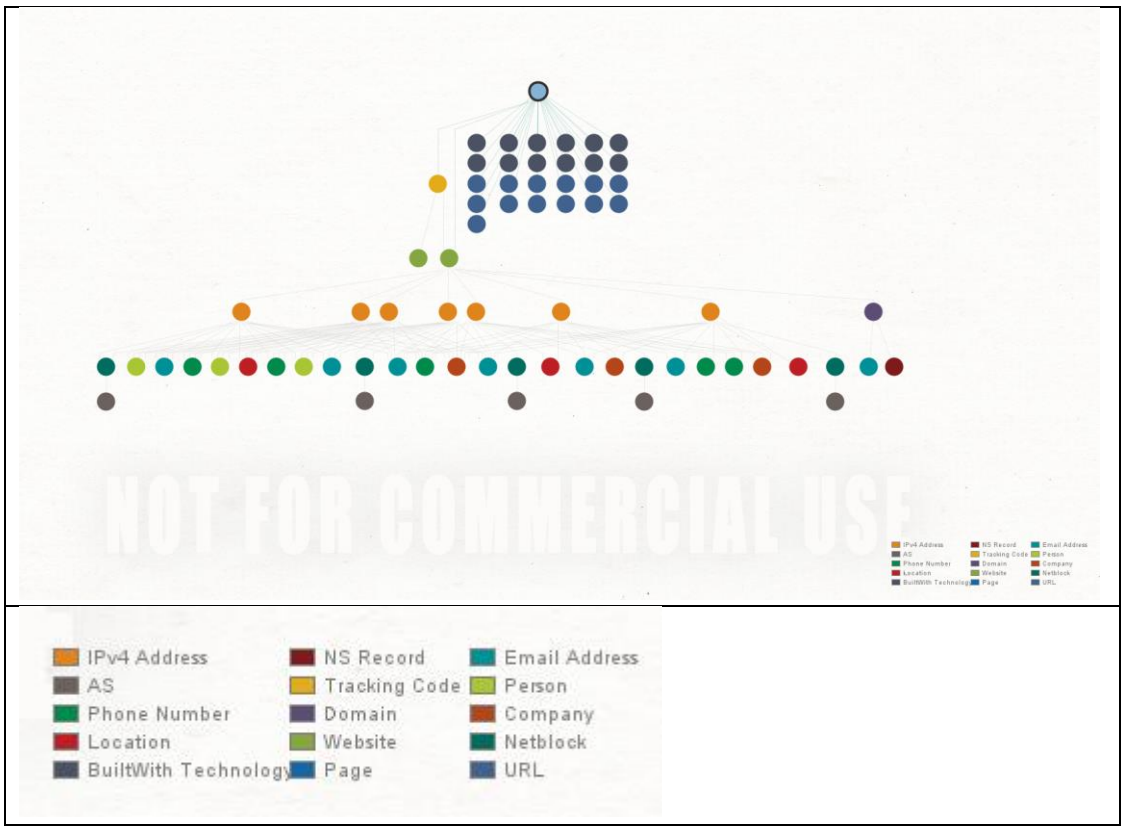
A személyes adatok kezelőinek körébe tartozik még egy EU-n kívüli adatfeldolgozó, aki azonban az Adatvédelmi Pajzs Egyezmény (Privacy Shild List) részese, így kerül biztosításra, hogy az Európai Unióban érvényes garanciák mellett történik az adatkezelés.
A honlapon lévő tájékoztató kellően közérthető formában mutatta be a vásárlói jogokat.
A fentiek alapján az online áruház jól szabályozott tevékenységet mutat, a vásárlók adatai megfelelően kezeltek, maguk a vásárlók pedig megfelelően tájékoztatva vannak.

Online keresés

Online keresés vizsgálata kapcsán az index.hu portál 2017-es tárolt változatát (www.web.archive.org) és a 2022-es aktuális változatát hasonlítottam össze tartalom és kapcsolódások tekintetében. A Maltego 4.3. CE edition segítségével az alábbi adatok közötti összefüggések lettek megvizsgálva:

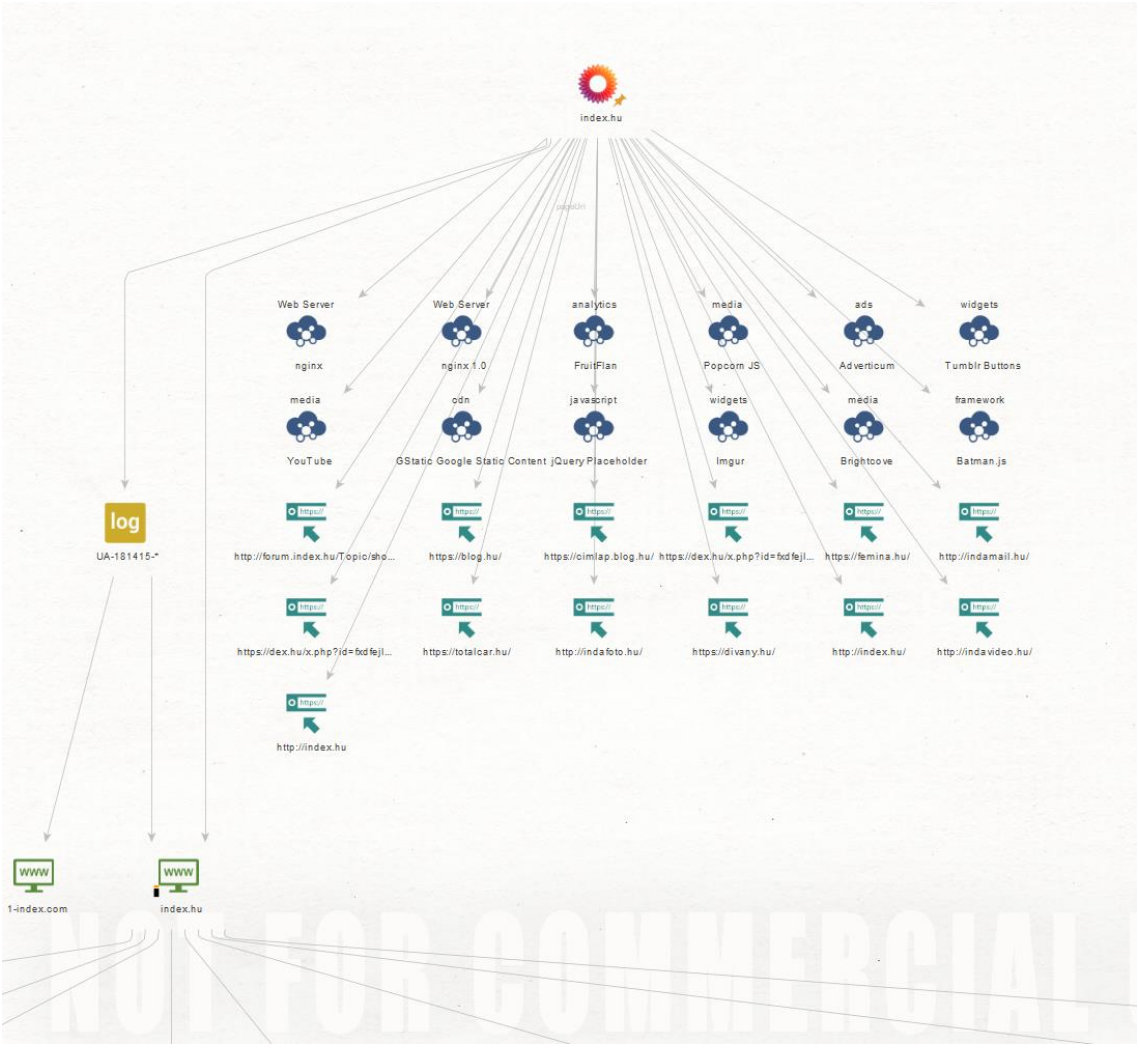
- IPv4 címek,
- AS (Autonomous Systems)
- Telefonszámok
- Hely adatok
- Személyek
- Milyen technológiával készült (BuiltWith Technology)
- Tracking Code (Google Analytics ID),
- Domain,
- Website
- Honlapok (al-honlapok),
- e-mail címek
- Cégnevek,
- Netblock,
- URL,

A megjelenítésre példa az alábbi ábrán látható:



5. ábra Az index.hu-n végzett Maltego lekérdezés kategóriái (saját mentés)

A CE változat korlátja, hogy nem lehet közvetlen domain lekérdezést indítani, csak wiki-oldalként lehetett az index-hu-t megvizsgálni.



6. ábra Az index.hu adatvizualizációja: URL, BuiltWith Technology, Tracking Code, Website kapcsolatai (saját mentés Maltego-ból)

A tracking code értéke: UA-181415-*, ez a 2022-es mentésben és a 2017-es változat esetén is azonos, ahogy alábbi kódokból is látható (lapok lényeges részének mentései a 2. és a 3. mellékletben találhatók).

```
}
ga( 'create', ga_base_config );
ga( 'require', 'displayfeatures' );
ga( 'set', ga_set_config );
    Common.ga_secondary = true;
    var ga_secondary_config = $.extend( {}, ga_base_config
    ga_secondary_config.name = 'secondary';
    ga_secondary_config.trackingId = 'UA-181415-11';
    ga_secondary_config.sampleRate = 10;
    ga( 'create', ga_secondary_config );
    ga( 'secondary.require', 'displayfeatures' );
    ga( 'secondary.set', ga_set_config );
// cross_site ajanlo kivetelkezelese
```

index.hu (2017-es mentés)

```
ga( 'create', ga_base_config );
ga( 'require', 'displayfeatures' );
ga( 'set', ga_set_config );
    Common.ga_secondary = true;
    var ga_secondary_config = $.extend( {}, ga_base_config
    ga_secondary_config.name = 'secondary';
    ga_secondary_config.trackingId = 'UA-181415-11';
    ga_secondary_config.sampleRate = 10;
    ga( 'create', ga_secondary_config );
    ga( 'secondary.require', 'displayfeatures' );
    ga( 'secondary.set', ga_set_config );
ga('set', 'anonymizeIp', true);
// cross_site ajanlo kivetelkezelese
```

index.hu (2022-es mentés)

7. ábra A mentések trackingID-jai (saját mentés)

Az alábbi kód a Facebook login API meghívását mutatja a két különböző mentés esetén, egyértelmű különbség a verziószámokban lelhető fel, az appID azonos mindkét esetben.

```
    //--><![]>
    </script>
        <script type="text/javascript">
            Common.folder_id = 261;
            Common.folder_parent_ids = [  ];
        </script>
    <script>
        window.fbAsyncInit = function() {
            FB.init({
                appId      : '330827937019153',
                xfbml      : true,
                status     : false, // nem kerdezzuk le a login statust, ritkan
van ra szukseg
                version    : 'v2.0'
            });
            window.fb_initialized = true; // beallitjuk, mert ha valami gixer
miatt nem futott le (pl. adblock, akkor ne is probalkozzunk)
```

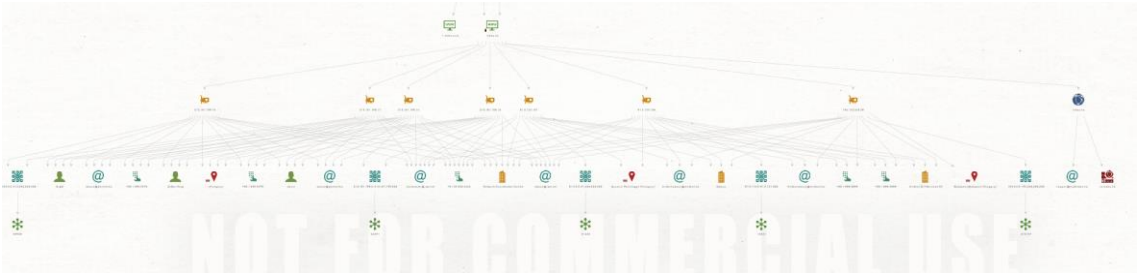
index.hu (2017-es saját mentés)

```
    </script>
    <script type="text/javascript">
        Common.folder_id = 261;
        Common.folder_parent_ids = [  ];
        Common.is_new_design = 1;
    </script>
<script>
    window.fbAsyncInit = function() {
        FB.init({
            appId      : '330827937019153',
            xfbml      : true,
            status     : false,
            version    : 'v5.0'
        });
        window.fb_initialized = true;
    };
```

index.hu (2022-es saját mentés)

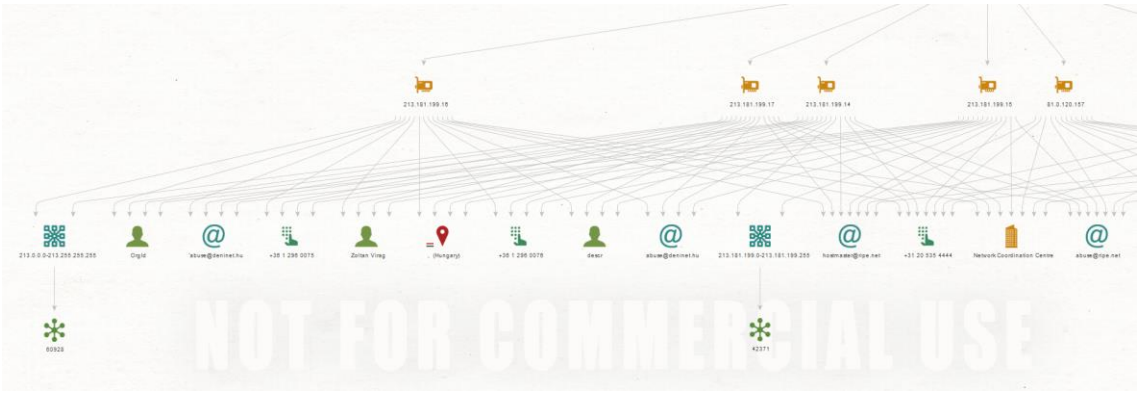
8. ábra FaceBook login API a két pillanatfelvétel esetén (saját mentés)

Az index.hu Maltego vizsgálata során az adatvizualizáció és a beépülő modulok segítségével a 9., 10., és 11. ábrán látható alábbi adatok váltak kinyerhetővé: IPv4 címek, helyadatok, magánszemélyek nevei, telefonszámaik.

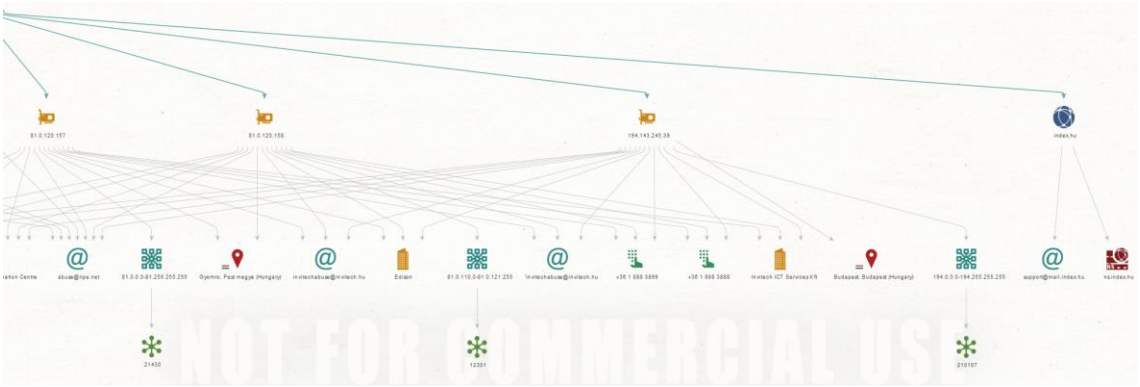


9. ábra Az index.hu kinyerhető információi

A 9. ábra bal oldal és a jobb oldal nagyításából látható, hogy az index-hu oldal igazából 4 db egymás utáni, utána szintén 2 db egymást követő és végül egy harmadik tartományba eső IP címekkel jellemezhető.

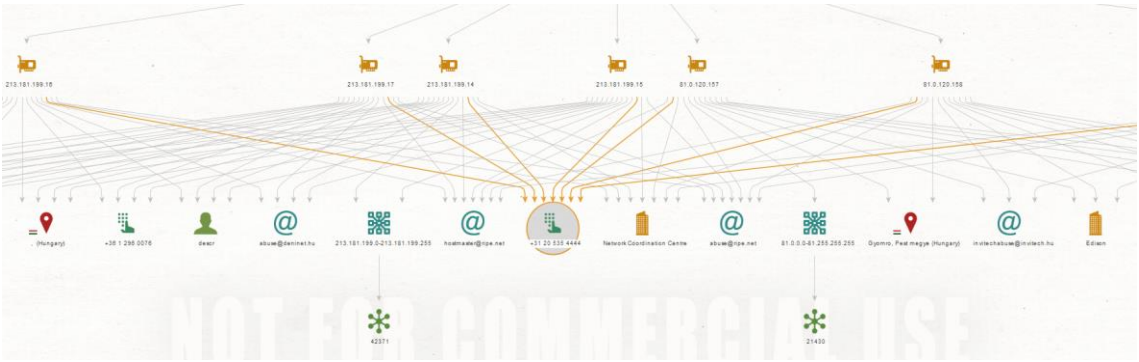


10. ábra A 9. ábra bal oldal (saját mentés)



11. ábra A 9. ábra jobb oldal (saját mentés)

A feltárt +31 20 … kezdetű, mobilszám volt megadva valamennyi IPv4 cím elérhetőségének (12. ábra).



12. ábra A feltárt telefonszám IPv4 címekhez rendelve (saját mentés)

A Maltego jól alkalmazható olyan információk kinyerésére, amelyek segítségével további keresések vagy akár célzott támadások is végrehajthatók.

4.2 Alvállalkozói szerződés GDPR konformitásának ellenőrzése és értékelése

A vizsgált szerződés Nagy Máté (Megbízott/Adatfeldolgozó) és a Certop Kft. (Megbízó/Adatkezelő) között már több mint 6 éve meglévő szerződés újrakötése. Az újrakötés a GDPR szerződésbe foglalása és az aktuális díjszabás változása miatt volt időszerű, ugyanakkor mindkettő ennél sokkal egyszerűbben is módosítható lett volna.
A vizsgálat tárgya a szerződés 7. fejezete, amely az adatvédelemmel foglalkozik. A dolgozat 4. mellékleteként a szerződés kivonata becsatolásra került.
A vizsgált dokumentum 7. fejezete Megbízót (Certop Kft.) Adatkezelőként, Megbízottat (Nagy Máté) pedig Adatfeldolgozóként határozza meg. Ez egybevág a GDPR 4. cikk 7. pontjában lévő fogalmakkal. A szerződés némileg pongyola, ugyanis a GDPR 4. cikke igazából csak magát a definíciókat foglalja össze, ebben a részben a 7. pont az adatkezelő, a 8. pont pedig az adatfeldolgozó meghatározását adja meg.
Megbízó (Certop Kft.), a felügyelő hatóság (NAH: Nemzeti Akkreditáló Hatóság: https://nah.gov.hu/hu/ , amelynek az adatkezelési tájékoztatója a 7. mellékletben került csatolásra) elvárásainak biztosításához a Megbízott bizonyos személyes adatait is fel kell hogy használja (iskolai végzettségek, szakmai tapasztalat, szakmai önéletrajz, felsőfokú és szakirányú diploma fénymásolatok, lakcím adatok, telefonszám, stb.). Adatfeldolgozó személyes adatait ezután Megbízó kezeli belső rendszerében, amelyről a szerződés további információval nem rendelkezik (csak annyit, hogy megfelel a hatályos adatkezelési előírásoknak). Adatfeldolgozó kompetenciái és személyes adatai összerendelésre kerülnek (bizonyítékként), így kerülnek a igazolásra az ún. IAF kódoknak való megfelelőségek a NAH felé.
Adatfeldolgozó személyes adatai tárolásának körülményeiről azonban nem ír továbbit a szerződés sem a főszöveg, sem a mellékletek szintjén, ezt mindenképpen kezelni kell az aláírás előtt.
A 7. fejezet fontos része az adatkezelő kötelezettségeinek definiálása:

- Megbízott a 3. számú mellékletben felsorolt adatfeldolgozási tevékenységeket végzi és az abban megadott személyes adatokat köteles kezelni ennek kapcsán.
- Megbízott a kapott személyes adatokat csak és kizárólag a megadott feladatainak ellátásához kezelheti és a feladatok ellátása után köteles visszaadni Megbízónak, majd megsemmisíteni a nála lévő példányt. Megbízott köteles figyelembe venni Megbízó utasításait.

Az első feltétel nem megfelelően t a 3. mellékletre hivatkozik, a helyes hivatkozás a 2. mellékletre kellene, hogy mutasson.

A szerződés 2. melléklete felsorolja az elvégzendő adatfeldolgozások körét, amelynek adatfeldolgozói szempontú értékelését a 6. táblázat tartalmazza:

S.Sz.	*Szerződés adatfeldolgozói tevékenységének leírása*	*Adott feltétel értékelése adatfeldolgozói szempontból*
1	„A Megbízó/Adatkezelő ügyfelei által működtetett irányítási rendszerek Megbízó/Adatkezelő nevében elvégzett auditálása és annak dokumentálása alábbiak szerint: - A tanúsítás során kapcsolattartás az Adatkezelő munkavállalóival és az Adatkezelő felügyelete alatt dolgozó auditorokkal, ügyfeleivel. - A megismert nyilvántartások, szabályzatok, belső utasítások kezelése. Az irányítási rendszerek kezdeti/megújító/felügyeleti/rendkívüli auditjainak végrehajtása, dokumentálása és a kapcsolódó objektív bizonyítékok gyűjtése és kezelése.”	A melléklet nem teljeskörűen sorolja fel az érintett személyek körét. Vélhetően a Megbízó saját adatkezelési szabályzatából maradtak az anyagban helytelen meghatározások. Az auditok végrehajtása során *számos esetben különleges személyes adattal (egészségügyi adatok, munkabaleseti jegyzőkönyvek) is kapcsolatba kerülnek az adatfeldolgozók. Ezek szabályozása teljesen hiányzik az anyagból*.
2	„Az adatfeldolgozás céljai: Auditok megszervezése, dokumentálása és lebonyolítása.”	Nem pontos a megfogalmazás a szerződésben: az audit célja nem egyértelmű. *Az adatfeldolgozó nem szervez auditot, hanem a követelmények teljesülését ellenőrzi objektív bizonyítékok alapján.* Valószínűleg a Megbízó saját fel-

		adatai kerültek hibásan feltűntetésre a szerződés ezen pontjában.
3	„Az adatok érintettjei: Az Adatkezelő munkavállalói, auditorai, ügyfelei.”	Hiányos a felsorolás: a hatósági felek is az érintettekhez tartoznak.
4	„Adatok kategóriái: Kapcsolattartási adatok: név, email, cím, telefonszám, beosztás, üzenetek, e-mailek, az elektronikus rendszerekben tárolt dokumentumok adatok. Az Adatkezelő által a munkavállalóiról, ügyfelekről nyilvántartott adatok.”	Megfelelő.
5	„Adatok különleges kategóriái: Az adatkezelés során az Adatfeldolgozó nem kezeli az érintettek különleges a GDPR rendelet 9 és 10 cikkében meghatározott kategóriába eső adatait.”	A melléklet kifejezetten az ellenkezőjéről nyilatkozik, ugyanis az ISO 45001 auditok keretében különleges személyes adatokkal is találkoznak az adatfeldolgozók, a legtöbb esetben ezeket azonban igyekeznek anonimizálva kezelni. A büntetőjogi felelősség megállapításához kapcsolódó auditbizonyítékok köre is hasonló kategóriába esik, hiszen az adatfeldolgozók ezen joghatással járó bizonyítékokba is be kell hogy tekintsenek.
6	„Az adatfeldolgozási tevékenységek helyszíne: Az Adatkezelő telephelye és informatikai rendszere.”	A megfogalmazás nem megfelelő: a helyszíni ellenőrzések során az Ügyfelek telephelyein történik az adatfeldolgozási tevékenység. *A szabályozás ezen helyszínekre nem terjed ki*.
7	„Az Adatkezelő és az Adatfeldolgozó Adatvédelmi Tisztviselőjének (ha van) vagy Adatvédelmi kapcsolattartójának kapcsolatfelvételi információi:”	Túl általános megfogalmazás: egyszemélyes vállalkozás esetén nincs külön adatvédelmi tisztviselő.

6 táblázat A szerződés 2. melléklete: Az adatfeldolgozó elvárt feladatai

A szerződés 3. számú melléklete arra vonatkozóan is fogalmaz meg előírást, hogy amennyiben adatfeldolgozó több munkatárssal dolgozik, akkor külön beléptető rendszert kell kiépítenie és üzemeltetnie azon munkatársak ellenőrzésére, akik ezen adatokhoz hozzáférhetnek.
Az alábbi 7. táblázat sorolja fel és értékeli mindazon általános szabályokat és elvárt műszaki intézkedések körét, amelyek a beléptető rendszerrel és/vagy személyes adatok védelmével kapcsolatban elvárások adatkezelő részéről.

S.Sz.	*Szerződésben elvárt intézkedés leírása*	*Elvárt intézkedés értékelése adatfeldolgozói szempontból*
1	„Az informatikai rendszerekhez való hozzáféréshez hitelesítéssel és engedélyezéssel; pl. Bitlocker vagy VeraCrypt alkalmazása a merevlemez titkosítására, vagy külön Certop felhasználó létrehozásával”	Abban az esetben, ha az Adatfeldolgozó harmadik fél részére is dolgozik ugyanazon az eszközön, akkor ez nehezen kivitelezhető. *Az Adatfeldolgozótól származó adatok titkosított külön adathordozón történő tárolása a megoldás.*
2	„Erős jelszavak az informatikai rendszerhez való hozzáféréshez; pl. min. a jelszó 8 karakter, kisbetű, nagybetű, szám és speciális karakter kombinációja.”	Nagyobb rendszerekben ez már alap, a felhasználók többsége ugyanakkor még mindig sérülékeny ilyen téren.
3	„Megfelelő eljárások a személyes adatokhoz való hozzáférési jogok megadásának, rendszeres felülvizsgálatának (pl. szerepenként, objektumonként) és visszavonásának ellenőrzéséhez. Adatfeldolgozó megakadályozza jogosulatlan személyek belépését a személyes adatok kezelésének helyére, illetve megtagadja ennek a helynek a jogosulatlan használatát. Ennek keretében kizárólag a személyes adatok feldolgozására jogosult, meghatalmazott személyek részére biztosít belépési lehetőséget a rendszerébe”	Egyszemélyes cég esetén a feltétel egyszerűen teljesíthető. Alkalmazottakat is tartalmazó többszemélyes cég esetén a hozzáférésvezérlést központi Access Control rendszeren keresztül javasolt megoldani.
4	„Adatfeldolgozó által üzemeltetett informatikai rendszerekben tárolt és kezelt adatok bizalmassága, sértetlensége és rendelkezésre állásának fenntartása érdekében a felmért kockázatokkal arányos szervezési, technikai és logikai védelmet valósított meg”	A megfogalmazás pontatlan: amennyiben csak a szerződés hatálya alá tartozó adatokat értjük bele, akkor a feltétel egy titkosított külső adathordozó alkalmazásával teljesíthető. Amennyiben

		azonban kiterjedt rendszert üzemeltet az Adatfeldolgozó, ahol tárolást is megvalósít, akkor sokkal összetettebb hozzáférés-vezérlést kell megvalósítani.
5	„Naprakész adatbázisú vírusvédelmi rendszert üzemeltet az informatikai rendszerén”	A piacon különféle árkategóriákban, különböző szintű védelmeket biztosító vírus és kártevővédelmi megoldások elérhetők.
6	„Az informatikai rendszeren behatolás elleni védelmi megoldását alkalmaz (tűzfalat üzemeltet)”	A megoldást az jelenti, ha a Win10 beépített tűzfal szolgáltatását használjuk.
7	„Az informatikai rendszerben tárolt és kezelt adatokról adatmentést végez. A mentett adatokról rendszeres adatvisszaállítási tesztet hajt végre”	Az adatmentés esetén fontos a redundancia és a diverzitás elvének érvényesítése. *Az adatmentés követelménye részben ellent mond a Megbízott kötelezettségei részben lévő 6. pontnak.*
8	„Adatfeldolgozó a rendszerben kizárólag olyan szoftvereket használ, amelyek megfelelnek a reájuk vonatkozó szerződésbéli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak; a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek használatát”	Ez a feltétel jogtiszta alkalmazások használatával teljesíthető.

7 táblázat A szerződés 3. melléklete: Elvárt műszaki intézkedések az adatfeldolgozó részéről

A szerződés 3. melléklet második része az Információ Biztonsági (IB) felülvizsgálatra tér ki, ahol deklarálásra került, hogy Megbízott vállalja, hogy Megbízó IT rendszerének üzemeltetőjének igény esetén hozzáférést biztosít ellenőrzés céljára. Az ellenőrzés a vírusvédelemre, a számítógépek integritásának ellenőrzésére irányul, amely adott esetben jelentős többlet terhet jelenthet egy többfelé dolgozó cég számára, hiába az egy hónappal korábbi bejelentés és az egyeztetett időpont.
A feltételek legegyszerűbben kivitelezhető teljesítése vélhetően egy Adatfeldolgozói célra elkülönített számítógép alkalmazása.

Az adatvédelmi előírások meghatározása után a szerződés az adatkezelő (Megbízó) utasításairól értekezik, amelynél minden esetben fontos az írásbeliség, vagyis csak írásban utasíthatja Megbízó a Megbízottat.

Az adatfeldolgozó szerződésben elvárt kötelezettségeit a 8. táblázat tartalmazza, amely az alább nyolc feltételt szabja meg:

S.Sz.	*A szerződés adatfeldolgozóra vonatkozó kötelezettségének leírása*	*Adott feltétel értékelése adatfeldolgozói oldalról*
1	„Az Adatfeldolgozó számára a személyes adatok kezelése, feldolgozása kizárólag az Adatkezelő írásbeli utasításaival összhangban és a megállapított célokból (3. melléklet) engedélyezett. Az Adatkezelő kérése alapján köteles a személyes adatokat javítani, törölni stb. Személyes adatokról az Adatkezelő tudomása nélkül semmilyen másolat nem készülhet.”	*Az adatkezelési célok nem a 3. mellékletben, hanem a 2. mellékletben vannak.*
2	„Az Adatfeldolgozó köteles az adatkezelés során a 4. mellékletben részletezett, megfelelő műszaki és szervezeti intézkedéseket megvalósítani és betartani a GDPR 32. cikke értelmében, annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. Az Adatfeldolgozó kifejezetten úgy állítja fel szervezetét, hogy az megfeleljen az adatvédelmet érintő követelményeknek, és ezeket a követelményeket dokumentálja. Ide tartoznak a kockázati szinthez megfelelő biztonsági szint biztosításához szükséges műszaki és szervezeti intézkedések, ideértve legalább az alábbiakat, amennyiben lehetséges: - Személyes adatok álnevesítése és titkosítása; - Képesség a feldolgozó (IT) rendszerek és szolgáltatások folyamatos bizalmas jellegének, integritásának, rendelkezésre állásának és ellenálló képességének biztosítására; - Képesség a személyes adatok elérhetőségének és az azokhoz való hozzáférésnek időben történő visszaállítására fizikai vagy műszaki incidens esetén;	Mivel a szerződés nem tartalmazott 4. fejezetet az a feltételezés, hogy ennek elkészítése a Megbízott feladata lenne, amely aránytalan az elvégzendő feladat méreteihez képest.

	- Eljárás a feldolgozás biztonságának biztosítására szolgáló műszaki és szervezeti intézkedések hatékonyságának és megfelelőségének rendszeres teszteléséhez, felméréséhez és értékeléséhez. Az Adatfeldolgozó köteles a fenti eljárást fenntartani és rendszeresen frissíteni, valamint a frissítésekről értesíteni az Adatkezelőt. Az Adatfeldolgozó műszaki és szervezeti intézkedéseinek konkrét leírása a 4. számú Mellékletben található."	
3	„Az Adatfeldolgozó köteles gondoskodni arról, hogy a személyes adatok feldolgozásával foglalkozó minden alkalmazottját gondosan válassza ki, titoktartási kötelezettséget vállaljanak (vagy álljanak megfelelő jogszabályi titoktartási kötelezettség alatt) és ismerjék meg a vonatkozó adatvédelmi törvények rendelkezéseit."	Egyszemélyes vállalkozás esetén a titoktartás személyes feladat és felelősség.
4	„Az Adatfeldolgozó megadja az Adatkezelő részére az adatvédelmi tisztviselője („DPO") kapcsolatfelvételi adatait, ha az Adatfeldolgozó köteles DPO-t kinevezni, illetve ennek hiányában az adatvédelmi kapcsolattartó személy kapcsolatfelvételi adatait. Az Adatfeldolgozó köteles azonnal és kérés nélkül értesíteni az Adatfeldolgozót a fenti tisztviselők személyében bekövetkezett változásokról. Az Adatfeldolgozó köteles tudomásszerzést követően szükségtelen késedelem nélkül, haladéktalanul értesíteni az Adatkezelőt minden gyanított adatvédelmi incidensről, személyes adatok feltöréséről, illetve minden egyéb rendellenességről a személyes adatok feldolgozásával kapcsolatban."	DPO kinevezése egyszemélyes vállalkozás esetén nem kivitelezhető, egyébként a követelmény maga betartható.
5	„Az Adatfeldolgozó köteles a náluk bekövetkezett adatvédelmi incidenst az arról való tudomásszerzését követően indokolatlan késedelem nélkül jelenteni a szerződésben megadott adatvédelmi kapcsolattartónak. A jelentés tartalmának legalább azokat az információkat kell tartalmaznia, amelyek az Adatfeldolgozónak is szükségesek lehetnek az incidens hatásainak megfelelő felméréséhez. Az Adatfeldolgozó köteles	Ez az elvárás szükséges a feladatok teljesítéséhez és arányban van a teljesítés ellenszolgáltatásával.

	segíteni az Adatkezelőt minden kommunikációban a felügyelő hatóságokkal és az érintettekkel, így megfelelő technikai és szervezési intézkedésekkel segíti az Adatkezelőt abban, hogy az érintett GDPR III. fejezetében megfogalmazott jogainak gyakorlásával összefüggő kérelmeket teljesíteni tudja, továbbá segíti az Adatkezelőt a GPPR 32.-36. cikke szerinti kötelezettségeinek teljesítésében.”	
6	„Az Adatfeldolgozó köteles az Adatkezelő által átadott minden adathalmazt és adathordozót, valamint az ezekről készült minden másolatot biztos helyen tárolni és gondoskodni arról, hogy harmadik fél ne férhessen hozzá. Az adatkezelési szolgáltatás (audit) befejezését követően a személyes adatokat tartalmazó adathalmazokat és dokumentumokat vissza kell juttatni az Adatkezelő részére. Az Adatfeldolgozó köteles az adathalmaz másolatait is törölni az adatkezelési szolgáltatás befejezését követően. Az adatok (ideértve másolatokat is) törlését köteles írásban megerősíteni az Adatkezelő felé.”	Ez az elvárás szükséges a feladatok teljesítéséhez és arányban van a teljesítés ellenszolgáltatásával. Adatfeldolgozó a leírás alapján az adatkezelési feladat végeztével köteles átadni a Megbízó felé, majd törölni a feldolgozott adatokat. *Az adatok törlésével a a későbbi visszaellenőrzés lehetősége – amely alapvető jellemzője az auditoknak – elvész.*
7	„Az Adatfeldolgozó köteles az érintetteknek a GDPR és a vonatkozó törvények/jogszabályok alapján fennálló jogaikat érintő és a személyes adataik feldolgozására vonatkozó kérései és követelései esetében az Adatkezelőt támogatni. Az Adatfeldolgozó ebből a célból ezeket a folyamatokat megfelelően dokumentálja és az adatkezelőt értesíti.”	Ez az elvárás szükséges a feladatok teljesítéséhez és arányban van a teljesítés ellenszolgáltatásával.
8	„Az Adatfeldolgozó köteles az Adatkezelő rendelkezésére bocsátani minden olyan információt, amely a GDPR 28. cikkében foglalt kötelezettségek igazolásához szükséges, továbbá köteles lehetővé tenni az Adatkezelő által végzett ellenőrzéseket. Az időben megtett írásbeli értesítés után az Adatkezelőnek rendes munkaidőben jogában áll meggyőződnie az Adatfeldolgozó által a jelen szerződés és a GDPR betartása érdek-	Ez az elvárás szükséges a feladatok teljesítéséhez és arányban van a teljesítés ellenszolgáltatásával.

	ében megtett lépések megfelelőségéről és megvalósításáról, a műszaki és szervezeti követelmények megfelelőségéről.”	

8. táblázat Adatfeldolgozói kötelezettségek

A feltárt ellentmondások és hibák alapján a keretszerződés ebben a formában nem írható alá. A fenti táblázatban jelölt problémákat mindenképpen kezelni kell.
A szerződés talán legkirívóbb hiányossága, hogy amíg a Megbízói oldal részéről a rendkívüli felmondási feltételek tételesen felsorolásra kerülnek (pl. GDPR okokból), addig Megbízotti oldalon rendkívüli felmondásra mindössze a megbízási díj jogosulatlan visszatartása szolgálhat, adatkezelési hiányosságok nem. Anna ismeretében, hogy milyen adatokat kezel a Megbízó és a feltétel aránytalan.
A szerződés a fenti hiányosságok és egyéb üzleti szempontok figyelembevételével nem került újra kötésre, a felsorolt feltételek rendezése az Adatkezelői oldalról nem került megoldásra.

5 EREDMÉNYEK, KONKLÚZIÓ

Az online vásárlás adatkezelési és a felhasználó tájékoztatása szempontból elfogadható eredményt adott. A tájékoztatás kellően érthető és olvasható volt.
Közismert honlap Maltego-val történő elemzése feltárt olyan adatokat, amelyek további vizsgálattal egyéb összefüggések feltárására is lehetőséget adnak. A lementett paraméterek alapján a vizsgált honlapok a DNT opció bekapcsolt állapota mellett is gyűjtöttek adatokat a felhasználóról.
A saját szerződésem adatvédelmi elemzése sajnos olyan súlyos hiányosságokat tárt fel, amelyek mellett ebben a formában a szerződés nem írható alá.

6 Összefoglalás

A dolgozat azzal a céllal készült, hogy ismertesse az adatvédelmi szabályozás fejlődésének kialakulását és bemutassa a user profiling eszközök működésén keresztül mindazokat a területeket, ahol a szabályozások kiterjesztésére várhatóan szükség lesz. A dolgozat gyakorlati példákat sorol fel a profilozási technikákra és a meglévő szabályozási feltételek teljesülésére – vagy éppen azok hibájára.

Az első fejezet a szabályozási környezet kialakulásával foglalkozik, feltárva az ok-okozati összefüggéseket. A személyes adatokról szóló törvény és az infotörvény bemutatását a GDPR ismertetése követi.

A második fejezet a GDPR alkalmazásának időszakában fennálló problémákat, példákat ismerteti az alapelvek bemutatása mellett.

A harmadik fejezet azon eszközök ismertetésével foglalkozik, amelyekkel lehetőség nyílik a mindennapok során, hogy a felhasználókról információt tároljanak, vagy kinyerhetővé tegyenek.

A negyedik fejezet személyes példákon keresztül mutatja be mindazon problémákat, amivel bármelyik felhasználó szembesülhet a saját munkavégzése vagy csupán egy egyszerű internetes vásárlás során

Az ötödik fejezet foglalkozik a gyakorlatból származó példák ismertetésével és a következtetések levonásával.

7 SUMMARY

The aim of my thesis is to describe the evolution of data protection regulation and to illustrate, through the operation of user profiling tools, the areas where it is likely that there will be a need for further regulation. The paper will provide practical examples of profiling techniques and of how existing regulatory conditions are met - or not met.
The first chapter deals with the evolution of the regulatory environment, exploring the causal links. The introduction to the Personal Data Act and the Information Act is followed by a description of the GDPR.
The second chapter describes the problems and examples of the period of application of the GDPR, along with the principles.
The third chapter describes the tools that can be used in everyday life to store or retrieve information about users.
The fourth chapter illustrates, through personal examples, the problems that any user may encounter in the course of his or her own work or simply when shopping online.
The fifth chapter is devoted to presenting examples from practice and drawing conclusions.

ÁBRAJEGYZÉK

TÁBLÁZATOK JEGYZÉKE

IRODALOMJEGYZÉK

[1] Ayse Cufoglu: User Profiling-A Short Review. International Journal of Computer Applications (0975 8887), Volume 108 - No. 3, December 2014

[2] Giovanni Ballocca, Roberto Politi, Giancarlo Ruffo, Rossano Schifanella: Integrated Techniques and Tools for Web Mining, User Profiling and Benchmarking analysis. 2003, Proceeding of CMG'03

[3] Gulyás Gábor György: Anonim-e az anonim böngésző? Technológiák és szolgáltatások elemzése. ALMA MATER SOROZAT AZ INFORMÁCIÓ- ÉS TUDÁSFOLYAMATOKRÓL 10.; 2006/1; 9-30. O.

[4] Kiss Attila – Krasznay Csaba: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. Információs Társadalom. XVII. 2017. július.

[5] Kovács Zoltán: WEBES NYOMKÖVETÉSI TRENDEK VIZSGÁLATA. Szakdolgozat. BME VIK. 2016.

[6] Labancz Andrea: AZ ADATVÉDELMI JOG ÉS A SZEMÉLYES ADATOK MÚLTJA, JELENE ÉS JÖVŐJE AZ UNIÓS SZABÁLYOZÁSBAN. Külügyi Műhely 2020/1. szám.

[7] SZERK.: POLYÁK GÁBOR: ALGORITMUSOK, KERESŐK, KÖZÖSSÉGI OLDALAK ÉS A JOG – A FORGALOMIRÁNYÍTÓ SZOLGÁLTATÁSOK SZABÁLYOZÁSA. HVG-ORAC Lap- és Könyvkiadó Kft., 2020.

[8] Sumitkumar Kanoje, Sheetal Girase, Debajyoti Mukhopadhyay: User Profiling Trends, Techniques and Applications, International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 1, Jan 2014.

[9] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. Infotörvény. NetJogtár: https://net.jogtar.hu/jogszabaly?docid=a1100112.tv Hozzáférés: 2021. 05. 18.

[10] Általános adatvédelmi rendelet: https://gdprinfo.eu/hu Hozzáférés: 2021.05.18.

[11] What is FLoC?: https://web.dev/floc/ Hozzáférés: 2021. 05. 18.

[12] https://amifloced.org/ Hozzáférés: 2021. 05. 18.

[13] https://gs.statcounter.com/browser-market-share/desktop/worldwide hozzáférés: 2022.04.27.

[14] Balogh Zoltán: Személyes adatok gyűjtése és profilírozás az interneten, Doktori értekezés, 2017.

[15] Rákos Dóra: A személyes adatok védelme az új európai adatvédelmi rendelet (GDPR) tükrében, NKE, 2019/2.

[16] https://en.wikipedia.org/wiki/Maltego

[17] https://mkogy.jogtar.hu/jogszabaly?docid=99200063.TV

[18] www.web.archive.org

[19] https://iaf.nu/en/about/code-of-conduct/

[20] Electronic Frontier Foundation honlapja: http://panopticlick.eff.org

MELLÉKLETEK

1. melléklet: A www.boreger.hu webáruházban történt vásárlás adatvédelmi szabályzata (Érvényes: 2022.01.01.-től)
2. melléklet: Index.hu 2017.02.10.-i mentése (www.webarchive.org) (Header-footer)
3. melléklet: Index.hu 2022.04.22.-i mentése (Header-footer)
4. melléklet: Certop Kft. és Nagy Máté közötti auditori új keretszerződés – kivonat (7. fejezet: Adatvédelmi rendelkezések, valamint a 2. és a 3. sz. melléklet)
5. melléklet: A Certop Kft. által az új keretszerződéssel együtt megküldött tájékoztató levél
6. melléklet: a Certop Kft. jelenleg érvényes Adatkezelési tájékoztatója
7. melléklet: a NAH adatvédelmi tájékoztatója

RÖVIDÍTÉSEK

AMI: Advanced Measurement Infrastructures

API: Application Programming Interface

AS: Autonomus Systems

Avtv.: Adatvédelmi törvény (1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról)

CRM: Customer Relationship Management: Ügyfélkapcsolati adatok tárolására szolgáló eszköz

CNIL: Commission Nationale de l'Informatique et des Libertés (Francia Adatvédelmi Hatóság)

DNT: Do-Not-Track

DNS: dezoxiribonukleinsav, valamint más kontextusban Domain Name Server

DPO: Data Protection Officer (adatvédelmi tisztviselő)

EFF: Electronic Frontier Foundation

EGT: Európai Gazdasági Térség

EU: Európai Unió

FLoC: Federated Learning of Cohorts

GDPR: General Data Protection Regulation

HAN: Home Appliance Network

HTML: HyperText Markup Language=hiperszöveges jelölőnyelv

IAF: International Accreditation Forum (https://iaf.nu/en/about/code-of-conduct/)

IE: Internet Explorer

iOS: az Apple Inc. mobil operációs rendszere

IP: Internet Protocol

ISO/OSI: International organization of Standardization /Open Systems Interconnection Model

IPv4: Internet Protocol 32 bites címtartomány

IT: Information Technology

MB: Mega Byte

NAH: Nemzeti Akkreditáló Hatóság

NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság

OSINT: Open Source Intelligence (nyílt forrású hírszerzés)

TCP/IP: Transmission Control Protocol/Internet Protocol

URL: Uniform Resource Locator (webcím)

WebSQL: Web Structured Query Language (strukturált lekérdezőnyelv) relációsadatbázis-kezelők lekérdezési nyelve

JOGSZABÁLYOK JEGYZÉKE

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. Infotörvény. NetJogtár: https://net.jogtar.hu/jogszabaly?docid=a1100112.tv Hozzáférés: 2021. 05. 18.

Általános adatvédelmi rendelet: https://gdprinfo.eu/hu Hozzáférés: 2021.05.18.

95/46/EK számú adatvédelmi irányelv

Alkotmány módosításáról szóló 1989. évi XXXI. törvény

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról https://mkogy.jogtar.hu/jogszabaly?docid=99200063.TV Hozzáférés: 2022.04.29.