

1. SZÁMÚ FÜGGELÉK

36. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2023. április 18-20.
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar

Az internetes mélycsomag vizsgálat és a magánszféra kapcsolata

Jelige: EUVEGHAT

Pályamunka lezárásának időpontja: 2022.június

2023.

**Nemzeti Közszerológati Egyetem
Államtudományi és Nemzetközi Tanulmányok Kar
Emberi Erőforrás Tanszék
Közigazgatás-szervező szak
Nemzetközi közigazgatás szakirány**

Az internetes mélycsomag vizsgálat és a magánszféra kapcsolata

A konzulens:

Dr. Bányász Péter, adjunktus

Készítette:

Lakatos Szilárd

**Budapest
2022**

Tartalomjegyzék

Bevezetés	5
Téma aktualitása.....	5
Tudományos probléma megfogalmazása	6
Kutatási célkitűzések.....	6
Hipotézisek.....	7
Kutatási módszertan	7
1. Az internetes mélycsomag vizsgálat	8
1.1 Magánszféra és dimenziói.....	8
1.2 Az internetes mélycsomag vizsgálat	12
1.3 Mélycsomag vizsgálat és az egyén kapcsolata.....	16
Következtetések	21
2. Mélycsomag vizsgálat jogi szabályozása	22
2.1 A magánszféra és a technológia által érintett jogok	22
2.2 Európai Unió és nemzetközi szabályozások	25
2.3 Hazai szakértők véleménye	28
3. Mélycsomag vizsgálat kockázatai	32
3.1 Mélycsomag vizsgálat és az állampolgárok kapcsolata	32
3.2 A fenyegetettség bemutatása	39
3.3 Megoldási lehetőségek	43
Eredmények.....	46
Összefoglalás	46
Hivatkozások.....	47
Táblázatok jegyzéke.....	51
Mellékletek	52
Interjúkérdések:	52
Rövidítések jegyzéke:	55

Bevezetés

Téma aktualitása

2022-ben az általunk használt internet gyakorlatilag már felismerhetetlen 1969-ben létrehozott Apranet¹-hez képest. Laikusokként bele gondolni sem tudunk, hogy az általunk használt alkalmazások hány dologhoz kérnek engedélyt, mekkora biztonsági kockázatot jelentenek és milyen informatikai háttértudáshoz van szükség ahhoz, hogy rájövünk mit is jelent valójában egy kattintásunk, vagy egy levélüzenet-váltásunk az interneten.² Edward Snowden írta le könyvében, hogy „a cégek rájöttek, hogy akik a netre mennek fel, inkább megosztani kívánnak, mintsem költeni, és hogy az emberi kapcsolatokon pénzt lehet keresni.”³ Ezek után már az lett a cél a különböző multinacionális vállalatok számára, hogyan tudják a megszerzett információt személyes haszon céljából felhasználni.

Mindenki elé került már egy olyan vásárlási hirdetés, amely egy olyan árucikkről vagy termékről szólt, amelyről barátaiknak vagy ismerőseiknek chateltek egy közösségi platformon. Ez az algoritmusoknak és az internetes mélycsomag vizsgálat módszerének köszönhető, amely során, adott szavakra, esetleg kifejezésekre keresnek rá a módszer algoritmusai.

Különböző államok, különböző telekommunikációs cégek más-más jogszabályi háttérrel rendelkeznek erről a tevékenységről. Egyes országokban, mint például Venezuelában nincs erre a területre vonatkozó releváns jogszabály, ezzel ellentétben Európai Unióban szigorúbb szabályozások találhatók, amelyek érvényesek a közösséghez csatlakozott tagállamok számára (így Magyarországra is), de kevés országnál figyelhető meg külön jogszabályozási háttér. Amennyiben az amerikai jogszabályozási hátteret nézzük, ott sincs erre vonatkozó normatív joganyag, így hatalmas kapukat hagynak nyitva olyan multinacionális vállalatok számára, mint a Facebook, Google, akik az általunk kinyert adatokat értékesíteni tudják kisebb-nagyobb vállalatok felé, illetve kommunikációnk mélyebb betekintésébe is lehetőség adódik.

Ezek tudatában jogosan merülhet fel a kérdés, hogy a hétköznapi állampolgárok mennyire tartják veszélyesnek a személyre szabott hirdetéseket, avagy mennyire ítélik kockázatosnak a tényt, hogy a mélycsomag vizsgálat használatával több minden is lekövethető róluk.

Ez a vizsgálati módszer azonban olyan lehetőséggel is felruházhatja alkalmazóját, amely által a szükségesebbnél több információt megtudhat az őt érdeklő személyekről. Jogosan merül fel

¹Az internet hazai megjelenése In. Médiatudományi Intézet, 2015. július 17. https://nmhh.hu/cikk/192602/Az_internet_hazai_megjelenese Letöltés dátuma 2022.01.30.

² Puskás Tivadar Közalapítvány: Internet Biztonsági Tanulmány, Az Internet Szerepének Gyors Növekedésében Rejlő Pénzügyi Visszaélésekkel Kapcsolatos Kockázatok, 2009. szeptember, 82 p.

³ Snowden, Edward: Rendszerhiba, 21. Század Kiadó, 2019. szeptember 17., p. 11.

a kérdés, hogy ezen cselekedet megakadályozására egyes országok törvényalkotói mennyire figyeltek, mennyire próbálták elkerülni, avagy mennyire próbálták saját javukra kialakítani a jogszabályalkotások során a technológiában rejlő lehetőségeket.

Emellett felmerül a kérdés, hogy az állampolgárok mennyire ítélik ezeket kockázati tényezőnek, mennyire vannak tisztában a mélycsomag vizsgálat során felmerülő veszélyekkel. A terület egyre jobban érinti a világ társadalmát, hiszen az internet-szolgáltatók törvényes ellenőrzése hatalmas kihívások elé állítja a különböző nemzetek nemzetbiztonsági és rendvédelmi szerveit.

Tudományos probléma megfogalmazása

E biztonsági technológiából eredő elsődleges probléma az internetes szokásaink teljes nyomon követéséből és a technológia rossz célú felhasználásából fakad. Az Európai Unió állampolgáraként is használhatunk olyan internetes oldalakat, mind videómegosztó, mind különböző üzenetküldő, illetve egyéb közösségi médiafelületeket, amelyeket többnyire amerikai cégek szolgáztatnak, így használatuk során adataink mélycsomag vizsgálaton mennek keresztül a szolgáltató államban. Ezeken kívül a WeChat (Kína), TikTok (Kína), QQ (Kína), Telegram (Dubai) is fellelhető a leggyakrabban használt alkalmazások között, amelyek használata során adatcsomagjaink szintén átvizsgáláson eshetnek át.

Felmerülhet a kérdés, hogy az „Öt Szem országai” (Amerikai Egyesült Államok, Nagy-Britannia, Új-Zéland, Ausztrália, Kanada) az így kinyert információkat hogyan és milyen módon osztják meg egymás között.

Egy másik lényeges probléma az állampolgárok biztonságtudatossága. Mivel különböző iskolázottsági szinttel, különböző korról és különböző szemléleti háttérrel rendelkeznek, így mindenki véleménye eltér a „hétköznapi megfigyeléssel” kapcsolatban. Megfigyelhető, hogy különböző államokban, különböző módon alakul az állampolgárok biztonságérzete. Ez köszönhető országok kultúrájának, objektív biztonsági érzetüknek is.⁴

Kutatási célkitűzések

Kutatásom célja, hogy a nemzetközi és hazai szakirodalmak felhasználásával bemutassam, hogy a mélycsomag vizsgálat milyen módon sértheti az állampolgárok magánszféráját. Amíg a technológiával és az algoritmusokkal kinyert információk egy állam percepciójának növelését jelenti, ugyanakkor állampolgárai biztonságérzetének csökkenésével is egyenlő. Ezek

⁴ Dr. Kirstie Ball: Megfigyelés, magánszféra és biztonság – Mi az Ön véleménye? In. Surprise Project, 2014.04. – http://surprise-project.eu/wp-content/uploads/2014/04/B7_Median_Information_Magazine_Hungarian.pdf (Letöltés dátuma 2022.03.08.)

igazolásához nemzetközi és hazai jogi szabályozások elemzését és összehasonlítását is elvégzem, hogy milyen kockázatok állnak fent egyes államokban a magánszférára. Továbbá kérdőív segítségével vizsgálom a magyar állampolgárok biztonságtudatát és az interneten történő kommunikációjuk tudatosságát, amelyek alapját a technológiai befogadást vizsgáló modellek adják.

Hipotézisek

Kutatásom során az alábbi hipotéziseket fogalmaztam meg:

- H1.: Adatvédelmi szakértők és jogászok szerint a hazai és nemzetközi jogi szabályozás hiátusokat tartalmaz a mélycsomag vizsgálatot illetően.
- H2.: Az állampolgárok, a technológia ismerete nélkül is feltételezik, hogy személyes adataikhoz juthat hozzá egy harmadik fél.
- H3.: A mélycsomag vizsgálat magán és vállalati célú felhasználása kiemelt kockázatot jelent a magánszféra megsértésével kapcsolatban.

Kutatási módszertan

Kutatásom során kvantitatív és kvalitatív kutatási módszereket is használtam. Az egyik egy átfogó elemzés, amely során a mélycsomag vizsgálatról szóló hazai és nemzetközi szakirodalmak és folyóiratok segítségével próbálom bemutatni, illetve alátámasztani a felállított hipotéziseim és a választott témaköröm. Ehhez segítségül használtam a primer adatgyűjtési-kutatási módszerek egyik leggyakoribb módszerét is, a kérdőíves felmérést és az interjúkészítést. A kérdőív kitöltését 2020 őszén⁵ egy mindenki számára elérhető felületen történt. Ezen kívül, meglévő statisztikai adatgyűjtést is folytattam, hogy a mások által vizsgált jelenségek és folyamatok által egy átfogóbb jellemzést érjek el dolgozatomban. Hogy a lehető legfrissebb adatokkal dolgozzak, a talált statisztikai adatok az Eurostat és a Statista által kibocsátott statisztikák fognak szolgálni. Dolgozatom további részében jogászokkal és adatvédelmi szakértő(k)kel interjút készítettem, melyben az ő véleményükre, álláspontjukra és megállapításaikra támaszkodok feltételezéseim igazolásához. Végezetül kockázatelemzés segítségével mutatnám be az internetes mélycsomag vizsgálat által fellelhető fenyegetettségeket.

⁵ A dolgozat megalkotása a 2020. évben kezdődött

1. Az internetes mélycsomag vizsgálat

1.1 Magánszféra és dimenziói

A bevezetőben leírtak alapján kiderül, hogy dolgozatomban az internetes mélycsomag vizsgálat és a magánszféra kapcsolatára épül. Ennek értelmében először a két fogalmat járom körbe, hogy nagyobb rálátást nyerjünk külön-külön a fogalmi elemekre, annak érdekében, hogy meg tudjam határozni, mi a kapcsolat közöttük.

A magánszféra fogalmi meghatározására több kísérlet történt. Egy értelmező kéziszótárt vagy egy szaklexikont kinyitva könnyen megtalálhatnánk mit is jelent. Azonban több tudós és szakértő is megfogalmazta már azzal kapcsolatban véleményét, mely szerint a magánszféra fogalmi meghatározása erősen függ attól a kontextustól, amelyben éppen használni kívánjuk⁶. David Lindsay például egyfajta jószágként értelmezi a magánszférát, amely össze tud fonódni a személyiséggel, a szabadsággal és a méltósággal. Másik megközelítésből vizsgálva, Warren és Brandeis a magánszférát az „egyedül hagyáshoz való jog”-gal azonosítják, ami alatt azt értik, hogy az egyének a nem kívánatos külső (mind társadalmi, mind állami szinten) hatásokat távol tartsák maguktól, velük szemben jogorvoslati lehetőséggel rendelkezessenek.

Solove, 2008-ban fogalmazta meg, hogy a magánszféra tisztázatlan fogalom. Egyszerre tartalmazza a vélemény szabadságot, a test feletti rendelkezés jogát, az otthon háborítatlanságát, a megfigyeléstől való menetességet, a jó hírnév védelmét, a kihallgatásokkal és a házkutatásokkal szembeni védelmet és a személyes adatok feletti védelmet⁷.

E fogalmi meghatározás is megmutatja, hogy mennyire sokrétű szó a magánszféra. A fentiek alapján a következőkben a magánszféra dimenzióinak meghatározására fókuszálok, azaz arra, hogyan és milyen módon lehet „halmazokba” sorolni ezt a sokrétű fogalmat.

A szakterület képviselői különböző csoportokba osztják fel a magánszférát, az idő előre haladtával kiegészítik újabb csoportosítási módszerekkel. A magánszféra gondolatának legnagyobb megújítása Roger Clarke nevéhez kötődik. Clarke négy kategóriába sorolta fel a magánszféra típusait:

- a személyes adatok magánszférája,
- a személyes viselkedés magánszférája,
- a személy magánszférája és
- a személyes kommunikáció magánszférája.

Ezt egészített ki a későbbiekben a személyes tapasztalatok magánszférájával.

⁶ Finn, el. al. : Seven Types of Privacy . In European Data Protection. Coming of Age? New York – London, 2012.10.12., pp. 3-32.

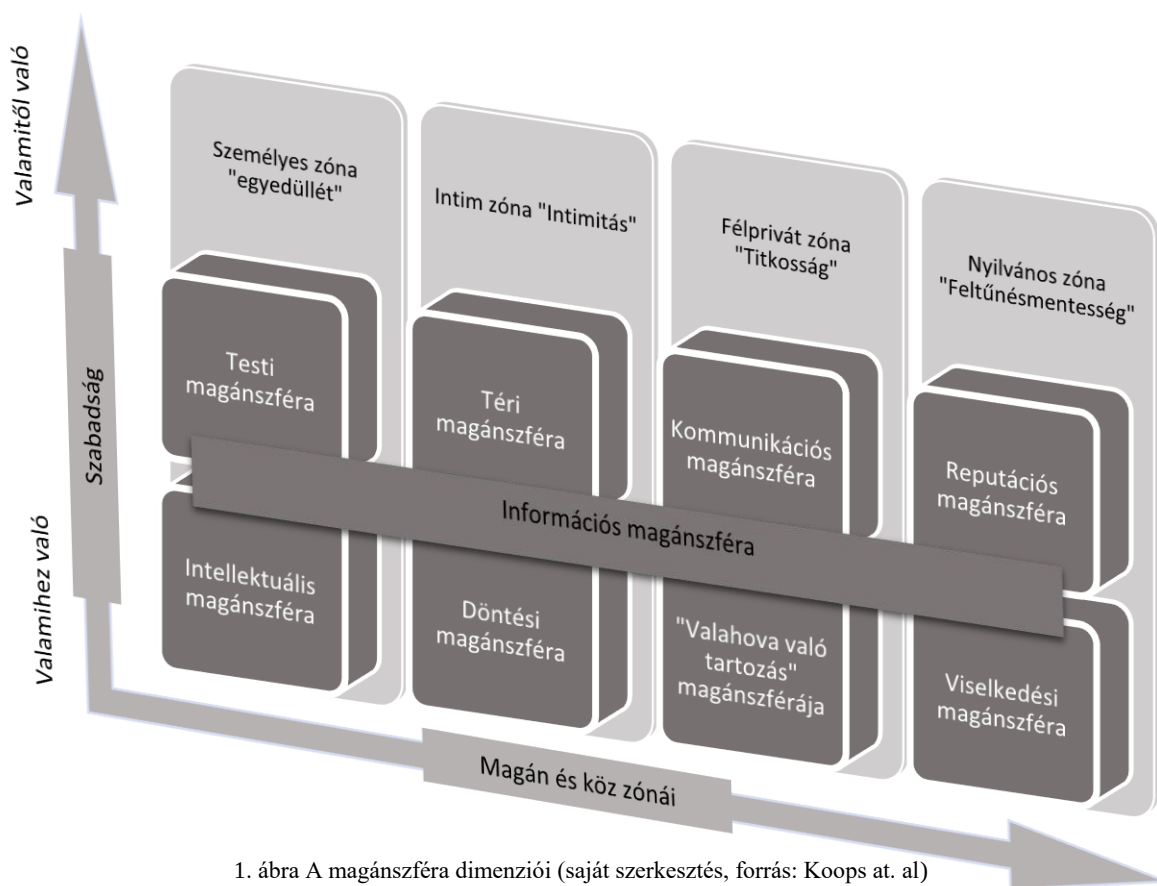
⁷ Solove, Daniel J.: Understanding Privacy, Cambridge, MA_London, Haarward University Press, 2008. , 24 pp.

Anita Allen különféle kategóriákba osztotta fel a magánszférát, amelyek szerint létezik az információs magánszféra, a reputációs magánszféra, a döntési magánszféra, „valahova tartozás” magánszférája és a fizikai, avagy térbeli magánszféra.⁸

Solove a magánszféra megfoghatatlanságát igazolva, a megsértéshez vezető aktusokat sorolta fel, mint csoportosítási szempontot. Ő információgyűjtési, információfeldolgozási, információterjesztési és inváziós csoportokba sorolja fel a magánszféra halmazainak.

Finn, Wright és Friedewald Roger Clarke öt kategóriáját egészített ki további kettővel, amelyek a „valahova tartozás” és a „téri és lokális magánszférát” említik meg további részhalmazainak, a magánszférának⁹.

A legátfogóbb tipológiát 2016-ban Koops és munkatársai állították össze, amely tökéletesen igazolja a Solove szerinti „megfoghatatlanságot” (lásd: 1. ábra)¹⁰.



1. ábra A magánszféra dimenziói (saját szerkesztés, forrás: Koops at. al)

Ahogy az 1. számú ábrán is látszik, van a magánszférának egy olyan dimenziója, amely az összes többit érinti. Ez nem egyfajta függési kapcsolódás a dimenziók és az információs

⁸ Székely el. al.: Biztonság és magánélet Az alkumodell megkérdőjelezése és meghaladása, In. Replika 2017. évfolyam 3. szám, 2017. 24 p.

⁹ uo. p. 24.

¹⁰ uo. 17. p.

magánszféra között, hanem egy halmaz – részhalmaz közötti kapcsolódás. Az ábrán szereplő másik 8 dimenziónak, mind van 1-1 olyan aspektusa, amely érinti az információs magánszférát. A kommunikációs technológiák népszerűvé válása a hétköznapi életben hozzájárul egy „adatosításhoz” amely által a magánszférát, mint átfogó fogalmat, könnyebb megsérteni.

A biztonság ugyanúgy kontextus függő, szöveggörnyezettől függően más – más jelentéstartalmat hordoz magában, mint a magánszféra. Létezik a biztonságnak egy pozitív jelentéstartalma, amely szerint, amely olyan fogalmakkal kapcsolódik össze, mint a biztonságérzet és az önbizalom, létezik egy negatív jelentéstartalma, amely olyan fogalmakkal fonódik össze, mint a kockázatok és a veszély elleni védelem vagy a kárt okozó behatások és van a harmadik, szűkebb jelentéskörrel értelmező jelentéstartalma, a vagyonbiztosítékok, mint értékpapírok, vagy egyéb birtoklást igazoló iratok.

A biztonságra, éppen ugyanúgy, mint a magánszférára, különböző megközelítési módszerek vannak. Vannak, akik a biztonságra, az egyéni és a csoportszintű szabadság korlátozójaként tekintenek, de vannak olyanok, mint például Zedner, aki a biztonságot a szabadság előfeltételének tekinti, amennyiben az állam minél kevésbé avatkozik bele az egyének és csoportok szabadságába, annál biztonságosabban érzik magukat.¹¹ Csoportosítási szempontból, ugyanúgy, mint a magánszféra esetében az évek folyamán egyre több és átfogóbb részeit határozták meg a tudósok. Lagazio egy ötös csoportosítási rendszert alkotott, melynek alapjául a károkat elszenvedhető entitások szolgálnak. Ezek szerint említ nemzetközi biztonságot, állambiztonságot, társadalmi biztonságot, egyéni biztonságot és üzleti biztonságot.

Friedewald és szerzőtársai a magánszféra 7 csoportosítási megfelelőjével párhuzamba állítható tipológiát alkotott meg:

- fizikai biztonság,
- társadalmi – gazdasági biztonság,
- környezeti biztonság,
- politikai biztonság,
- radikális bizonytalansággal szembeni biztonság,
- információs biztonság és
- kulturális biztonság.

Lagazio, ezt a 7 csoportosítási, összevetette, mennyire húzhatóak rá az ő által felvázolt 5 entitástípusra:

- nemzetközi szervezetek,

¹¹ uo. p. 24.

- állam,
- vállalatok,
- társadalom,
- egyének és háztartások.

Létrehozott egy 35 mezőből álló táblázat

os formát, amelyben az entitásokat és a biztonság adott típusait vetette össze.

Ezek alapján a hétköznapi cselekedeteket is be tudjuk azonosítani a biztonságot fenyegető tényezőkkel. Például, ha a politikai biztonságot vetjük össze az egyének és háztartásokkal, akkor Lagazio azt állapította meg, hogy ez, az egyéni jogok és szabadságok érvényesülését jelenti. Ugyanebben a módszerben leképezte az információs biztonságot a civil társadalom vetületében, amely alapján megállapította, hogy ez az egyének és csoportjaik identitásának megőrzését foglalja magába. Lagazio itt említette még meg egy eltérést, amelyben a biztonság és a magánszféra különbözik. Itt ugyanis a biztonságok egymás ellen is hathatnak, ezzel is rombolva a fogalom egységes koncepcióját. Például, ha az állam, mint entitás, nemzetbiztonsági intézkedést vezet be, gyengíti ezzel az egyének biztonságérzetét.

A biztonság és a magánszféra fogalmának körbejárása során már körvonalazódott, hogy a két fogalmi elem sok esetben hasonlít vagy áll összefüggésben egymással. A többek között a megfigyelés is olyan fogalom, amely mind a magánszférát, mind a biztonságot is érinti. Fogalmi meghatározásban a megfigyelés „az információk átvitelének vagy kiszivárgásának figyelése és felhasználása, pl. információs csatornák lehallgatása, rejtett csatornák alkalmazása”.¹² A Cambridge Dictionary megfogalmazásában a megfigyelés egy olyan cselekedet, amely során egy személyt vagy egy helyet figyelnek meg, különös tekintettel olyan személyeket, akik részesei voltak bűncselekménynek, vagy olyan helyszínen, ahol a bűnözők összegyűlnek.¹³

Összességében elmondható, hogy a magánélet szabadsága két változó által definiálható „érték”, amely a magánszféra és a biztonság közötti összefüggés.

Ennek értelmében központi szerepe van a rendszerben a központi megfigyelésnek és a folyamatos megfigyelés alatt tartásnak. Ennek átalakulása következett be az iparosodással és a monopóliumok kiépülésével, amely által az ellenőrző-szankcionáló megfigyelés már a magánszektorban is megjelent.

¹² Krasznay Csaba: A magyar elektronikus közigazgatási alkalmazások információbiztonsági megoldásai, Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Kar Katonai Műszaki Doktori I, Budapest, 2011., p. 109.

¹³ Meaning of surveillance in English In. Cambridge Dictionary, 2022, <https://dictionary.cambridge.org/dictionary/english/surveillance> (Letöltés dátuma: 2022.03.08.)

1.2 Az internetes mélycsomag vizsgálat

Az elmúlt egy évtizedben hatalmas változások mentek végbe az európai biztonsági színtéren, amely hatott az érintett szervek feladataira és a biztonsági gondolkodásra is.¹⁴ Már a hidegháborútól megfigyelhető, hogy a biztonságpolitikai veszélyekre, kihívásokra a különböző államok próbáltak megfelelő technológiákat találni, amelyekkel mind a terrorizmust, mind a hétköznapi bűncselekményeket (gyermekpornográfia, szerzői jogokkal való visszaélések, pedofília) fel lehet deríteni. Ennek tükrében megnöttek a hírszerzési és információgyűjtési igények, ezzel párhuzamosan biztonsághoz kapcsolódó információk is felértékelődtek¹⁵.

Egy 2014-ben készült Privacy and Civil Liberties Oversight Board jelentés¹⁶ (tömeges adatgyűjtés) részletezi a hírszerzési célú technikai információgyűjtés két fő típusát, amely a downstream és az upstream adatgyűjtés. Dolgozatom központi eleme, az internetes mélycsomag vizsgálat (Deep Packet Inspection, továbbiakban DPI), mely az upstream adatgyűjtésbe tartozik, ahol szűrések segítségével nyerhetőek ki azok a metaadatok vagy tartalmi elemek, amelyek a szolgáltatóknak, vagy az adott kormányzati szerveknek, csoportosulásoknak szükségesek. A mélycsomag vizsgálat, az információ-kinyerésnek és a hálózati csomagszűrésnek egy fajtája. A mélycsomag vizsgálat ellenőrző pontokon keresztül a továbbított csomag adatrészét és fejlécét, kiszűri a protokollnak való meg nem felelést, a spamet, a vírusokat, a behatolást és minden más meghatározott kritériumot, hogy megakadályozza a csomag áthaladását az ellenőrzési ponton.¹⁷

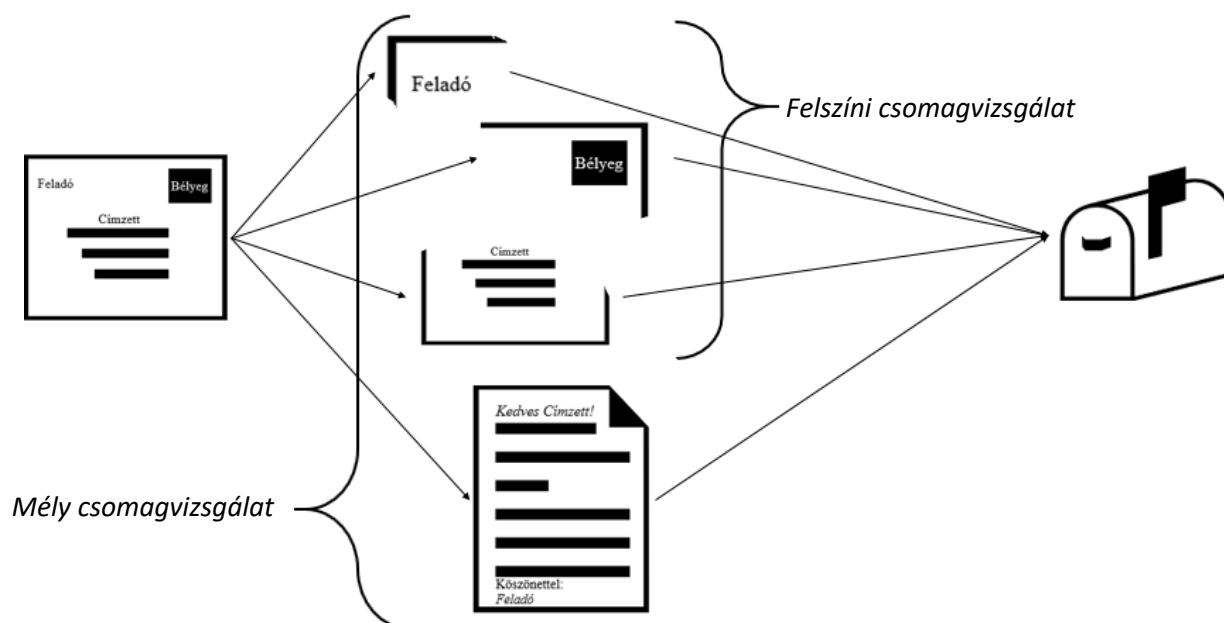
¹⁴ Dobák Imre: Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében, In Hadmérnök, 7. évfolyam 2. szám, 2017, pp. 235-249.

¹⁵ u.o. pp. 235-249.

¹⁶ u.o. pp. 235-249.

¹⁷ Chris Brook: What is deep packet inspection? How it works, use cases for dpi, and more, In. Digital Guardian, 2018.12.05., <https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more> (Letöltés dátuma 2021.03.25.)

A technológia létrehozásakor a kifejlesztők célja a malwarek („vírusok, rosszindulatú szoftverek, digitális kártevők gyűjtőneve”¹⁸) és a vírusok kiszűrése volt, hogy csökkenteni



2. ábra Az internetes felszíni – és a mélycsomag vizsgálat közötti különbség (saját szerkesztés, forrás: SurPRISE Research)

tudják a számítógépes hálózatokban okozta károkat. Egyes információk, amelyeket küldünk és/vagy fogadunk az interneten keresztül, egy bonyolult folyamaton haladnak keresztül, több számítógépen, akár több államon is. A legegyszerűbb magyarázat erre a postára feladott levél hasonlata. Amikor egy levelet feladunk, azt megcímezzük és a borítékot lezárjuk. Amennyiben a postás feladatát nézzük, akkor felszíni csomagvizsgálatról beszélünk. Nekik elég a címzést nézniük, feladatuk során figyelmen kívül hagyják a levél tartalmát. Ezzel ellentétben a mélycsomag vizsgálatnál az algoritmusok a címkéken, (példánkban a levél címzettjén és küldőjén) kívül a mélyebb rétegeket is megnézik (így a levél tartalmát is).

A mélycsomag vizsgálat tűzfalakon és routereken („Intelligens hálózati eszköz, amelynek feladata a beérkező adatcsomagok továbbítása a célállomás felé a lehető leghatékonyabb úton.”¹⁹) keresztül történik, amely az adatforgalmat és a rajtuk keresztül folyó összes üzeneteket irányítja a hálózatokban. Mivel a routerek az internetszolgáltatók kezében van, így ellenőrzés alatt tudják tartani a teljes internethasználatot, nemzetközi, országos, de lokálisan szinten is. Elsődlegesen magáncélra szánták a technológiát, de rövidtávon belátták, hogy hatalmas

¹⁸ Malware In. Kiberbiztonsági Fogalomtár, <https://makay.net/kiberbiztonsagi-fogalomtar> (Letöltés dátuma: 2021. 03. 25.)

¹⁹ Router, In. MiMi. <https://www.mimi.hu/informatika/router.html> (Letöltés dátuma: 2021. április 4.)

haszonra tehetnek szert, ha ezt eladják különböző vállaltoknak, akár védelmi ipari cégeknek is. Ennek köszönhetően a mélycsomag vizsgálat a technológia komoly piaca lett.²⁰

Mélycsomag vizsgálatot sokféleképpen fel lehet használni. Egyik ilyen fajtája a kereskedelmi célú használat. Ennek egyik alfajtája a hálózati biztonság, amelynek célja, hogy az üzenetek átvizsgálása során kiszűrje az esetleges malware-ket, illetve a felhasználók egymás közötti nagyméretű fájlmegosztását. A másik, talán leggyakoribb felhasználási formája - amely szintén minden állampolgárt érint -, a viselkedés alapú internetes reklám. Ennek alkalmazása során az adatok gyűjtésének az a célja, hogy megtudjuk, a felhasználók, milyen termékeket részesítenek előnyben. Ez a vásárlók számára egy szűkítő tényező annak érdekében, hogy könnyebben hozzájussanak azokhoz a termékekhez vagy szolgáltatásokhoz, amelyeket előnyben részesítenek. Ezt a módszert leginkább a mobil – és más hasonló szolgáltatók alkalmazzák, annak érdekében, hogy ügyfeleik számára minél személyre szabottabb ajánlatokat tudjanak felkínálni. A csoportosítási tényező harmadik alcsoportja a digitális jogok védelme, amellyel szakdolgozat, diplomamunka, doktori disszertáció vagy könyv esetleg cikk megírása közben is találkozhatunk, itt ugyanis az átvizsgálás célja, hogy leleplezzék az illegális fájlmegosztásokat és védjék a szerzői szabadságot. Erre a legegyszerűbb példa a szerzői-jog tulajdonosok, akik arra kérhetik az internetszolgáltatókat, hogy akadályozzák meg tartalmaik illegális letöltését. A másik nagy csoportosítási rész a közbiztonsági és a nemzetbiztonsági használat, hiszen a mélycsomag vizsgálat célja attól függ, ki alkalmazza. Itt beszélhetünk a bűncselekmények állami megfigyeléséről, habár ennek használata jogilag vitatott. Ennek segítségével ki lehet szűrni a különböző rasszista indíttatású vagy rasszista fenyegetéseket, a különböző szervezetek általi felbujtást, terrorcselekményeket, emberiség ellen elkövetett vagy elkövetést tervező magatartásokat, illetve számítógépek által elkövetett jogsértéseket, gondolva akár a gyermekpornográfiára. Másik nagy alcsoportja a cenzúra. A világ számos pontján, több diktatórikus rezsimben vélhető felfedezni, hogy a hatalmon lévő politikai erők, ellenfeleik elnyomása, félrevezetése, megtévesztése céljából használják ezt a technológiát. Ezen kívül idesorolható még az állampolgárok tudatos megtévesztése, tartalmak megváltoztatása, vagy elérhetetlenné tétele félrevezetés céljából.

Összességében elmondható, hogy a mélycsomag vizsgálatnak vannak pozitív és negatív oldalai is. (lásd: 1. táblázat)²¹

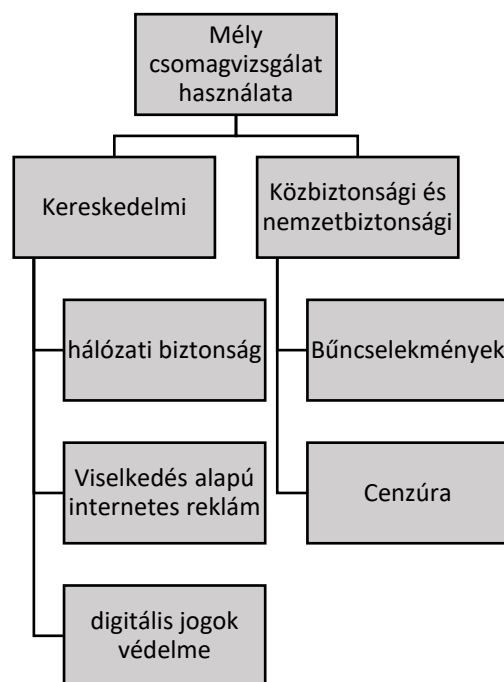
²⁰ Dr. Kirstie Ball, 2014. i.m.

²¹ Ibrahim, Ahmad . – Bayramoglu, Husnu: Preparation of Papers on A Survey on Network Data Collection In. Survey on Network Data collection, 2021.01. https://www.researchgate.net/publication/348390795_Preparation_of_Papers_on_A_Survey_on_Network_Data_Collection (Letöltés dátuma: 2021. december 14.)

1. táblázat: Az internetes mélycsomag vizsgálat pozitív és negatív aspektusai (saját szerkesztés, forrás: Preparation of Papers on a Survey on Network Data Collection)

technológia negatív felhasználása	technológia pozitív felhasználása
- magánszféra sérülése, - profilozás, - kommunikáció sérülése	- közbiztonság javítása, - információbiztonság javítása, - bűncselekmények bekövetkezésének csökkenése, - digitális jogok védelme

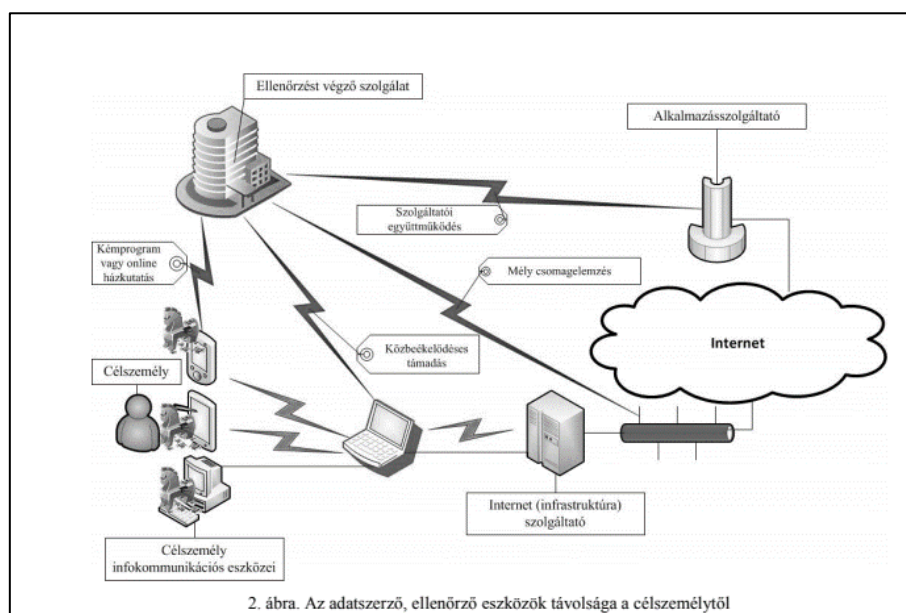
A technikai módszer egyszerre képes javítani a közbiztonságon, a súlyosabb bűncselekmények bekövetkeztének a csökkentésén és javíthatja az információbiztonságot. Megelőzni természetesen nem tudja, de a technológia által kinyert információk bizonyítékkul szolgálhatnak egy bűntény megoldásában. Ugyanakkor, a technológia lehetővé teszi az interneten áthaladó mindennemű metaadat és bizalmas tartalmak hozzáférését, ami a hálózatokon folyik, így a magánszféra sértetlensége megkérdőjelezhető. Ennek tudatában sok emberben merülhet fel a kérdés, hogy mit és hogyan posztol vagy egyszerűen mit ír, így az öncenzúra is megnőhet. Ezen felül nehéz megállapítani az átláthatóságát és nehéz megállapítani azt is, ki és milyen céllal használja fel a kiszűrt adatokat. A legnagyobb aggályok mégis az adatvédelemmel és a magánszféra megsértéssel kapcsolatban állnak fent. Ugyanis, ha a mélycsomag vizsgálatot marketing és reklámozás keretében használják, lehetőség nyílik a felhasználók viselkedésének nyomon követésére, valamint a böngészési és egyéb adataik marketing – vagy reklámcégeknek történő értékesítésére (lásd: 3. ábra).



3. ábra Az internetes mélycsomag vizsgálat használata (saját szerkesztés, forrás: SurPRISE Research)

1.3 Mélycsomag vizsgálat és az egyén kapcsolata

Az internetes technológiára épülő megfigyelésnek 4 fajtáját különböztetjük meg, amelyeket csak az arra felhatalmazott szolgáltatók használhatnak. Ezek között szerepel az aktív ellenőrző eszköz, a közbeékelődéses ellenőrzés (Man-in-the-Middle), az együttműködés a szolgáltatóval és a mélycsomag vizsgálat. A négy megfigyelési módszerben egy közös tulajdonság van, hogy mindenhol jelentős a célszemélytől való távolság. (lásd: 4. ábra)²²



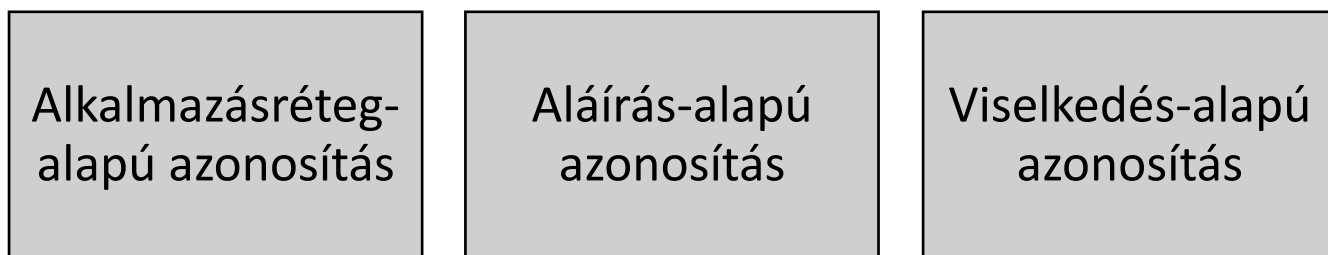
2. ábra. Az adatszerző, ellenőrző eszközök távolsága a célszemélytől

4. ábra Az adatszerző és a célszemély távolsága (Kovács Zoltán)

²² Kovács Zoltán: Biztonság vs. törvényes ellenőrzés az internet alapú kommunikációban – Ellentétes vagy egymással megférő követelményeknek? I. In. Hadmérnök 6. évfolyam. 4. szám, 2016., pp. 222-230.

A mélycsomag vizsgálat – ahogy azt az előző alfejezetben hosszabban kibontottuk – azt jelenti, hogy „az adatcsomagoknak nem csak a fejlécét, hanem azok adattartalmát is vizsgálat alá vetik”²³ és ezek alapján kiszűrjük az értékes adatcsomagokat. Felhasználási célja a szűrés jellegétől függ, mit szeretnének az adott szolgáltatók, szervek, vállalatok vagy más entitások megtudni. A technológiát főleg a nagy sebességű hálózatok valós idejű hálózati forgalmának kezelésére és elemzésére használják. Ezek között olyan feladatokat is szerepelhetnek, mint a hálózat sávszélességének kezelése, annak megfigyelése, kezelése, a tartalom optimalizálása, a szerzői jogok érvényesítése vagy a kormányzati felügyelet elősegítése. De ezek még mindig nem az összes lehetőség, amire a technológia képes. A mélycsomag ellenőrzés a nyílt rendszer-összekapcsolási modell összes rétegében képes figyelemmel kísérni a hálózatokon keresztülmenő adatforgalmat és kommunikációt is. Lehetővé teszi a hálózati operátorok számára az IP-csomagok fejlécének és a terhelésének beolvasását. Más technológia erre nem képes.²⁴

A mélycsomag ellenőrzés felhasználhatósága szerint három kategóriába sorolható. Ezek közé tartozik az aláírás-alapú azonosítás, alkalmazásréteg-alapú azonosítás és a viselkedés-alapú azonosítás. Az aláírás-alapú azonosítás tekintetében a DPI a bejövő csomagok szignatúrájának egyeztetéséhez nyújt segítséget, amelynek köszönhetően könnyebben ki lehet szűrni az illegális fájlmegosztásokat, és a szerzői jogok védelmében is segít. Az alkalmazásréteg-alapú azonosításnál a DPI az alkalmazások és az internet közötti lekérések, illetve az ott lezajló párbeszéd ellenőrzését végzi. A viselkedés-alapú azonosítás során a felhasználók viselkedésének megítélésére használják a csomagok azonosítása alapján. (lásd: 5. ábra)



5. ábra DPI által végezhető azonosítás típusai (saját szerkesztés, forrás: An Approach for Detecting Man-In-The-Middle Attack Using DPI and DFI)

Minden alkalommal, amikor kutatunk valami után az interneten, a felhasználó egy adott domain név vagy a böngészőnk által egy kérelmet küld a webszerverhez, a webhely megadására. Ilyenkor jelentkezik a mélycsomag ellenőrzés, ahol a forgalom jellemző kódjai kerülnek

²³ uo. pp. 222-230.

²⁴ Gosh, Argha - Senthilrajan, A.: An Approach for Detecting Man-In-The-Middle Attack Using DPI and DFI In. Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI - 2019), 2020.03.05., https://link.springer.com/chapter/10.1007/978-3-030-43192-1_64#Sec10 (Letöltés dátuma: 2021.11.23.)

ellenőrzés alá. Ezek segítségével próbálja azonosítani az alkalmazás forráspontját, forráscímét, típusát, célportját, célcímét és a csomagok számát. Elsősorban próbál minden összegyűjthető adatot összeszedni, ami csak lehetséges, mindezt úgy, hogy közben a csomagokról másolatokat készít, hogy forgalmunk sebességén ne lássunk változtatást.²⁵

A fent leírtak alapján már tudhatjuk, hogy a DPI által lehetőség nyílik a különböző kommunikációs testekhez (mint például a tartalmi részhez) való hozzáféréshez is. Ezáltal könnyen hozzá lehet férni üzenetváltásainkhoz (mind e-mailjeink, személyes beszélgetéseink), egy általunk nézett YouTube-videó tartalmához, de akár egy Skype-beszélgetés (vagy a különböző alkalmazások, amelyek segítik a távoktatást, táv munkavégzést, például: Zoom, Microsoft Teams, Coospace) részleteihez is. Itt is, mint a mélycsomag vizsgálatnál már említettük, az ellenőrzés megadott minták és kulcsszavak alapján történik.

De a mélycsomag vizsgálatot nem csak a kommunikáció nyomon követésére lehet használni, hanem annak megváltoztatására is. A csomagok fejlécének ellenőrzésénél a kulcsszavas azonosítás által lehetőség nyílik bizonyos információk cenzúrázására. Így lehet blokkolni adott adatokat vagy kapcsolatokat megszakítani, miáltal az általunk felkeresett információt egy új csomag injektálásával kapjuk meg. Itt érdemes megemlíteni Kínát, ahol jelentősen felfedezhető az internetes cenzúra nyomai. A teljeskörű ellenőrzésnek köszönhetően az államba belépő kommunikáció a nemzetközi kapcsolatokról egy, az állam által láttatni kívánt képet vízionál. A nem kívánatos tartalmakat automatikusan vagy manuálisan távolítják el. Egy tanulmány 56 millió üzenetet a Sina Weibo-ról és 11 millió kínai nyelvű Twitter üzenetet vizsgált, amely rávilágított arra, hogy a cenzúra igenis jelen van az országban. Ezt bizonyítja, hogy példának okáért bizonyos - jellemzően politikailag érzékeny - kifejezések használata automatikus cenzúra alá esik, annak érdekében, hogy a felhasználók adott időpontban ne tudjanak meghatározott kifejezéseknek utána keresni. Ilyen volt az „Egyiptom” szó az Arab Tavasz idején.²⁶ A vizsgálatokból kiderül, hogy olyan is előfordult, hogy visszamenőleg töröltek politikailag érzékeny üzeneteket, hogy úgy tűnjön, nem egységes az ország. Erre a Tibetből és Csinghaj-ból érkező üzenetek gyakoribb törlése enged következtetni.²⁷ A cenzúrázott kommunikáció másik nagyszabású elemzésében King és csapata arra a következtetésre jutott, hogy „a cenzúra program célja, hogy csökkentse a kollektív cselekvés valószínűségét a

²⁵ u.o.

²⁶ Bamman, D. - O'Connor, B. - Smith, N: 'Censorship and deletion practices in Chinese social media', In. First Monday, 2012.03.04., pp. 2., <https://journals.uic.edu/ojs/index.php/fm/article/view/3943> (Letöltés dátuma: 2021.12.03.)

²⁷ King et. al.: How Censorship in China Allows Government Criticism but Silences Collective Expression In. American Political Science Review, 2013.05., <https://gking.harvard.edu/publications/how-censorship-china-allows-government-criticism-silences-collective-expression> (Letöltés dátuma 2021.12.03.)

társadalmi kapcsolatokban”.²⁸ Ilyenkor a kollektív fellépéshez kapcsolódó hozzászólások tartalmát felülvizsgálják és törlik attól függetlenül, hogy azok kritikusak-e az államra nézve, vagy sem. A kínai kormányról ismert, hogy a technológia adta lehetőségeket az ország hálózatának megfigyelésére használják, és cenzúrázzák az érdekeiket sértő tartalmakat, webhelyeket. Ennek segítségével a Kínai Népköztársaság blokkolja a pornográfiát, a vallási információkat, a politikai nézeteltérésekre vonatkozó anyagokat és olyan népszerű weboldalakat, mint a Wikipédia, a Facebook, vagy a Google. (A technológia felhasználási formáit a 2. táblázat szemlélteti)

2. táblázat: Az internetes mélycsomag vizsgálat felhasználási formái (saját szerkesztés, forrás: Ibrahim, Ahmad)²⁹

Internetes mélycsomag vizsgálat felhasználási területei		
Biztonság	Hálózat optimalizálás	Üzleti megoldások
IPS/IDS	tapasztalati minőség (Quality of Experience – QoE)	számlázás és alkalmazások
tűzfal	csomagirányítás	feliratkozás vizsgálás
alkalmazás biztonság	szolgáltatásláncolás	hálózatfigyelés
behatolásérzékelő	tartalom-gyorsítótárazás	

Rengeteg olyan alkalmazást lehetne felsorolni, amelyeket baráti üzenetváltások, munkahelyi e-mailek, családi SMS-ek küldésére, fogadására használunk. Üzenetek, amelyeket egy általunk meghatározott személynek vagy csoportnak küldünk. De belegondoltunk-e abba, hogy ezeket az üzeneteket vagy azok egy meghatározott részét mások is láthatják? A mélycsomag vizsgálatot végző alkalmazások - annak érdekében, hogy kiszűrjék a veszélyeket tartalmazható üzeneteket, így a hálózaton áthaladó összes kommunikációt, közöttük a felkeresett weboldalakat, elküldött üzeneteinket-, akár a lehallgatást is lehetővé teszik a megfigyelők számára. Mivel ezáltal nem konkrét személyek után kutatnak, így nem szükséges gyanúsítottak lennünk ahhoz, hogy mi is mélycsomag vizsgálat alá essünk.

Már a kezdetektől fogva a telefon – és internetszolgáltatók képesek voltak hálózatukon keresztülmenő folyamatok monitorozására. Az így kinyert adatokat többféle módon

²⁸ Snapshot of Xi on making Internet an interconnected world In. China Daily Online, 2015.12.11., https://usa.chinadaily.com.cn/2015-12/11/content_22693550_4.htm (Letöltés dátuma: 2021.12.03.)

²⁹ Ibrahim, Ahmad, 2021. i.m.

felhasználják, de a leggyakoribb ezek közül a számlázás, a marketing célú hirdetések és a monitorozás. Elsődleges céljuk, hogy a csomagok átvizsgálása közben észlelnek-e olyan tartalmakat, amelyek veszélyesek lehetnek. Üzeneteink, mielőtt elérnek a címzetthez, több csomagra darabolódnak, amelyeknek egy részét kötelező, hogy az internetszolgáltatók megnézzék és átvizsgálják, hiszen így tudják meg azt is, hogy kihez kell eljuttatniuk az üzenetet. A mélycsomag vizsgálat ezzel ellentétben több adatsomagot is átvizsgál és kiértékel a különböző ellenőrzőpontokon, különböző algoritmusokat és szűrőket alkalmazva, kulcsszavakra keresve. Ez hasonlóan működik, mint amikor a Google keresőjét használjuk. Így a beállított kulcsszavak kapcsolatban állhatnak rosszindulatú alkalmazásokkal irányított marketinggel, bűncselekménnyel, de akár vásárlási szokásokkal is. Ezen beállítások csak a felhasználótól függenek.

Következtetések

1. fejezetben kifejtésre került a magánszféra, biztonság és az internetes mélycsomag vizsgálat meghatározásának lehetőségei szakirodalmak és folyóiratok és internetes oldalak feldolgozása alapján. A feldolgozott irodalmak alapján elmondható, hogy a 3 fogalom között szoros az összekapcsolódás. Ahogy az a magánszféra és a biztonság csoportosításai módja hasonló, és létezik egy olyan alcsoportjuk, amely közrefogja az összes csoportot. Az internetes mélycsomag vizsgálat technológiai ismertetése során kiderült, különböző területeken történő felhasználása milyen módon van jelen mindennapi életünk során, hogyan segíti hétköznapi életünket, ugyanakkor melyek azok a felhasználási területek, amelyekkel magánszféra és biztonságunk is sérülhet.

2. Mélycsomag vizsgálat jogi szabályozása

2.1 A magánszféra és a technológia által érintett jogok

Ahogy az a bevezető részben és az első fejezetben is láthattuk, a technológia gyors fejlődése és elterjedése növelte a magánszemélyek kiszolgáltatottságát a hétköznapi életben és rendkívül sérülékennyé tette a magánszférát. Manapság nem csak az állam tárol rólunk adatokat, hanem a különböző gazdasági és piaci szereplők is, hiszen marketingpolitikájuk egyik fontos eleme, hogy minél többet tudjanak meg rólunk.³⁰ Napjainkra a család és a személyiségünk védelme kulcsfontosságú tényezővé vált, hiszen az egyén „ellenőrzése” alatt már csak ez a szűk szelet maradt a mindennapjaiból, amelyet próbálunk megvédeni a külön fajta külső hatásoktól a jog által biztosított eszközökkel.³¹ Věra Jourová 2018. május 24-én fogalmazott úgy egy nyilatkozatában, hogy: „Az adatvédelem alapvető jog az EU-ban. Az új szabályok jóvoltából az európaiak visszaszerzik az ellenőrzést adataik felett. A döntés arról, hogy mi történjen és ki, milyen jellegű adatokkal rendelkezzen, immár a mi kezünkben van.”³²

Amennyiben az Európai Unió adatvédelmi fejlődését tekintjük, akkor visszatekinthetünk az Európai Unió Alapjogi Chartájára, amelynek 8. cikke már magába foglalta a személyes adatok védelméhez és a hozzá kapcsolódó elveket és jogokat.³³ 2016 május 24-ei kihirdetéssel megszületett az Európai Unió egészére vonatkozó, egységes adatvédelmi szabályozása, „A természetes személyeknek a személyes adatok kezelése tekintetében történő védelemről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről” szóló 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet” (Általános Adatvédelmi Rendelet, továbbiakban: GDPR).³⁴

A rendelethez kapcsolódó első fontos megjegyzés, hogy nem csak az Európai Unió tagállamira vonatkozólag érvényes, hanem az Európai Gazdasági Társaság tagállamaira is érvényes, amely magába foglalja, Izlandot, Lichtensteint és Norvégiát is.³⁵

³⁰ Törley Gábor: Informatikai Biztonságtudatosság, ELTE Informatikai Kar, Budapest, 2019, p. 5.

³¹

³² Jourová Věra, ‘Andrus Ansip alelnök és Věra Jourová biztos nyilatkozata az általános adatvédelmi rendelet alkalmazásának kezdete előtt’, In. European Commission - European Commission, p. 1, https://ec.europa.eu/commission/presscorner/detail/hu/STATEMENT_18_3889 (Letöltés dátuma 2022. 03.22.)

³³ Sziklay 2018 i.m. p. 12.

³⁴ Sziklay 2018 i.m. p. 13.

³⁵ Az Európai Gazdasági Térség tagállamai In. Konzuli Szolgálat, <https://konzuliszolgalat.kormany.hu/egt-tagallamok> (Letöltés dátuma: 2022.03.10.)

A Rendelet megalkotásának célja, egy harmonizált jogrendszer megalkotása, mely hozzájárul az egyéneknek jogaiknak megismeréséhez és az adatkezelési gyakorlatok javulásához.³⁶ A Rendelet megalkotása során figyelembe kellett venni, hogy a technológia mindig előre fog járni, mint az azt szabályozó jogszabályi háttér. Ennek értelmében a jogszabályalkotók egy technológiailag semleges jogszabályt hoztak létre, amely részletességéből fakadóan könnyen rá lehet húzni egy-egy újabb technológiára.³⁷ A GDPR a korábbiaktól eltérően az elszámoltathatóság elvéhez kapcsolódva, szigorúbb részletszabályokat tartalmaz az adatkezelőkre vonatkozóan. Ugyanis a 23. cikk kötelezi mind az adatfeldolgozókat mind az adatkezelőket, hogy rendszeres felülvizsgálati dokumentációt vezessenek. Ezen kívül itt kerül leírásra, hogy mely célok elérése érdekében lehet adatok gyűjteni az egyénekről. A GDPR 11 fejezetre tagolódik, amelyek közül a dolgozat tekintetében az alábbiak relevánsak:³⁸

- a II. fejezet egy alapvető feltételrendszert tartalmaz az adatkezelés elveiről, mint például az adattakarékosság, az elszámoltathatóság és a jogszerűség,
- a III. fejezet az egyének jogait és azok érvényesíthetőségét tartalmazza,
- a IV. fejezet az adatfeldolgozóról állapít meg különböző kötelezettségeket, mint például a dokumentációs kötelezettség. Ezen kívül egy kockázatalapú megközelítést tartalmaz, amely alapján az adatfeldolgozónak az adatvédelmi felügyeleti hatósággal kell a konzultációt lefolytatnia,
- a VIII. fejezet a jogorvoslati lehetőségeket és az adatkezelőkre vonatkozó felelősségi szabályokat tartalmazza,
- a IX. fejezet a Rendelet különös része, amely az egyes szabályoktól való eltérés lehetőségeit részletezi a tagállamok számára.

Azonban az egységes adatvédelmi jog kialakulása még nem valósult meg teljesen a GDPR-nak köszönhetően sem. Habár a GDPR 5. cikke részletezi a személyes adatok kezelésére vonatkozó alapelveket³⁹, és a 12-22. cikkben felsorolásra kerülnek az egyének jogai⁴⁰, a nemzetállamok tagországainak adattvédelmi hatóságai más-más értelmezési keretet adhatnak egy-egy

³⁶ Nagy Renáta - Dr. Sziklay Júlia: A GDPR Egyszerűen Kis- és Középvállalkozások Számára, Magyar Közlöny Lap- És Könyvkiadó Kft, Budapest, 2020, p. 18.

³⁷ GDPR Preambulum 15. bekezdés.

³⁸ Sziklay, 2018. i.m. , pp. 14-16

³⁹ GDPR 5. cikk: Jogszerűség, tisztességes eljárás és átláthatóság; Célhoz kötöttség; Adattakarékosság; Pontosság; Korlátozott tárolhatóság; Integritás és bizalmas jelleg; Elszámoltathatóság

⁴⁰ GDPR 12-22. cikk: Átlátható tájékoztatáshoz való jog; Hozzáféréshez való jog; Helyesbítéshez való jog; Törléshez és elfeledtetéshez való jog; Korlátozáshoz való jog; Adathordozhatósághoz való jog; Tiltakozáshoz való jog; Automatikus döntéshozatal elutasításához való jog

részletszabályt illetően, amelyek bizonytalan környezetet teremtenek az adatvédelmi rendelet jogszerű betartásában.⁴¹

Magyarország Alaptörvényének VI. cikkében megfogalmazásra kerül, hogy „Mindenkinek joga van személyes adatai védelméhez valamint a közérdelű adatok megismeréséhez és terjesztéséhez”⁴² és „A személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi.”⁴³

A korábbi, 2005. évi XIX. törvény újraszabályozása és az Alaptörvényben foglalt alapvető jogok való összeegyeztetésével született meg a Magyarországon a jelenleg hatályos törvény, a 2011. évi CXII. törvény, az információs önrendelkezési jogról és az információszabadságról szóló törvény. (Továbbiakban: Infotörvény) Az Infotörvény szabályai az információs önrendelkezési jog és az információszabadsághoz fűződő jogok érvényesüléséhez szükséges rendelkezéseket tartalmazza. Ennek értelmében ide tartoznak a nemzetbiztonsági adatkezelések,⁴⁴ a bűnüldözési célú adatkezelések⁴⁵ és honvédelmi célú adatkezelések⁴⁶. Említésre méltó, hogy az Infotörvényt létrehozó jogalkotók a GDPR-t kiegészítve különbséget tesz automatizált és manuális eszközzel végzett adatkezelési műveletek között. A GDPR-hoz hasonlóan részletezi az Infotörvény is a személyes adatok védelmére vonatkozólag azokat a tartalmi elemeket, amelyeket az adatkezelőknek alkalmazniuk kell, és ugyanúgy az adatkezelő hazai tevékenységi helyéhez köti. Ezenkívül ezeket a részletszabályokat kiterjeszti azon tevékenységekre is, amelyek az egyének részére áruk, vagy szolgáltatások nyújtására, vagy viselkedésük megfigyelésére irányul.⁴⁷

Az egyes jogszabályokon kívül fontosnak tartom megemlíteni a biztonságtudatosságot is, mint fogalmat. Mint befolyásoló tényező, ez is rendkívül fontos mérési mutatója lehet az egyének egyes technológiákhoz való hozzáállásához. A biztonságtudatosság alapját maguk az egyének képzik, pontosabban az egyének tudata, hogy képesek-e felismerni, hogy a tudatosságuk hiánya veszélybe sodorhatja őket illetve munkahelyüket, és képesek átlátni, hogy az adott helyzetben mi a leghatékonyabb cselekvési módszer.

Összefoglalóan elmondható, hogy az uniós és a hazai szabályozás a magánszférát és az információszabadságot prioritásként kezelik. A hazai szabályozás élt a GDPR-ban foglalt lehetőséggel, mely kimondja, hogy a különös részben foglalt szabályoktól a tagállamok

⁴¹ Nagy -Dr. Sziklay 2018. p. 14.

⁴² AT VI. cikk (3)

⁴³ AT VI. cikk (4)

⁴⁴ Infotv. 3. § 10b. pont.

⁴⁵ Infotv. 3. § 10a. pont

⁴⁶ Infotv. 3. § 10c. pont

⁴⁷ Sziklay 2018., i.m. p. 20.

eltérhetnek. Azonban ezek a szabályozások a technológiai fejlődésre és a technológia adta lehetőségekre nem válaszol. Sem az Általános Adatvédelmi Rendelet sem a magyar Információs önrendelkezési jogról és az információszabadságról szóló törvény nem tér ki a magánszférát érintő és sértő technológiákra.⁴⁸

2.2 Európai Unió és nemzetközi szabályozások

Ahány ország vagy nemzeti entitás létezik, ugyanannyi jogszabály is. Ahogy a nemzetek különböznek, úgy jogalkotási mechanizmusok és törvénybe foglalt gondolatok, szabályozások is különböznek. Ebben a fejezetben a mélycsomag vizsgálat szabályozásait szeretném bemutatni egy Európai Unió kívüli és egy Európai Unió belüli országokban.

A világ egyik talán legrészletesebb szabályozási hátterét a kolumbiai jogszabályokban találhatjuk meg, ezzel kapcsolatban. A technológiai berendezésekről már az 1991. évi alkotmányuk 15. cikke úgy fogalmaz, hogy *„A levelezés és a magánjellegű kommunikáció egyéb formái sérthetetlenek. Ezek azonban csak a törvény által előírt esetekben, bírósági végzéssel és az alaki követelményeket betartva lehet lehallgatóvá tenni vagy nyilvántartásba venni.”*⁴⁹ Ennek következtében a helyi jogalkotók úgy gondolják, hogy az adatok és tulajdonosaik sértetlensége érdekében további jogszabályokat hoznak létre. Így jött létre a 2009. évi 1273-as és a 2012. évi 1581-es törvény. Utóbbit a helyiek a *„Személyes adatokról szóló törvény”*-ként tartják számon, amelynek első cikke már megfogalmazza, hogy *„E törvény célja, hogy biztosítsa minden ember alkotmányos jogát, hogy hozzáférjen, frissítse és helyesbítse a róluk adatbázisokban vagy fájlokban gyűjtött információkat, valamint egyéb jogokat, szabadságot és alkotmányos garanciákat, amelyeket az Alaptörvény 15. cikkében szerepelnek...”*⁵⁰, amely szintén a kolumbiai Magna Charta 15. cikkére utal, ezzel is erősítve az alaptörvényükben leírtak jelentőségét. Mindezekhez hozzátartozik még a 2013. évi 1377-es törvény, amelyet részben kiegészít a Heabes Data törvényük.

Országuk 2012. évi 1704. számú rendelete szabályozza, hogy mely szerv milyen körülmények között alkalmazhatja a törvényes lehallgatás módszerét, amely megemlíti a mélycsomag vizsgálatot is. *„Az lehallgatások, mint hivatalos eljárások csak a Nemzet Legfőbb Ügyészének előzetes jóváhagyásával indulhat el, konkrétan megfogalmazva a kommunikáció lehallgatásának okát, mint a közbiztonság mechanizmusa. Ezen soroknak kiemelt szerepe van*

⁴⁸ Mógor Tamásné - Az emberi tényező szerepe az információbiztonság megvalósítása és erősítése terén. Az információbiztonsági kultúra fejlesztésének lehetőségei a Magyar Honvédségben - Biztonságtudományi Doktori Iskola, Budapest, 2017, p. 49.

⁴⁹ Asamblea Nacional Constituyente, Artículo 15, Constitucion Politica De Colombia 1991., Kolumbia, 1991 (Saját fordítás)

⁵⁰ Congreso de Colombia, Ley estatutaria 1581 de 2012. Kolumbia, 2012. (Saját fordítás)

*a szükséges jogi keretek megértéséhez, amelyekben Kolumbia a mélycsomag vizsgálatot használja... A közbiztonság mechanizmusa optimalizálja a bűncselekmények kivizsgálásának munkáját, az alkotmányos és törvényes keretek között.*⁵¹ A rendelet olyan szempontból hiátust tartalmaz, mivel az internetszolgáltatók által gyűjtött adatokra nem tekint ki, azokat nem emeli be a törvényi szabályozásba, hiszen ők is előzetes engedély nélkül végeznek elemzéseket és analizálják az információinkat. Annak ellenére, hogy Kolumbia jogszabálya a DPI-t nagyon részletesen szabályozni kívánja, itt is találatok hibák. Ezek között szerepel a jogszabályi ismeretek hiánya az állampolgárok körében, mivel a megalkotott jogszabályok nem kerülnek kihirdetésre, és nincs egy olyan nemzeti felügyelőszerv, amely betartatná a meghozott döntéseket.⁵²

Az Európai Unió elsődleges jogforrása az előző fejezetben kifejtésre került. Itt egy 2012-ben megjelent, az európai adatvédelmi biztos véleményét mutatom be, mivel ebben a véleményben részletesen kitért a hálózatsemlegességre, a mélycsomag vizsgálat jelentette kockázatokra, később az ezzel kapcsolatosan megfogalmazott javaslataira.

Peter Hustinx⁵³ a „Nyílt internet és hálózat semlegesség Európában” című közleményre reflektált. Véleményét 6 szakaszra osztotta, amelyek a következőképpen alakultak:

- bevezetés,
- hálózatsemlegesség és forgalomkezelési politikák,
- a hálózat semlegességre vonatkozó uniós jogi keret áttekintése és további szakpolitikai fejlemények,
- műszaki háttér és a kapcsolódó, a magánélet és az adatok védelmével összefüggő egyéb szempontok,
- a magánélet és az adatok védelmére vonatkozó uniós jogi keret alkalmazása,
- politikai és jogszabályi intézkedésekkel kapcsolatos javaslatok,
- következtetések.

Az európai adatvédelmi biztos már az elején vízionálja a problémát. Ő a hálózatsemlegesség fogalmából vezeti le az egész problémafelvetést, hogy vajon az internetszolgáltatóknak meg lehet-e engedni, hogy különböző módokon (korlátozásokkal, blokkolásokkal vagy szűrésekkel) hatást gyakoroljanak az internet teljesítményére. Peter H. szerint az információkat

⁵¹ Decreto Numero 1704 de 2012. Kolumbia, 2012.

⁵² Parra et al. : Legal assessment of DPI in telecommunication networks in Columbia, IEEE, London, 2014, 86.p.

⁵³ Európai Adatvédelmi Biztos 2004-2014-ig In. European Data Protection Supervisor, Wikipedia 2022.02.07, https://en.wikipedia.org/wiki/European_Data_Protection_Supervisor (Letöltés dátuma 2022.03.02.)

„Részrehajlás nélkül, tartalomtól, címtől és forrástól függetlenül kell továbbítani”.⁵⁴ Mint ahogy a korábbi fejezetekben is kibontásra került, az internetszolgáltatók általi hálózathatalom-szűrés, - blokkolás, - ellenőrzés érintheti a kommunikáció tartalmát, az elküldött és fogadott e-maileket, de akár a megtekintett forgalmakat is. Az európai adatvédelmi biztos szerint komoly aggályokat vet fel a technológia alkalmazása a kommunikáció titkosságának elve, a magánélet védelme és az adatvédelem fontossága ügyében.

A véleményezésben is kifejtésre kerül, hogy az internetszolgáltatóknak számos okuk van az internetforgalom ellenőrzésére. Ennek segítségével tudják az „idő szempontjából érzékeny forgalmakat, például a videoadatfolyam-átvitelt” és a hálózaton keresztülmenő tartalmakat vizsgálni, amely segítségképpen szolgálhat a szerzői jogok érvényesítése érdekében és a pornográf tartalmak kiszűrésében.

Peter Hustinx azt a következtetést vonja le, hogy az IP-hasznosadatokon alapuló vizsgálati technológiák által megszerzett információknak köszönhetően nem csak a külön fajta vírusok azonosítására használhatják fel, hanem olyan felhasználói profilok létrehozásához is, amely viselkedésalapú reklámtevékenységhez köthető. Minél átfogóbb és mélyrehatóbb a kapott információk elemzése, annál jobban sérül a közlések titkosságának elvével.⁵⁵

Az európai adatvédelmi biztos azt a következtetést vonta le konklúzióként, hogy habár a szolgáltatók egyre nagyobb mértékben hagyatkoznak az ellenőrzési és vizsgálati technológiákra, ez veszélyezteti az internet semlegességét és a közlések titkosságának elvét, de problémákat jelent a magánélet és a személyes adatok védelmét tekintve is. Javaslatában egy új bizottság, szakmai csoport létrehozását javasolja, amely vállalja az iránymutatás kidolgozását. Ezen kívül szakpolitikai vitákat is javasol, amely koordinációjának és irányítása a Bizottság feladata lenne. A legfontosabb kérdések szerinte, hogy az ellenőrzések mikor teszik szükségessé az egyén tájékoztatását és hozzájárulását; melyek azok az ellenőrzési gyakorlatok az internetszolgáltatók tekintetében, amelyek feladatiak ellátása érdekében elengedhetetlenül fontosak; illetve melyek azok az adatvédelmi garanciák, amelyekkel az érintett egyének élhetnek.

Az adatvédelmi biztos következtéseinek megvalósulásával kapcsolatosan felvettem a kapcsolatot az Európai Unió Adatvédelmi Biztos Titkárságával. Kérdésemre azt a választ

⁵⁴ Hustinx, Peter: Az európai adatvédelmi biztos véleménye a hálózatszemlegességről, a forgalomkezelésről, valamint a magánélet és a személyes adatok védelméről In. Az Európai Unió Hivatalos Lapja, 2012.02.08., pp. 1, [https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52012XX0208\(01\)&from=FR](https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52012XX0208(01)&from=FR) (Letöltés dátuma : 2022.03.08.)

⁵⁵ 2002/58 irányelv 5. cikk In. Az Európai Parlament és a Tanács 2002/58/EK Irányelve, 2002.07.12., <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:02002L0058-20091219&from=HU#tocId7> (Letöltés dátuma: 2022.03.08.)

kaptam, hogy az Európai Elektronikus Hírközlési és Szabályozók Testülete (Body of European Regulators for Electronic Communications) 2016-ban közzétett a tagállamok felügyelő szervei számára (Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság) egy általános iránymutatást (melyet a későbbiekben frissített) a hálózatsemlegesség garantálásáról, és a személyes adatok védelmének feldolgozási kérdésköréről. Ezek értelmében a nemzeti szabályozó hatóságoknak értékelni kell, hogy az internetszolgáltatók által végzett kezelések megfelelően arányosak-e az adott cél elérésére érdekében.⁵⁶ Továbbá a nemzeti illetékes hatóságoknak értékelni kell, hogy a személyes adatok kezelése megfelel-e az Unió jogának.

Ahogy az látható, több országban, térségben próbálnak megfelelő jogi keretet adni a technológiai haladásnak, de mindenhol megfigyelhető, hogy a regulációs folyamatok még nem tekinthetők véglegesnek. Kolumbiában fellelhető több, a személyes adatokat védő jogi aktus, de ezekről a jogszabályokról a helyiek tájékoztatása elmarad. Az Európai Unióban hozott döntések technológiailag semlegesnek tekinthetők, mivel konkrét technológiát érintő szabályozások nem állnak fent, csak a vizsgálati technikákat szabályozó rendelkezések lelhetők fel a jogi szabályozásban. Ezeken túlmenően még ott az Amerikai Egyesült Államok, amely egy akkora monopóliummal rendelkezik (pl. Alphabet, META, Amazon, Microsoft), hogy egységes szabályozása többenél több kérdést vet fel. Amíg a világ országai meghozzák részletesebbnél részletesebb szabályozásaikat, mindig ott lesznek az Amerikai Egyesült Államokban székhellyel rendelkező tech óriások, kikre a meghozott szabályozásokat nem tudják egységesen alkalmazni.

2.3 Hazai szakértők véleménye

A mélycsomag vizsgálat és a magánszféra kapcsolatában 15 kérdést tettem 3 különböző interjúalanynak. Kitértek anonimitását megtartva, „A” interjúalany egy adatvédelmi mérnök, „B” interjúalany egy adatvédelmi szakértő és oktató és a „C” interjúalany egy adatvédelmi jogász. A feltett kérdések a dolgozat 1. számú mellékeltét képezik. Az interjúalanyok kiválasztása során nagy hangsúlyt fektettem arra, hogy szakmabelieket kérdezzek, végzettségüket, munkaterületüket tekintve eltérő jelleggel, hogy egy átfogóbb képet kaphassak a feltett kérdésekhez fűződő válaszokból. A dolgozatban nem kerül megemlítésre minden kérdés, mivel az egyes válaszoknál az interjúalanyok érintettek egy másik kérdést is. Az első kérdésre, amely arról szólt, hogy a technológia által érheti – e fenyegetés a magánszférát, két hasonló és egy eltérő válasz érkezett. Amíg az „A” és a „C” interjúalanyok kibontották a

⁵⁶Telecoms Single Market: BEUC's key demands 3. cikk, In. The European Consumer Organisation, p. 13-14.2015.03.26., https://www.beuc.eu/publications/beuc-x-2015-028_gbe-telecom_single_market_trilogue-key_beuc_demands.pdf (Letöltés dátuma: 2022.02.25.)

különböző területek vélt fenyegetéseket, addig a „B” interjúalany a kérdés megválaszolását a GDPR-hoz kötötte. Szerinte, amennyiben biztosítva van a megfelelő jogszabályi háttér, a technológia alkalmazása elfogadható és információbiztonsági tevékenységként kerül végrehajtásra az alkalmazás, akkor elfogadható. Az „A” és „C” interjúalany hasonlóan kibontotta, hogy mely területeken hogyan jelenthet fenyegetést a DPI a magánszféra tekintetében. Az adatvédelmi mérnök a kérdést a mélycsomag vizsgálat alkalmazási területe felől, közelítette meg, amely szerint 3 irányból érkehetnek a fenyegetések. Internetszolgáltatók felől, nagyobb cégek a hivatali hálózatokon keresztül, és a komolyabb otthoni routereken vagy tűzfalakon keresztül. A két szakértő válaszában egyértelműen kifejtésre került, hogy a legfontosabb kérdés, hogy ki, mennyire elemzi a kinyert információkat és a megszerzett tudással mihez kezd. Válaszaikban kitértek, hogy a technológiának köszönhetően általános cselekedetek (filmezés, nagyobb fájlok megosztása, torrent) tudnak felhasználókhöz kötni, illetve ha az adatkezelő kellően hosszú ideig, megfelelő hálózati portokon történő információgyűjtés során, kellő számú apró csomag vizsgálatát elvégezve létrehozható az egyénről alkotott profil. Arra a kérdésre mely szerint a technológiáról honnan értesülnek az egyének egységes válasz érkezett, mely szerint burkoltan, az adatvédelmi tájékoztatók által értesülnek az egyének, hogy információbiztonsági szempontból az internetes forgalom megfigyelésre kerülhet. Mivel célzott profilozás nem történik, a technológia használatának célja nem az egyének viselkedésének elemzése, így a használt technológiák ismertetése sem szükséges. Az adat – és információbiztonsági szempontból az interjúalanyok szintén adekvát választ adtak. Szerintük nem lehet egyértelmű választ adni a kérdésre, hiszen sok változó tényező érinti a kérdést, mint a területi megoszlás, a betöltött munkakör és az egyének kora. A „C” interjúalany egészítette ezt a választ azzal ki, hogy a korból fakadóan a fiatalabb korosztály IT biztonságtudata magasabb, amíg az idősebb korosztály adatvédelmi tudatosága magasabb. Ez szintén a generációk közötti különbségekből vezethető le, mivel a fiatalabb generáció rendelkezik a megfelelő technológiai tudással, amíg az idősebb korosztály korukból fakadóan rendelkezik egyfajta tapasztalattal a magánszférájuk védelmének tekintetében. Arra a kérdésre, hogy kik jelentenek a legnagyobb veszélyt a technológia által megszerzett információk tükrében, mindenki a nagyvállalti közeget említette. Itt ugyanis, amennyiben az adatkezelők nincsenek megfelelően kontrolálva, elképzelhető olyan visszaélés, amely az egyének szabadságjogainak korlátozásához, személyes adataikkal való visszaéléshez vezethet. Ez tipikusan előfordulhat különböző pénzintézeteknél és távközlési szolgáltatóknál is, ahol a munkáltató a technológiai lehetőségeket a munkavállalók produktivitásának mérésére, tevékenységük figyelemmel kísérésére használhatják. A személyes adatok védelmére

vonatkozó kérdésnél az interjúalanyok hasonló választ adtak, mint az adat – és információbiztonság tudatosságánál, mely szerint nem lehet egy általános következtetést levonni. „C” csoportosította a tudatosságot 3 csoportba, amely központjában a viselkedés és a cselekvés korrelációja állt. Ezek szerint, az első csoportba tartoznak azon egyének, akiket érdekel, mi történik személyes adataikkal, a következő csoportba azok tartoznak, akiket érdekel és információkat is gyűjtenek a megelőzésre, amíg a harmadik csoportba tartoznak azok az egyének, akik nem csak utánanéznak a megoldási lehetőségeknek, hanem aktívan használják is azokat a gyakorlatban. Arra a kérdésre, amely a technológia által érintett célcsoportra volt kíváncsi, szintén hasonló válaszok érkeztek, mely szerint mindenki esett már át mélycsomag vizsgálaton, hiszen legális keretek között a hálózat forgalmának figyelésére is használhatják. Ezen kívül adott területen élő csoportok is eshetnek a technológia által megfigyelés alá. A technológia által megszerzett információk tekintetében is hasonló vélemények születtek. A válaszok között szerepelt a hálózat – és információbiztonság növelése, forgalomszabályozás, cenzúra, profilozás, adatelemzés, és cenzúra. A privátszférát erősítő technológiák közül a válaszadók ugyanazon technológiákat ajánlják, mint amelyeket ők is használnak. „A” fejtette ki bőven ő miket használ és ajánl másoknak is, mivel használatuk nem igényel sok technikai tudást. Ezek között szerepelt a biztonságos böngésző (Brave) és biztonságot növelő böngésző kiegészítő (uBlock) használata, jelszókezelő (KeePass) és VPN alkalmazása. Az utolsó két kérdésnél az aktuális jogszabályi háttérre kérdeztem rá, hogy mennyire tartják megfelelőnek, illetve ha lenne, lehetőségük miben változtatnának. A jogszabályi hátteret, mind a hazait mind a nemzetközi szabályozást kellően részletesnek gondolják az interjúalanyok. Szerintük a jogalkotók megfelelően próbálták a hálózatsemleges megoldásokat alkalmazni és elveket megfogalmazni, annak tekintetében, hogy az, a technológiáktól független problémákra is válaszul tudjon szolgálni. Arra kérdésre, amely lehetőséget teremtené, a jogszabályalkotás során meghatározni mire kellene nagyobb hangsúlyt fektetni. A különböző válaszokat elemezve elmondható, hogy az interjúalanyok munkakörüknek megfelelő válaszokkal válaszoltak a kérdésre. Az adatvédelmi mérnök az informatikai szakemberek jogszabályalkotási mechanizmusokba való bevonásának hiányosságát írta le, mivel szerinte a megfelelő szakértelem nélkül megfelelő és gyors választ, amely informatikailag kivitelezhető és betartható, a szakemberek nélkül nem lehetséges. Az adatvédelmi szakértő, aki oktatói tevékenységet is ellát, az új technológiák alkalmazását egy útmutatóba illesztené bele, amely segítséget nyújthatna a GDPR-nak való megfeleléshez, pontosítja, magyarázza és értelmezi az adott környezetben az adatvédelem megvalósulását. Az adatvédelmi jogász vázolta azon lehetőségeket, amelyekkel a tagállamok felügyeleti szervei élhetnek. Elmondása szerint a

jogalkotó, amikor egy életviszonyt szeretne, szabályozni mindig lemaradásban van, ezért törekszik a semlegességre és az elvi megfogalmazásokra, amelyek segítségével irányt tud mutatni a különböző alkalmazási területeknek. Továbbá elmondta, mivel a GDPR rendeleti szintű, így elsőbbséget élvez a tagállamokban. Ennek értelmében eltérő rendelkezéseket a nemzeti jogszabályok nem határozhatnak meg, azonban a GDPR, hogy többletgaranciákat vezethet be az állam egyes területeken. Ilyen a hazai Infotörvény is, amely 5. §-ban meghatározza a kötelező adatkezelés tartalmát, megőrzési idejét, ezzel is garanciális szabályokat teremtve.

Összességében elmondható, hogy az interjúalanyok a megválaszolt kérdések többségében egybehangzó véleményt fogalmaztak meg. A jogszabályi háttér, a privátszférát fenyegető technológiát ismertetése, az egyének digitális lábnyomának csökkentése érdekében fontosnak tekintik a társadalmi kommunikációt. Véleményük szerint a megfelelő jogszabályi háttér létezik, csak annak ismertetése szükséges akár már általános iskolától kezdve az idősebb generációkig.

3. Mélycsomag vizsgálat kockázatai

3.1 Mélycsomag vizsgálat és az állampolgárok kapcsolata

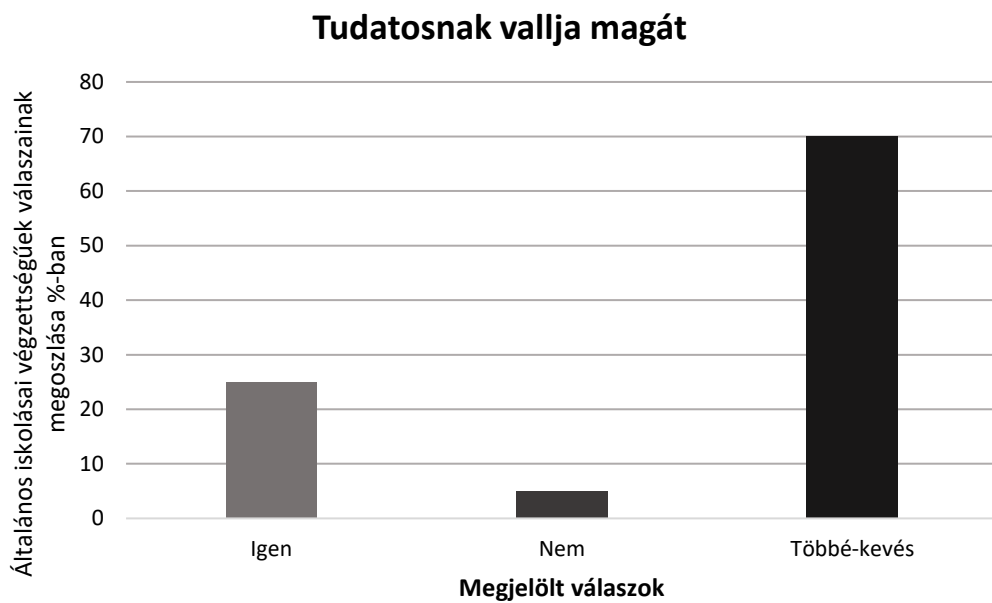
Kérdőíves kutatásom során arra kerestem a választ, hogy milyen a technológia és az állampolgárok közötti kapcsolat. Igyekeztem a kérdések közötti kapcsolatot feltárni és megvizsgálni a kapcsolatot a mélycsomag vizsgálat és az állampolgárok, valamint az állampolgárok és a biztonságtudat között. Továbbá a második hipotézisemre próbáltam választ találni, ami szerint az állampolgárok a technológia ismerete nélkül is feltételezik, hogy személyes adataikhoz juthat hozzá egy harmadik fél.

Először a hipotézisem vizsgálatával kezdem, amely során a kérdések közötti kapcsolatot is feltárom, valamint kitérek az állampolgárok és a biztonságtudat közötti kapcsolatra. Annak a vizsgálatával kezdtem, hogy a végzettség függvényében mennyire tekintik magukat a válaszadók tudatosnak. Az elemzés lefuttatását követően figyelmeztetést kapunk, ami szerint van olyan cella, ahol az elemszám kisebb, mint 5. A khi-négyzet próba szignifikanciája 1.0, így nem vethetjük el azt a feltételezést, hogy nincs kapcsolat a két változó között. (3. táblázat)

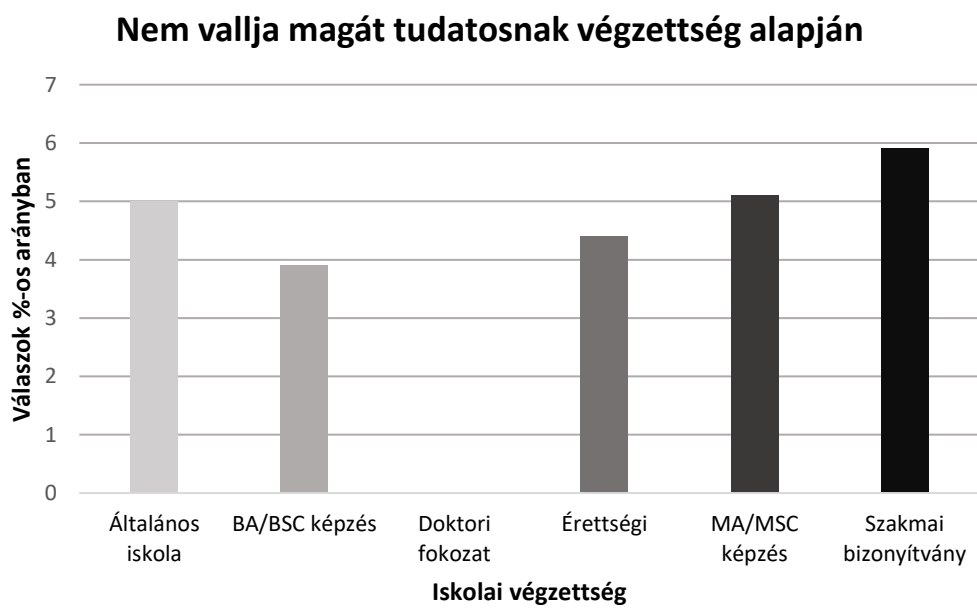
3. táblázat: Khi-négyzet próba az állampolgárok és a biztonságtudatuk közötti kapcsolat vizsgálatára

	Érték	Szabadságfok	Aszimptotikus szignifikancia (kétoldalú)
Pearson-féle khi négyzet	1.253	12	1.000
Valószínűségi arány	1.828	12	1.000
N érvényes eset	226		

A Cramer's V értéke 0,053. Az adatokból megállapítható, hogy az általános iskolát végzettek 70 százaléka többé kevésbé tudatos. Hasonló értékek vannak a többi végzettség esetén is. Igennel legnagyobb arányban a doktori fokozattal rendelkezők válaszoltak (28,6 %). A szakmai bizonyítvánnyal rendelkezők körében volt a legmagasabb azok aránya, akik a nemet jelölték meg (5,9 %). (lásd 53. oldal, 11. táblázat)



6. ábra: Kérdőív elemzés (saját szerkesztés, forrás: dolgozathoz készült kérdőív)



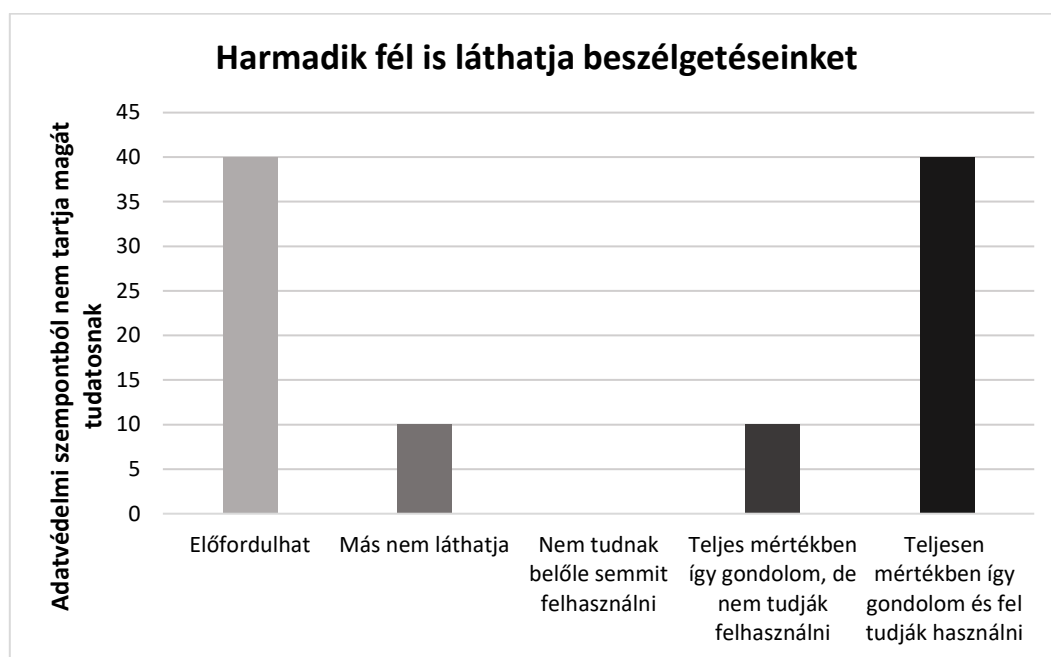
7. ábra: Kérdőív elemzés (saját szerkesztés, forrás: dolgozathoz készült kérdőív)

Hipotézisem bizonyítása során ezt követően a tudatosságot vettem össze a különböző kérdésekre adott válaszokkal. Először a tudatosság és privát beszélgetések láthatóságával foglalkozó kérdés közötti kapcsolatot vizsgáltam. Az elemzés elején itt is figyelmeztetést kapunk, ami szerint van olyan cella, ahol az elemszám kisebb, mint 5. A chí-négyzet próba szignifikanciája 0,369, így nem vethetjük el azt a feltételezést, hogy nincs kapcsolat a két változó között. (lásd 4. táblázat)

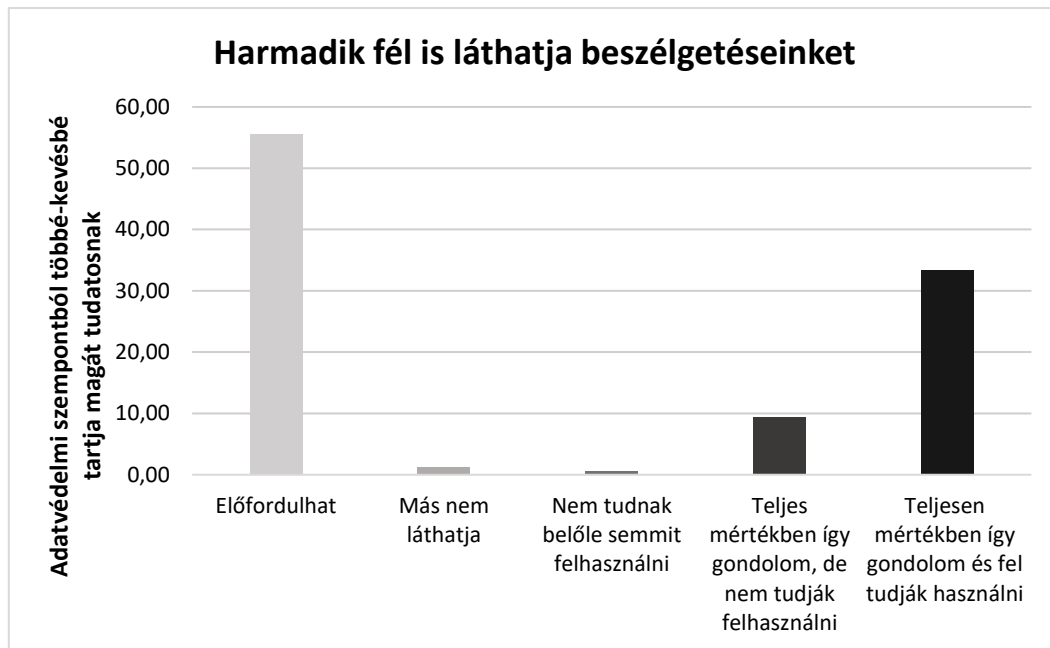
4. táblázat: Kí-négyzet próba a tudatosság és privát beszélgetések láthatóságának összehasonlításával (saját szerkesztés)

	Érték	Szabadságfok	Aszimptotikus szignifikancia (kétoldalú)
Pearson-féle kí négyzet	8.689	8	.369
Valószínűségi arány	7.679	8	.465
N érvényes eset	226		

A Cramer's V értéke 0,139. Először a tudatosak válaszait vizsgáltam. Közülük a legtöbben (42,6 %) úgy gondolják, hogy előfordulhat, hogy harmadik fél is látja a beszélgetéseket. 35,2 százalékuk véli úgy, hogy ez teljes mértékben így van és fel is tudják használni az adatokat ellenük. A többé-kevésbé tudatosak között magasabb azok aránya, akik bizonytalanok (55,6 %). Egyharmaduk azonban úgy véli, hogy ez teljes mértékben igaz és fel tudják használni ellenük az adatokat. A nem tudatosak körében már kicsit alacsonyabb azok aránya, aki szerint ez előfordulhat (40 %). 40 százalékuk azonban teljesen biztos benne és abban, hogy fel tudják használni ellene az információkat. (9., 10. ábra és 54. oldal 12. táblázat)



8. ábra Kérdőív elemzés (saját szerkesztés, forrás: dolgozathoz készült kérdőív)



9. ábra Kérdőív elemzés (saját szerkesztés, forrás: dolgozathoz készült kérdőív)

Úgy gondolom, hogy ezen adatokból jól látszik, hogy a válaszadók többé-kevésbé tudatosak az adataik biztonságát illetően, valamint nagyobb arányban gondolják úgy, hogy hozzá juthat harmadik fél is a beszélgetéseik, az adataikhoz, amit akár fel is tudnak használni ellenük. A hipotézisem azon része helytálló, hogy a válaszadók feltételezik a harmadik felet, viszont mivel azok aránya, akiknek ezzel a témával kapcsolatos végzettsége van alacsony (2,65 %), így a hipotézisem első fele is helytálló, hiszen majdnem a teljes mintában szereplő egyének végzettségüket tekintve nem ismerhetik a technológia működését.

A következőkben a mélycsomag vizsgálattal kapcsolatos válaszokat igyekszem bemutatni. Először összevettem azt a tényt, hogy hallottak e róla vagy sem azzal, hogy mit gondolnak, mire használhatják a mélycsomag vizsgálatot. A mire használhatják kérdésnél a következő opciók voltak megadva és egyszerre többet is ki tudtak választani a kitöltők:

- Személyre szabott hirdetések megjelenítésében
- Titkos szolgálati kommunikációs csatorna
- Illegális fájlmegosztás leleplezése
- Politikai ellenfelek ellehetetlenítése (pl. cenzúra)
- Bűncselekmények előrejelzése
- Emberek személyi vagyonának felderítése

Az adatok alapján a lehetséges válaszokat egyesével vettem össze azzal, hogy ismerték e már a mélycsomag vizsgálatot. Először a személyre szabott hirdetések és a halott e már róla kérdésekre adott válaszok közötti kapcsolatot vizsgáltam. Az elemzés elején itt is figyelmeztetést kapunk, ami szerint van olyan cella, ahol az elemszám kisebb, mint 5. A khi-négyzet próba szignifikanciája 0,092, így nem vethetjük el azt a feltételezést, hogy nincs kapcsolat a két változó között. (lásd 5. táblázat)

5. táblázat: Khi-négyzet próba a technológia ismerete és a személyre szabott hirdetések összevetésével (saját szerkesztés)

	Érték	Szabadságfok	Aszimptotikus szignifikancia (kétoldalú)
Pearson-féle khi négyzet	4.764	2	.092
Valószínűségi arány	5.505	2	.064
N érvényes eset	226		

A Cramer's V értéke 0,145. Azok közül, akik hallottak róla 89, 3 százalékuk véli úgy, hogy a személyre szabott hirdetések megjelenítésében játszik szerepet. Hasonlóan magas azok aránya is, akik nem vagy nem tudják, hogy ismerik- e a mélycsomag vizsgálatot. Az előbbi 71,6 százaléka, mg az utóbbi 87,5 százaléka jelölte meg ezt a lehetőséget a válaszok közül.

A titkosszolgálati kommunikációs csatorna esetében szintén kapunk figyelmeztetést, hogy vannak olyan cellák, ahol az elemszám kisebb, mint öt. A khi-négyzet próba szignifikanciája 0,184, így nem vethetjük el azt a feltételezést, hogy nincs kapcsolat a két változó között. (lásd 6. táblázat)

6. táblázat: Khí négyzet próba a technológia ismerete és technológia felhasználása vonatkozásában (saját szerkesztés)

	Érték	Szabadságfok	Aszimptotikus szignifikancia (kétoldalú)
Pearson-féle khí négyzet	3.382	2	.184
Valószínűségi arány	3.323	2	.190
N érvényes eset	226		

A Cramer's V értéke 0,122. Az arányok a korábbihoz képest megfordultak. Összességében a többség úgy gondolja, hogy ez nem igaz állítás. Akik hallottak róla azoknak a többsége (57,1 %) úgy hiszi, hogy igaz. Ezzel szemben azok, akik nem tudják, hogy hallottak-e róla (62,5 %) vagy biztosan nem hallottak róla (61,1 %) inkább gondolják úgy, hogy erre nem használják a mélycsomag vizsgálatot.

A bűncselekmények előrejelzésével kapcsolatban ugyanúgy figyelmeztetést kapunk, ami szerint van olyan cella, ahol az elemszám kisebb, mint 5. A khí-négyzet próba szignifikanciája 0,006, így elvethetjük azt a feltételezést, hogy nincs kapcsolat a két változó között. A Cramer's V értéke 0,213. A válaszadók többsége igaznak gondolja, hogy erre használják a mélycsomag vizsgálatot. Akik tudják, miről van szó, azok 85,7 százaléka gondolja így. Ezzel szemben, akik biztosan nem hallottak még róla azok közül pusztán 55,3 %, míg, akik nem tudják, hogy hallottak-e róla, azok kétharmada gondolja így.

Az illegális fájlmegosztás leleplezésénél szintén megkapjuk a figyelmeztetést az alacsony elemszámú cellákkal kapcsolatban. A khí-négyzet próba szignifikanciája 0,188, így nem vethetjük el azt a feltételezést, hogy nincs kapcsolat a két változó között. A Cramer's V értéke 0,122. Ezt az állítást összességében hamisnak gondolják a válaszadók. Akik ismerik a mélycsomag vizsgálatot, azoknak 57,1 százaléka gondolja ezt igaznak, míg, akik biztosan nem ismerik, azoknak 60,5 százaléka gondolja hamisnak és a bizonytalanok fele-fele gondolja igaznak vagy hamisnak.

A politikai ellenfelek ellehetetlenítése esetén a már korábbiakban is jelzett figyelmeztetést megkapjuk. A khí-négyzet próba szignifikanciája kisebb, mint 0,001, így elvethetjük azt a feltételezést, hogy nincs kapcsolat a két változó között. A Cramer's V értéke 0,257. Összesítve az adatokat, ezt az állítást hamisnak tartják. Akik tudják (67,9 %) és a bizonytalanok többsége (62,5 %) igaznak tartja, míg, akik nem tudják (67,4 %) a mélycsomag vizsgálatot, azok hamisnak tartják az állítást.

Az emberek személyi vagyonának felderítésével kapcsolatos vizsgálat során a figyelmeztetés ugyanúgy megjelent az elemszámra vonatkozóan. A khí-négyzet próba szignifikanciája kisebb, mint 0,001, így elvethetjük azt a feltételezést, hogy nincs kapcsolat a két változó között. A Cramer's V értéke 0,314. Összességében ezt az állítást is hamisnak tartják. Akik ismerik, azoknak a 67,9 százaléka tartja igaznak, míg a nem ismerők (75,8 %) és a bizonytalanok jelentős része (62,5 %) az ellenkezőjét gondolja.

Úgy vélem, hogy ezek az összefüggések jól megmutatják, hogy az emberek mit gondolnak a mélycsomag vizsgálat funkciójáról. Akik azt állítják, hogy tudják, kiről van szó, azok általában egyetértenek az állítással, míg, akik nem ismerik, azok közül már többen vannak, akik hamisnak gondolják némelyiket.

3.2 A fenyegetettség bemutatása

A fenyegetettség egy kitalált szituáció által kerül bemutatásra kockázati mátrix alkalmazásával⁵⁷. A választott módszer kiválasztása során figyelembe vettem, hogy a mélycsomag vizsgálat témakörében egy vagy több kockázati tényező meghatározása nehéz, mivel a bekövetkezés valószínűsége és a kifejtett hatás szorzatának meghatározása bonyolult. Példaként lehet említeni egy pénzügyi szektorban dolgozó, magas státuszú pozícióban foglalkoztatott személy könnyebben eshet a technológia vizsgálat alá, mint egy banki telefonos ügyintéző, mivel bizalmasabb információk birtokában van, amely kiszivárogtatása komoly kockázatot jelenthet az adott vállalat számára. A kockázatelemzéshez az alábbi szituációt állítottam fel:

Pénzes Dezső a Pénzfaktor Zrt-ben tölt be szakterületi vezetői pozíciót. Munkaköréből fakadóan a szervezet organogramjában a vezérigazgató alatt foglal helyet, saját szakterületéért felel, a vezetőség tagja és szervezetet érintő döntések meghozatalában részt vesz, a céget érintő szenzitív adatok birtokában van. Egy munkanapján kap egy e-mailt, melyben a vezérigazgató keresi sürgős ügyben. A beszélgetés témájául az szolgált, hogy Pénzes Dezső a munkaidejében egy közösségi platformon nagyobb fájlát osztott meg. Pénzes Dezső elmondta, hogy magánjellegű beszélgetést folytatott nejével, mely során az ingatlanvásárláshoz küldött át dokumentumokat neki.

A következőkben két táblázat segítségével leírásra kerül, hogy a megadott munkakörnyezetben mekkora valószínűséggel mi történhet a munkavállalóval (lásd 7. táblázat) és a bekövetkező

⁵⁷ A fenyegetettség bemutatásának alapjául Erick Galante – Daniele Bordalo – Marcelle Nobrega: Risk Assessment Methodology: Quantitative HazOp, Journal of Social Engineering, 3. (2014), 2. 31-36.

eseményeknek mekkora kockázati súlyossága van, mekkora kár keletkezhet az egyén magánszférájában (8. táblázat)

7. táblázat: Valószínűségi események – (saját szerkesztés, forrás: Erick Gaalnte)

Valószínűség		Leírás
1	Szinte biztos, hogy nem	A fenyegetés nem értelmezhető, így nem sérül az érintett személyes jogai, és nem keletkezik nem vagyoni kár.
2	Valószínűtlen	A mélycsomag vizsgálat által kinyert információ nem sérti az egyén személyes jogait, és nem keletkezik nem vagyoni kára.
3	Lehetséges	A mélycsomag vizsgálat által kinyert információ vagy az egyén személyes jogait sérti vagy nem vagyoni kára keletkezik.
4	Valószínű	A mélycsomag vizsgálat által kinyert információ az egyén személyes jogait védi, vagy vagyoni kára keletkezik.
5	Gyakori	A mélycsomag vizsgálat által kinyert információ sérti az egyén személyes jogait és nem anyagi kára keletkezik.

8. táblázat: Súlyossági következmények (saját szerkesztés, forrás: Erick Gaalnte)

Súlyosság		Leírás
A	Minimális	Nem sérül a magánszféra a technológia alkalmazása során.
B	Kicsi	A munkavállaló tudatában van, annak, hogy milyen technológiák vizsgálata alá eshet munkavégzése során.
C	Jelentős	A munkavállalók a technológia által megfigyelés alá kerülnek, de az ellenőrzött csomagokat nem használják fel profilalkotásra.
D	Kockázatos	A munkavállalók tevékenysége profilozásra kerül, de az általuk kialakított képre nem írnak elő retorziókat.
E	Óriási	A munkavállalók tevékenysége profilozásra kerül, és az így kialakított képre retorziókat írnak elő.

A két táblázat megfelelő értékeinek szorzatából jön létre a kockázatértékelési mátrix:

9. táblázat: Kockázatértékelés mátrix (saját szerkesztés, forrás: Erick Gaalnte)

Kockázat valószínűsége	5	5A	5B	5C	5D	5E
	4	4A	4B	4C	4D	4E
	3	3A	3B	3C	3D	3E
	2	2A	2B	2C	2D	2E
	1	1A	1B	1C	1D	1E
		A	B	C	D	E
		Kockázat súlyossága				

A 9. táblázat alapján a következőképpen alakult a színek megadása:

A vörös szín az elfogadhatatlan kockázati valószínűséget és súlyosságot jelöl. A megoldás érdekében jelentős változásokra van szükség szervezeten belül és a változások teljesülését követően új kockázatelemzést kell végezni, hogy ezen valószínűségi vagy súlyossági változó enyhítésre vagy megszüntetésre kerüljön.

A narancssárga szín az elfogadható, de változásokat igénylő kockázatokat jelöl. A javulás érdekében új intézkedések bevezetése vagy szervezeti jóváhagyás szükséges.

A zöld szín az elfogadható kockázatokat jelöli, Ezekben az esetekben a kockázat valószínűsége vagy súlyossága aggodalomra nem ad okot.

10. táblázat: Kockázatkezelési mátrix lehetséges kezelése (saját szerkesztés, forrás: Erick Gaalnte)

			Kockázatértékelés			
Kiváltó ok	Kiváltó ok kategóriája	Lehetséges következmény	Valószínűség	Súlyosság	Táblázati azonosító	Kockázati szint
Mélycsomag ellenőrzés alkalmazása	Adatvédelmi	Pillanatkép a munkavállaló cselekedetének lehetőségéről	Valószínű	Kicsi	4B	Elfogadható, de változásokat igénylő
Munkavállaló célzott, huzamosabb ideig történő megfigyelése	Adatvédelmi	Munkahelyi elbocsátás	Gyakori	Óriási	5E	Elfogadhatatlan

A kockázatértékelés befejezését enyhítő intézkedéseket kell megfogalmazni, amelyhez hozzá kell rendelni egy felelős személyt (lásd 10. táblázat). Mivel a technológia alkalmazását az egyének nem érzékelik, és minden esetben adatvédelmi probléma merülhet fel, így a legmegfelelőbb szakember a szervezeten belüli adatvédelmi szakértő. Az ő feladatkörébe tartozna a megfelelő adatvédelmi tájékoztató kialakítása melyben szerepel, hogy a munkáltató információbiztonsági szempontból megfigyelheti a munkavállalók internetes forgalmát és ennek technikai módjára és technikai részleteire is kitér. Ezen felül felügyelné, a megfelelő jogi szabályozás betartását, melynek következtében a munkavállalók profilozása nem történhet meg.

A választott módszertől eltekintve elmondható, hogy a magánszféra megsértése az internetes mélycsomag vizsgálat tükrében bonyolult. A technológia alkalmazásáról az érintettek ugyanis nem értesülnek, így az őket fenyegető kockázatok megállapítása nem lehet pontos, illetve nincs egy egységsugarú, általánosítható megfigyelt, hiszen a technológia alkalmazása, a korábban leírtakkal összhangban, történhet nagyobb vállalatok, egyes régióban élő személyek vonatkozásában is. Összességében elmondható, hogy a technológiában rejlő kockázatok attól függenek, hogy kik alkalmazzák, mire alkalmazzák a kinyert információkat és miért alkalmazzák a technológiát.

3.3 Megoldási lehetőségek

A titkosítás nélküli kommunikáció esetén a megfigyelési technikák könnyen alkalmazhatóvá válnak. Az egyik legegyszerűbb védekezési módszer a kommunikáció tartalmának titkosítása, amely által a mélycsomag ellenérzést végző személy feladata megnehezedik, de akár az általa ellenőrizni kívánt kommunikációt nem is tudja vizsgálni. Ilyen szoftver például a HTTPS Everywhere⁵⁸, amely egy ingyenesen telepíthető bővítmény, mely telepíthető Chrome, Firefox vagy akár Opera böngészőnkbe is.⁵⁹ Ez a technológiai megoldás azonban mára, már nem a leghasznosabb. A weboldalak URL-sémája már majdnem minden esetben https-sel kezdődik. Ez, egyfajta biztonságot jelenthet az egyének számára, hogy ne kelljen azzal foglalkozniuk, mikor szerepel a titkosító réteg az URL-sémában. Egy másik megelőzési mód lehet a Virtual Private Network (továbbiakban: VPN) használata. A VPN csatlakozáskor a felhasználó által használt internetforgalom titkosításra kerül, így a felhasználók által felkeresett weboldalakhoz nem tudják a személyeket hozzákapcsolni. Rengeteg előnnyel jár még a VPN használata (mint például régióspecifikus weboldalak elérése), de a mélycsomag ellenőrzés némely esetben legyőzheti a titkosítást, a specifikus „VPN-csomagokra” való rászűréssel de ezáltal a felkeresett oldalt maximum letiltásra kerülhet, feltörni vagy a felkeresett oldal tartalmába belenézni nem fognak tudni. A minél biztonságosabb titkosítás érdekében a felhasználók számára ajánlott a DNS-kiszolgáló módosításával együtt elvégzett VPN titkosítást használata.⁶⁰

Egy harmadik megoldási lehetőség a The Onion Router (továbbiakban: TOR) böngésző alkalmazása. A TOR lehetővé teszi az a felhasználó anonim jelenlétét, ezzel is védve személyes adatainkat, illetve lehetővé teszi a cenzúrázott weboldalak elérését.⁶¹ 2012-ben a „TOR anonimitás projekt” keretében segítettek az iráni állampolgároknak, hogy a kormány által cenzúrázott internetes tartalmakat elérjék.⁶² A TOR Projekt célja, hogy egyfajta „hagymaelvnek” köszönhetően biztosítsa a felhasználók számára az internet oly módon történő

⁵⁸ HTTPS Everywhere In. Electronic Frontier Foundation, <https://www.eff.org/am/https-everywhere> (Letöltés dátuma: 2022.02.04.)

⁵⁹ Kovács 2016. i.m. p. 134. .

⁶⁰SB: Does a VPN Protect You Against Deep Packet Inspection by ISPs? In. Security Bind, <https://www.securitybind.com/does-a-vpn-protect-against-deep-packet-inspection-by-isps/> (Letöltés dátuma: 2022.03.08.)

⁶¹ Tor szoftver, In. Wikipédia, 2021.12.19., [https://hu.wikipedia.org/wiki/Tor_\(szoftver\)](https://hu.wikipedia.org/wiki/Tor_(szoftver)) (Letöltés dátuma: 2022.01.08.)

⁶² Moyer, Edward: Tor anonymity project looks to help Iranians sidestep Net ban, In. Cnet, 2012.02.10., <https://www.cnet.com/tech/tech-industry/tor-anonymity-project-looks-to-help-iranians-sidestep-net-ban/> (Letöltés dátuma: 2022.02.10.)

használatát ingyenesen, amely által nem sérülnek személyes adataik, nem történik meg a felhasználók profilozása és többek között törlődnek a cookiek is.⁶³

Amennyiben globálisabb módon, az internetes lábnyomunkat minimalizáljuk, nem csak a mélycsomag vizsgálattól, de a külön fajta internetes visszaélésektől is meg tudjuk magunkat védeni (profilozás, személyre szabott hirdetések). Egyik ilyen lehetőség a privátszférát erősítő technológiák (továbbiakban: PET)⁶⁴ alkalmazása a privátszféránk és az adatvédelmünk megóvása érdekében.

A fogalom meghatározása alatt a személyazonosság technikai és szervezeti megoldásait, az egyén identitásának megőrzését értjük.⁶⁵ Mivel a PET-nek rendkívül sok alkalmazási lehetősége van, Ian Goldberg tipológiája segítségével részletezem a megvalósulási formákat.

Az első csoportba tartoznak azok a technológiai megoldások, amelyek segítenek az egyén anonimitását előidézni az internetes kommunikáció során. Ilyen lehetőség a „Remailerek”⁶⁶ és a pszeudoanonimitást⁶⁷ lehetővé tevő rendszerek. Továbbá ebbe a csoportba sorolható a fentebb említett Tor-projekt is.

A második csoportba az online kommunikáció során átvitt tartalmak titkosítással védő technológiák tartoznak (például: PipeNet; Anonymizer.com)⁶⁸ A harmadik csoportba pedig azokat a PET eszközöket sorolja, amelyek lehetővé teszi a biztonságos online fizetést, és segít elkerülni a cenzúrát és az adathalászatot. (például Cloudmark Anti-Fraud Toolbar, Google’s Safe Browsing toolbar)⁶⁹; ⁷⁰

Egy másik, magánszférát megerősítő mód, egy filozófiai megközelítés, a Privacy by Design elv, amely Ann Cavoukian munkásságának köszönhető. A kifejezés jelentése beépített adatvédelem, amely alapján a magánszféra védelmét szolgáló szempontokat a különböző technológiai követelményrendszerekbe kell beleilleszteni. Ezzel kapcsolatban 7 alapelv került kidolgozásra. Ezekből a dolgozat témáját tekintve a legfontosabbakat emeltem ki.

⁶³ Torproject In. Torproject, <https://www.torproject.org/> (Letöltés dátuma: 2022.02.10.)

⁶⁴ Ian Goldberg: Privacy Enhancing Technologies for the Internet III: Ten Years Later University of Waterloo, Waterloo, ON, 2007. 14. p.

⁶⁵ Dr. Szőke Gergely László : Adatvédelem és Önszabályozás. Adatvédelmi irányítási rendszer az adatkezelőknél , doktori értekezés, Pécsi Tudomány Egyetem Állam – és Jogtudományi Kar Doktori Iskola, Pécs, 2014., p. 101.

⁶⁶ lehetővé teszi az üzenetek tartalmának, az üzenetváltások időpontjának, sorrendjének, gyakoriságának és terjedelmének elfedését; Adatvédelem és információ szabadság - Adatvédelem és információszabadság in. VikWiki, 2016. p.2., https://vik.wiki/images/e/eb/Adatvedelem_jegyzet_2016_lm.pdf (Letöltés dátuma: 2022.02.10.)

⁶⁷ „van alanya az adatoknak, de az alany valós kilétét nem ismerjük; egy valós adatalanynak több fedőneve, profilja, virtuális személyisége is lehet” –Balogh el. al.: Technológia a jog szolgálatában? – Kísérletek az adatvédelem területén ,Pro Futuro 2014. évfolyam 1. szám. 2014. p. 37.

⁶⁸ Goldberg 2007 i.m., p. 5.

⁶⁹ Dr. Szőke 2014. i.m., p. 102.

⁷⁰ Goldberg 2007 i.m., p. 10.

Az első alapelvben a megelőzésre fókuszálnak, mely szerint az utólagos megoldások helyett megelőző cselekedeteket kell kidolgozni. A második alapelv a beépített, alapértelmezett adatvédelemről szól, amely a felhasználó aktív részvétel nélkül elősegíti a magánszféra védelmét. A hatodik alapelvben kerül megemlíetésre a láthatóság és az átláthatóság, amely olyan adatkezelési műveletek foglal magába, amely alapján mind a szolgáltató mind a felhasználó számára is átlátható. Az utolsó alapelv szól a felhasználó magánszférájának tiszteletben tartásáról, amely megköveteli az adatkezelők számára azt, hogy az ő szempontjaik szerint is első helyen szerepeljen az érintettek adatvédelmi érdekei.⁷¹

Ahogy a fent leírtakból is látszik, a technológia okozta fenyegetésektől és a magánszféránk védelmét szolgáló technológiákból is van lehetőségünk a választásra. Természetesen, ahogy a leírtakban is bemutatásra került, mindegyik technológiának, elvnek megvan a hiátusai, amely alapján a 100 %-os védelem nem garantálható. Egy másik akadályozó tényező az állampolgárok ismerethiánya, mivel a fenyegetések létezéséről tudnak, de a megelőzési technológiákat, technikákat nem ismerik.

⁷¹ Dr. Szőke 2014. i.m., p. 102.

Eredmények

A kutatás során felállított hipotézisek közül kettő beigazolódott és egy megcáfolásra került. A H1-es hipotézis, mely szerint az adatvédelmi szakértők és jogászok szerint a hazai és nemzetközi jogi szabályozás hiátusokat tartalmaz a mélycsomag vizsgálatot illetően nem igazolódott be. A dolgozatban kifejtésre került, hogy az interjú során a megkérdezettek egybehangzóan úgy nyilatkoztak, hogy a technológiát illetően részletes hazai és nemzetközi szabályozással rendelkezünk, csak annak ismerete hiányzik a társadalmi rétegekből.

A H2-es hipotézis, mely szerint az állampolgárok a technológia ismerete nélkül is feltételezik, hogy személyes adataikhoz juthat hozzá egy harmadik fél, beigazolódott, mivel a kérdőív kitöltését szolgáló egyének többsége nem rendelkezett ismerettel a technológiát érintőleg, mégis feltételezte, hogy személyes adataik nincsenek biztonságban.

A H3-as hipotézis, mely feltételezi, illetve, hogy a technológia magán és vállalati célú felhasználása kiemelet kockázatot jelent a magánszféra megsértésével kapcsolatban részben beigazolódott, mivel a technológia felhasználása sérti az egyének magánszféráját, ugyanakkor, a technológia piaci ára nem teszi lehetővé az internetes mélycsomag vizsgálat magencélú használatát.

Összefoglalás

Összességében elmondható, hogy az internetes mélycsomag vizsgálat használata számos előnnyel, ugyanakkor számos hátránnyal is járhat. A dolgozat vázát adó témakör, melyben a magánszféra és mélycsomag vizsgálat kapcsolata került elemzésre, sok kérdésre adott választ. Többek között a felállított hipotézisek igazolása és megcáfolása illetve, hogy fontos az újabb, kevésbé ismert informatikai technológiák ismertetése az állampolgárokkal. A dolgozat során számos témakörben, mind a kérdőív, mind az interjúk, mind a jogszabályozási hátterek elemzése megmutatta, hogy az állampolgárokkal fontos a kommunikáció. Fontos beszélni az őket megillető jogokról és jogorvoslati lehetőségekről, illetve azokról a technológiákról amelyekkel közvetlenül vagy közvetett módon találkozhatnak. Véleményem szerint a megfelelő tudás birtoklásában, és az állampolgárokból kialakított aktív cselekvési kényszer alapján elérhető, hogy egy olyan közösséget alakítsunk ki, akik figyelnek a digitális lábnyomuk nagyságára és megtesznek mindent a magánszférájuk megőrzésének érdekében. Ezen tudások birtokában nem szükséges részükre a legaktuálisabb informatikai technológiák ismerete, elég csupán a megfelelő védekezést felállítani.

Hivatkozások

Dobák Imre: Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében, In Hadmérnök, 7. évfolyam 2. szám, 2017

Erick Galante – Danielle Bordalo – Marcele Norbega: Risk Assessment Methodology: Quantitative HazOp, Journal of Safety Engineering, 3. (2014.) 2.

Finn, el. al. : Seven Types of Privacy . In European Data Protection. Coming of Age? New York – London, 2012.10.12.

Hankó Viktória: A drónokkal kapcsolatos kockázatok és kezelési lehetőségeik In. Hadmérnök 16. évfolyam 3. száma 2021

Ian Goldberg: Privacy Enhancing Technologies for the Internet III: Ten Years Later University of Waterloo, Waterloo, ON, 2007

Kovács Zoltán: Biztonság vs. törvényes ellenőrzés az internet alapú kommunikációban – Ellentétes vagy egymással megférő követelményeknek? I. In. Hadmérnök 6. évfolyam. 4. szám , 2016

Krasznay Csaba: A magyar elektronikus közigazgatási alkalmazások információbiztonsági megoldásai, Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Kar Katonai Műszaki Doktori I, Budapest, 2011

Mógor Tamásné - Az emberi tényező szerepe az információbiztonság megvalósítása és erősítése terén. Az információbiztonsági kultúra fejlesztésének lehetőségei a Magyar Honvédségben - Biztonságtudományi Doktori Iskola, Budapest, 2017

Nagy Renáta - Dr. Sziklay Júlia: A GDPR Egyszerűen Kis- és Középvállalkozások Számára, Magyar Közlöny Lap- És Könyvkiadó Kft, Budapest, 2020

Parra el. al. : Legal assessment of DPI in telecommunication networks in Columbia, IEEE, London, 2014

Puskás Tivadar Közalapítvány: Internet Biztonsági Tanulmány, Az Internet Szerepének Gyors Növekedésében Rejlő Pénzügyi Visszaélésekkel Kapcsolatos Kockázatok, 2009. szeptember

Snowden, Edward: Rendszerhiba, 21. Század Kiadó, 2019. szeptember 17.

Solove, Daniel J.: Understanding Privacy, Cambridge, MA_London, Haarward University Press, 2008

Székely el. al.: Biztonság és magánélet Az alkumodell megkérdőjelezése és meghaladása, In. Replika 2017. évfolyam 3. szám , 2017

Sziklay Júlia - Bendik Tamás: Az adatvédelem hazai és európai uniós szabályozása és alapintézményei,NKE, Budapest, 2018, Budapest,

Törley Gábor: Informatikai Biztonságtudatosság , ELTE Informatikai Kar, Budapest, 2019

Az Európai Parlament És A Tanács (Eu) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról Magyarország Alaptörvénye, 2011.

Congresso de Colombia, Ley estatutaria 1581 de 2012. Colombia, 2012.

Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv)

Asamblea Nacional Constituyente, Artículo 15, Constitucion Politica De Colombia Colombia, 1991

Adatvédelem és információ szabadság - Adatvédelem és információszabadság in. VikWiki, 2016, https://vik.wiki/images/e/eb/Adatvedelem_jegyzet_2016_lm.pdf (Letöltés dátuma: 2022.02.10.)

Az Európai Gazdasági Térség tagállamai In. Konzuli Szolgálat, <https://konzuliszolgalat.kormany.hu/egt-tagallamok> (Letöltés dátuma: 2022.03.10.)

Az internet hazai megjelenése In. Médiatudományi Intézet, 2015. július 17. https://nmhh.hu/cikk/192602/Az_internet_hazai_megjelenese (Letöltés dátuma 2022.01.30.)

Bamman, D. - O'Connor, B. - Smith, N: 'Censorship and deletion practices in Chinese social media',In. First Monday, 2012.03.04., <https://journals.uic.edu/ojs/index.php/fm/article/view/3943> (Letöltés dátuma: 2021.12.03.)

Chris Brook: What is deep packet inspection? How it works, use cases for dpi, and more, In. Digital Guardian, 2018.12.05., <https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more> (Letöltés dátuma 2021.03.25.)

Dr. Kirstie Ball: Megfigyelés, magánszféra és biztonság – Mi az Ön véleménye? In. Surprise Project, 2014.04. <http://surprise-project.eu/wp->

content/uploads/2014/04/B7_Median_Information_Magazine_Hungarian.pdf (Letöltés dátuma 2022.03.08.)

Európai Adatvédelmi Biztos 2004-2014-ig In. European Data Protection Supervisor, Wikipedia 2022.02.07, https://en.wikipedia.org/wiki/European_Data_Protection_Supervisor (Letöltés dátuma 2022.03.02.)

HTTPS Everywhere In. Electronic Frontier Foundation, <https://www.eff.org/am/https-everywhere> (Letöltés dátuma: 2022.02.04.)

Hustinx, Peter: Az európai adatvédelmi biztos véleménye a hálózatsemlegességről, a forgalomkezelésről, valamint a magánélet és a személyes adatok védelméről In. Az Európai Unió Hivatalos Lapja, 2012.02.08., [https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52012XX0208\(01\)&from=FR](https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52012XX0208(01)&from=FR) (Letöltés dátuma : 2022.03.08.)

King et. al.: How Censorship in China Allows Government Criticism but Silences Collective Expression In. American Political Science Review, 2013.05., <https://gking.harvard.edu/publications/how-censorship-china-allows-government-criticism-silences-collective-expression> (Letöltés dátuma 2021.12.03.)

Malware In. Kiberbiztonsági Fogalomtár, <https://makay.net/kiberbiztonsagi-fogalomtar> (Letöltés dátuma: 2021. 03. 25.)

Meaning of surveillance in English In. Cambridge Dictionary, 2022, <https://dictionary.cambridge.org/dictionary/english/surveillance> (Letöltés dátuma: 2022.03.08.)

Moyer, Edward: Tor anonymity project looks to help Iranians sidestep Net ban, In. Cnet, 2012.02.10., <https://www.cnet.com/tech/tech-industry/tor-anonymity-project-looks-to-help-iranians-sidestep-net-ban/> (Letöltés dátuma: 2022.02.10.)

Router, In. MiMi. <https://www.mimi.hu/informatika/router.html> (Letöltés dátuma: 2021. április 4.)

SB: Does a VPN Protect You Against Deep Packet Inspection by ISPs? In. Security Bind, <https://www.securitybind.com/does-a-vpn-protect-against-deep-packet-inspection-by-isps/> (Letöltés dátuma: 2022.03.08.)

Snapshot of Xi on making Internet an interconnected world In. China Daily Online, 2015.12.11., https://usa.chinadaily.com.cn/2015-12/11/content_22693550_4.htm (Letöltés dátuma: 2021.12.03.)

Telecoms Single Market: BEUC's key demands 3. cikk, In. The European Consumer Organisation, p. 13-14.2015.03.26., https://www.beuc.eu/publications/beuc-x-2015-028_gbe-telecom_single_market_trilogue-key_beuc_demands.pdf (Letöltés dátuma: 2022.02.25.)

Tor szoftver, In. Wikipédia, 2021.12.19., [https://hu.wikipedia.org/wiki/Tor_\(szoftver\)](https://hu.wikipedia.org/wiki/Tor_(szoftver)) (Letöltés dátuma: 2022.01.08.)

Torproject In. Torproject, <https://www.torproject.org/> (Letöltés dátuma: 2022.02.10.)

Táblázatok jegyzéke

1. táblázat Az internetes mélycsomag vizsgálat pozitív és negatív aspektusai (saját szerkesztés, forrás: Preparation of Papers on a Survey on Network Data Collection)	15
2. táblázat Az internetes mélycsomag vizsgálat felhasználási formái (saját szerkesztés, forrás: Ibrahim, Ahmad)	19
3. táblázat Khí-négyzet próba az állampolgárok és a biztonság tudatuk közötti kapcsolat vizsgálatára.....	32
4. táblázat Khí-négyzet próba a tudatosság és privát beszélgetések láthatóságának összehasonlításával (saját szerkesztés).....	35
5. táblázat Khí-négyzet próba a technológia ismerete és a személyre szabott hirdetések összevetésével (saját szerkesztés)	37
6. táblázat Khí négyzet próba a technológia ismerete és technológia felhasználása vonatkozásában (saját szerkesztés)	38
7. táblázat Valószínűségi események – (saját szerkesztés, forrás: Erick Gaalnte).....	40
8. táblázat Súlyossági következmények (saját szerkesztés, forrás: Erick Gaalnte).....	41
9. táblázat Kockázatértékelés mátrix (saját szerkesztés, forrás: Erick Gaalnte)	41
10. táblázat Kockázatkezelési mátrix lehetséges kezelése (saját szerkesztés, forrás: Erick Gaalnte)	42
11. táblázat Keresztábra vizsgálat a tudatosság és az iskolai végzettség függvényében (saját szerkesztés).....	53
12. táblázat Keresztábra a tudatosság és a feltételezés között (saját szerkesztés).....	54

Ábrák jegyzéke

1. ábra A magánszféra dimenziói (saját szerkesztés, forrás: Koops at. al)	9
2. ábra Az internetes felszíni - és mélycsomag vizsgálat közötti különbség (saját szerkesztés, forrás: SurPRISE Research)	13
3. ábra Az internetes mélycsomag vizsgálat használata (saját szerkesztés, forrás: SurPRISE Research).....	16
4. ábra Az adatszerző és a célszemély távolsága (Kovács Zoltán)	16
5. ábra DPI által végezhető azonosítás típusai (saját szerkesztés, forrás: An Approach for Detecting Man-In-The-Middle Attack Using DPI and DFI).....	17
6. ábra Kérdőív elemzés (saját szerkesztés, forrás: dolgozathoz készült kérdőív).....	33
7. ábra Kérdőív elemzés (saját szerkesztés, forrás: dolgozathoz készült kérdőív).....	33

8. ábra Kérdőív elemzés (saját szerkesztés, forrás: dolgozathoz készült kérdőív).....	35
9. ábra Kérdőív elemzés (saját szerkesztés, forrás: dolgozathoz készült kérdőív).....	36

Mellékletek

Interjúkérdések:

1. Ön szerint az internetes mélycsomag vizsgálat hogyan fenyegeti az emberek magánszféráját?
2. Ön szerint honnan értesülhetnek a DPI technológiájának fenyegetéséről az egyének?
3. Ön szerint, mennyire tudatosak az egyének (emberek) az adat – és információbiztonsági szempontból?
4. Ön szerint, milyen szereplők élnek vissza a mélycsomag vizsgálat jelentette lehetőségekkel?
5. Ön szerint mennyire védik az emberek személyes adataikat?
6. Ön szerint mekkora biztonsági kockázatot jelent az emberek adat – és információbiztonságában
7. Ön szerint, mely csoportok, csoportosulások kerülhetnek a DPI technológiájának vizsgálata alá?
8. Ön szerint mennyire ismert az állampolgárok körében a mélycsomag vizsgálat?
9. Ön szerint melyik korosztály védi jobban a saját adatait/figyel oda digitális lábnyomára?
10. Ön szerint milyen célra használhatják fel a technológia segítségével megszerzett információt?
11. Ön milyen privátszférát erősítő technológiákat használ a magánszférájának megvédése érdekében?
12. Ön milyen privátszférát erősítő technológiákat javasol az állampolgárok magánszférájának megvédése érdekében?
13. Ön szerint melyek a legcélravezetőbb módszerek a társadalom biztonságtudatának növelésének érdekében?
14. Ön szerint a technológiát érintő európai uniós és hazai szabályozás kellően részletes-e?
15. Ön szerint a technológiát érintő jogszabály alkotás során mire kellene több hangsúlyt fektetni?

Kérdőíves elemzések táblázatai:

5. táblázat: Keresztábra vizsgálat a tudatosság és az iskolai végzettség függvényében (saját szerkesztés)

Iskolai végzettség		Tudatosnak vallja magát			
		Igen	Nem	Többé-kevés	Összesen
Általános iskola	Kitöltők száma	5	1	14	20
	% az adott iskolai végzettségen belül	25.0%	5.0%	70.0%	100.0%
	% az adott tudatossági választáson belül	9.3%	10.0%	8.6%	8.8%
	% az összértéken belül	2.2%	0.4%	6.2%	8.8%
BA/BSC képzés	Kitöltők száma	13	2	36	51
	% az adott iskolai végzettségen belül	25.5%	3.9%	70.6%	100.0%
	% az adott tudatossági választáson belül	24.1%	20.0%	22.2%	22.6%
	% az összértéken belül	5.8%	0.9%	15.9%	22.6%
Doktori fokozat	Kitöltők száma	2	0	5	7
	% az adott iskolai végzettségen belül	28.6%	0.0%	71.4%	100.0%
	% az adott tudatossági választáson belül	3.7%	0.0%	3.1%	3.1%
	% az összértéken belül	0.9%	0.0%	2.2%	3.1%
Érettségi	Kitöltők száma	22	4	65	91
	% az adott iskolai végzettségen belül	24.2%	4.4%	71.4%	100.0%
	% az adott tudatossági választáson belül	40.7%	40.0%	40.1%	40.3%
	% az összértéken belül	9.7%	1.8%	28.8%	40.3%
MA/MSC képzés	Kitöltők száma	8	2	29	39
	% az adott iskolai végzettségen belül	20.5%	5.1%	74.4%	100.0%
	% az adott tudatossági választáson belül	14.8%	20.0%	17.9%	17.3%
	% az összértéken belül	3.5%	0.9%	12.8%	17.3%
Szakmai bizonyítvány	Kitöltők száma	4	1	12	17
	% az adott iskolai végzettségen belül	23.5%	5.9%	70.6%	100.0%
	% az adott tudatossági választáson belül	7.4%	10.0%	7.4%	7.5%
	% az összértéken belül	1.8%	0.4%	5.3%	7.5%

6. táblázat Keresztábra a tudatosság és a feltételezés között (saját szerkesztés)

Adatvédelmi szempontból tudatosnak tekinti magát		Harmadik fél is látja a privát beszélgetéseket				
		Előfordulhat	Más nem láthatja	Nem tudnak belőle semmit felhasználni	Teljes mértékben így gondolom, de nem tudják felhasználni	Teljesen mértékben így gondolom és fel tudják használni
Igen	Kitöltők száma	23	3	1	8	19
	% az adott tudatosságon belül	42.6%	5.6%	1.9%	14.8%	35.2%
	% az adott megállapításon belül	19.7%	50.0%	50.0%	33.3%	24.7%
	% az összértéken belül	10.2%	1.3%	0.4%	3.5%	8.4%
Nem	Kitöltők száma	4	1	0	1	4
	% az adott tudatosságon belül	40.0%	10.0%	0.0%	10.0%	40.0%
	% az adott megállapításon belül	3.4%	16.7%	0.0%	4.2%	5.2%
	% az összértéken belül	1.8%	0.4%	0.0%	0.4%	1.8%
Többé-kevesé	Kitöltők száma	90	2	1	15	54
	% az adott tudatosságon belül	55.6%	1.2%	0.6%	9.3%	33.3%
	% az adott megállapításon belül	76.9%	33.3%	50.0%	62.5%	70.1%
	% az összértéken belül	39.8%	0.9%	0.4%	6.6%	23.9%

Rövidítések jegyzéke:

DPI: Deep Packing Inspection, internetes mélycsomag vizsgálat

GDPR: General Data Protection Regulation, Általános Adatvédelmi Rendelet

Infotörvény.: az információs önrendelkezési jogról és az információszabadságról szóló törvény
(2011. évi CXII. törvény)

VPN: Virtual Private Network, Virtuális Privát Hálózat

TOR: The Onion Router

PET: Privacy Enhancing Technologies, privátszférát erősítő technológiák

