NEMZETI KÖZSZOLGÁLATI EGYETEM

Katonai Műszaki Doktori Iskola

Üveges András József őrnagy doktor-jelölt

„Az Európai Unió Általános Adatvédelmi Rendeletének (GDPR) hatása a kiberbiztonságra, különös tekintettel a személyes és üzleti adatok védelmére Magyarországon 2018-2020 között”

Doktori (PhD) értekezéstervezet

Témavezető:

Dr. Krasznay Csaba habilitált egyetemi docens

……

Budapest, 2025

Tartalomjegyzék

Tudományos probléma megfogalmazása

A személyes adatok[1] illegális felhasználása különféle tudományos és etikai aggályokhoz vezet napjainkban. [1] Fő probléma a magánélet esetleges megsértése[2], mivel az egyének érzékeny információival visszaélhetnek a kiberbűnözök vagy szélsőséges szervezetek a beleegyezésük vagy tudtuk nélkül. Ennek következtében személyazonosság-lopás, pénzügyi visszaélés és személyes biztonsági kockázat merül fel. A személyes adatok etikátlan felhasználása aláássa az adatbiztonsági intézkedésekbe vetett általános bizalmat a felhasználók részéről, és hátráltatja a felelősségteljes információkezelésen alapuló általános társadalmi folyamatokat.

Tudományos problémaként értékelhető az, hogy jelenleg, ha a társadalom nem érti az adataik védelmének fontosságát, a felhasználók kevésbé lesznek hajlandóak olyan technológiákat használni vagy támogatni, amelyek csökkenthetik a kiberbiztonsági /adatvédelmi kockázatokat.

Ez a tudatosságdeficit megnehezíti az adatvédelmi technológiák és szabályozások hatékony tesztelését, elterjedését és finomítását is. Ezen kívül a társadalmi ismerethiány növeli a sebezhetőséget az alkalmazott informatikai rendszerekkel szemben, ami széles körű gazdasági és szociális hatásokkal járhat az egész társadalomra nézve.

Alapvetően ez a probléma mára külön fogalommá vált, mégpedig a szakirodalom „kiberhigiénia[3]" néven hivatkozik rá. Ez a viszonylag új fogalom azt jelenti, hogy tudatosan és rendszeresen alkalmazunk olyan intézkedéseket és eszközöket, amelyek megóvják az általunk használt informatikai rendszereket, okoseszközeinket és személyes adatainkat a kiberfenyegetésektől, mint például a vírusok és a kémprogramok.

Összefoglalva elmondható, hogy a kiberhigiénia a személyes és szervezeti adatvédelmi biztonság fenntartására irányuló olyan tudatos és rendszeres tevékenység, amely segít lecsökkenteni a kibertámadások és adatlopások kockázatát. Olyan mindennapi rutin tevékenységet[4] jelent, amelyek hozzájárulnak a digitális eszközeink biztonságához. [2]

---

[1] A személyes adat minden olyan információ, amely valamely azonosított vagy azonosítható élő személlyel kapcsolatos. Mindazon információk, amelyek összegyűjtése egy bizonyos személy azonosításához vezethet, ugyancsak személyes adatnak minősülnek. Vagy " a meghatározott természetes személlyel kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható".

[2] Általában „privacy" -ként hivatkozik rá a szakirodalom. Az adatvédelem és a privacy tehát szoros kapcsolatban állnak egymással, hiszen az adatvédelem biztosítja, hogy a személyes adatok gyűjtése és felhasználása megfeleljen a jogi és etikai normáknak, így védve legyen az egyének magánélete.

[3] cyber hygiene - A kiberhigiénia az informatikai eszközeink és rendszereink biztonságos használatára vonatkozó szokások és intézkedések összessége, amelyek célja a kibertámadások megelőzése és az adataink védelme.

[4] Erős jelszavak használata, Rendszeres szoftverfrissítések, Antivírus és tűzfal alkalmazása, Kétlépcsős azonosítás (2FA), Biztonságos Wi-Fi használata, Adatok rendszeres mentése és titkosítása.

További tudományos problémaként értékelhető az is, hogy az új információtechnológiai megoldások esetében nem végeznek hatásvizsgálatot a személyes adatok védelmének tekintetében, így ezek a technológiák olyan kockázatokat hordozhatnak, amelyeket nem ismerünk fel időben. Hatásvizsgálat és kockázatértékelés nélkül nehéz meghatározni, hogy egy adott technológia milyen mértékben sérti a felhasználók magánéletét, vagy milyen adatvédelmi kihívásokkal járhat. Ez megnehezíti a megfelelő szabályozások és védelmi intézkedések kidolgozását. Hosszútávon ez hozzájárulhat a felhasználói bizalom csökkenéséhez és a technológiai innovációk társadalmi elfogadottságának visszaeséséhez is.

Például a személyes adatokhoz való jogosulatlan hozzáférés veszélyeztetheti egy kutatás integritását, és érvényteleníthet a tudományos eredményeket, ami pontatlanságokhoz vezethet a kutatási eredmények kimutatásában.

A személyes adatok eltulajdonítása számos kihívást és kockázatot jelent. Az egyik ilyen probléma az adatok integritásával és pontosságával kapcsolatos a tudományos kutatásokban. A személyes adatok eltulajdonítása a kutatási eredmények manipulálásához vezethet, ami veszélyezteti a tanulmányok és adatelemzések megbízhatóságát. Ennek messzemenő következményei lehetnek különböző tudományterületeken, befolyásolva a kutatási eredmények érvényességét, és hátráltatva a tudás fejlődését.

Az Európai Unió általános adatvédelmi rendeletnek (GDPR[5]) való megfelelés biztosítása az új műszaki megoldásoknál több okból is kulcsfontosságú lett napjainkra, mivel a GDPR egy átfogó adatvédelmi szabályozás, amely szigorú követelményeket támaszt a személyes adatok gyűjtésére, feldolgozására és tárolására vonatkozóan. [3] A GDPR előírásainak betartása törvényi kötelezettség az Európai Unión (EU és EGT) belül működő vagy uniós lakosok adataival foglalkozó vállalkozások számára. Az előírások be nem tartása súlyos pénzbírságot és jogi következményeket von maga után, és ezt kutatásom szerint számos szolgáltató és gyártó is figyelmen kívül hagyja. A GDPR megfelelőségének ellenőrzése és annak betartása segít megvédeni a személyes adatokat (és az adatok tulajdonosát) a jogosulatlan hozzáféréstől, jogsértésektől és visszaélésektől. A GDPR-kompatibilis műszaki megoldások megvalósítása javíthatja az adatbiztonsági intézkedéseket, csökkentheti az adatszivárgás kockázatát és biztosíthatja az egyének adatainak védelmét. A GDPR-megfelelőség jelzés a felhasználóknak, ügyfeleknek arról, hogy egy szervezet jelentős lépéseket tesz az adatvédelem érdekében. A

[5] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről.

bizalomépítés a személyes adatok védelmével és a személyiségi jogok tiszteletben tartásával javíthatja egy szervezet hírnevét és hitelességét az érintettek szemében.

Az egyének magánélethez és adatvédelemhez való jogának tiszteletben tartása nemcsak jogi követelmény, hanem etikai felelősség is. A GDPR-megfelelőség biztosítása tükrözi a szervezet elkötelezettségét az etikus adatkezelési gyakorlatok és az elszámoltathatóság iránt a mai adatközpontú világban.

Összefoglalva, az új technikai megoldások GDPR-megfelelőségének ellenőrzése szükséges a jogi kötelezettségek teljesítéséhez, az adatbiztonság fokozásához, az érdekelt felekkel való bizalom kiépítéséhez, valamint az adatkezelés és feldolgozás etikai normáinak betartásához.

További tudományos probléma, hogy az előbbiekben említettek mellett az érintettek egyáltalán nem rendelkeznek releváns információkkal, valamint nem áll rendelkezésre jelenleg megfelelő technológia ahhoz, hogy érvényesíthessék jogaikat (például törléshez való jog).

A személyes adatokhoz illetéktelen hozzáférés és azok az internet különböző rétegeiben történő kiszivárgása egyre komolyabb tudományos problémát jelent az adatvédelem és a kiberbiztonság területén. A Surface Web, Deep Web és Dark Web eltérő jellemzői és elérhetőségei különböző kockázatokat rejtenek az érzékeny információk kiszivárgása szempontjából.

Míg a Surface Web a nyílt internet szintje, ahol az adatvédelmi szabályozások és a törvényi előírások gyakran érvényesíthetők, a Deep Web és a Dark Web olyan területek, ahol a felhasználói anonimitás, az illegális tevékenységek és az adatlopás lehetőségei sokkal nagyobbak. A személyes adatok ezen szintek közötti áramlása jelentős adatvédelmi aggályokat vet fel, mivel az adatok kikerülhetnek olyan felhasználók vagy szervezetek kezébe, akik nem jogosultak azok kezelésére, és illetéktelenül felhasználják esetleg a későbbiekben ezeket.

A tudományos problémát az adja, hogy az egyének gyakran nem rendelkeznek kellő ismeretekkel arról, hogyan védhetik meg személyes adataikat az interneten, és hogyan kerülhetik el a potenciálisan veszélyes adatmegosztási gyakorlatokat. Emellett az adatvédelmi technológiák gyors fejlődése és a különböző internetes rétegek közötti átjárhatóság folyamatosan új kihívások elé állítja a jogi és etikai normákat. A személyes adatok védelme különböző jogi és technológiai aspektusokat érint, amelyek összetett kérdéseket vetnek fel az online adatkezelés biztonságáról. A probléma mélyebb megértéséhez szükséges az internetes

adatkezelési gyakorlatok hatékony szabályozása, valamint az új típusú adatvédelmi technológiák fejlesztése és alkalmazása.

Az adatvédelem, a kiberbiztonság, a kiberhigiénia, valamint a GDPR-megfelelés – közvetlen relevanciával bírnak a katonai tudományok szempontjából, mivel a korszerű hadviselés egyre inkább információs műveletekre és digitális infrastruktúrákra támaszkodik. A személyes adatokkal való visszaélés, a kiberbűnözés vagy a katonák digitális lábnyomának kiszolgáltatottságából eredő kockázatok nemcsak egyénekre, hanem honvédelmi szervezetekre is veszélyt jelent. A katonai tudományok egyik fő célja az ilyen jellegű veszélyforrások elemzése és kezelése – legyen szó információs hadviselésről, hírszerzési műveletekről vagy védelmi technológiai fejlesztésekről. A személyes adatokkal való visszaélés tudományos és etikai problémákat vet fel napjainkban, különösen a bizalom és az adatkezelés integritása miatt. A katonai tudományokban ez a kérdéskör közvetlenül kapcsolódik az információs műveletek témájához, mivel a dezinformáció, a pszichológiai műveletek és az ellenség adatainak manipulációja mind olyan eszközök, amelyek hatékony alkalmazása a hadtudomány stratégiai tervezési aspektusaiba tartozik. A GDPR-ral kapcsolatos problémák – például a hatásvizsgálat hiánya vagy a törléshez való jog gyakorlati alkalmazhatatlansága, amit tárgyalok a kutatásban – felhívják a figyelmet arra, hogy a technológiai újításokat a katonai szférában is etikailag és jogilag szabályozni kell. A katonai tudományok nemcsak a harcászati-technikai, hanem a normatív vonatkozásokkal is foglalkoznak. Ez különösen fontos például a mesterséges intelligenciát használó katonai rendszerek vagy a katonai megfigyelőeszközök esetében. A személyes adatok kiszivárgása a Surface Weben vagy Dark Weben – fokozottan érintik a honvédséget, ahol a személyes adatok mellett szolgálati adatok, hadműveleti tervek, szenzitív kommunikációk is célponttá válhatnak. A katonai tudomány ezekre a fenyegetésekre reagál védelmi stratégiák, megelőző intézkedések és oktatási programok kidolgozásával.

A fenti tudományos problémák tükrében a következő hipotéziseket állítottam fel.

Hipotézisek

1. sz. hipotézis (H1): ***Jelenleg a magyar társadalom jelentős része nem rendelkezik megfelelően mély ismeretekkel az adatvédelem, valamint az újonnan felmerült kiberbiztonsági kockázatokról, amelyek a személyes adatok kiszivárgása vagy illetéktelen felhasználása tekintetében jelentkeznek, emellett nem is bíznak a szolgáltatók adatvédelmi megoldásaiban.***

A vállalkozások, szolgáltatók által megfogalmazott adatkezelési nyilatkozatok[6] nehezen vagy egyáltalán nem értelmezhetőek, és jelenleg nincs olyan műszaki megoldás, amely biztosítja a felhasználók jogainak maradéktalan betartását a személyes adatok törlése tekintetében.

2. sz. hipotézis (H2): ***Az illegális és hanyag adatkezelés miatt a személyes adatok jelentős számban, folyamatos jelleggel kikerülnek a Surface Webre és a Dark Webre, ezzel egyre jelentősebb biztonsági kockázatot okoznak, és ez emelkedő tendenciát mutat majd a következő években is.***

A személyes adatok megjelenése az internet két rétegében különböző gyakoriságú és formájú, de kikerülésük célja és módja egyértelműen elválasztható és meghatározható.

3. sz. hipotézis (H3): ***A személyes adatok védelme minden új/már alkalmazott technológia esetében külön kockázatértékelést követel meg, valamint GDPR megfelelősségi vizsgálat is minden esetben szükséges, mivel nem készíthető el egy egységes adatvédelmi és kiberbiztonsági keretrendszer ebben a tekintetben.***

Jelenleg nincsen olyan közös adatvédelmi minta, ami minden technológia esetében alkalmazható a GDPR tekintetében.

[6] Hivatalosan ezek valójában adatkezelési tájékoztatók, a GDPR 12, 13-14. cikk szerint.

Kutatási célok

(C1) - A GDPR magyarországi társadalmi értékelésével kapcsolatban több kutatási cél merült fel, amely a felhasználók tudatosságának mérésére fókuszálva a következő alcélokat határozza meg.

(C1.1) - Cél, hogy felmérjem azt, hogy a magyarországi lakosság hogyan értékeli a GDPR-t és annak hatékonyságát (betartását), annak relevanciája és az adatvédelemre gyakorolt hatása szempontjából.

(C1.2) - Meghatározzam a GDPR ismertségének és megértésének szintjét a különböző magyarországi csoportok körében.

(C1.3) Meghatározzam a fejlesztendő területeket, és azonosítsam a GDPR azon szempontjait vagy rendelkezéseit, amelyeket a magyarországi felhasználók nem jól értenek, és felfedjem a tudatosság és az ismeretanyag bővítésének módjait.

(C1.4) További cél, hogy a magyarországi felhasználók a szervezetekkel és hatóságokkal szembeni bizalmát mérjem annak tekintetében, hogy személyes adataik GDPR szerinti kezelése megvalósul-e.

Ezek a kutatási célok vezetik a tanulmányt abban, hogy betekintést adjon a GDPR társadalmi értékelésébe és ismertségébe a magyarországi felhasználók körében.

(C2) További tudományos cél a személyes adatok védelmével kapcsolatos jelenlegi technológiák, jogszabályok tekintetében felmerült kiberbiztonsági kockázatok elemzése és bemutatása, a jelenlegi jogszabályok hatékonyságának elemzése és értékelése a kibertérben a személyes adatok fókuszában.

(C2.1) Az értekezés egyik alcélja a kiberbiztonsági stratégiai dokumentumokban a személyes adatok védelmének szerepét és fejlődését vizsgáló elemzése, amely segíti a megfelelő védelmi mechanizmusok és intézkedések integrálását a kormányzati szervek és más szervezetek adatvédelmi politikáiba.

(C2.2) Cél azonosítani a kulcsfontosságú kiberbiztonsági kihívásokat, a felmerülő fenyegetéseket, a legjobb gyakorlatokat és védelmi módszereket azzal a céllal, hogy csökkenteni lehessen a kiberbiztonsági incidensek bekövetkeztét, ahol a személyes adatok kikerülnek az adatkezelők, adatfeldolgozók kontrollja alól.

(C3) További kutatási célom, hogy felmérjem a személyes adatok illegális felhasználásának terjedelmét és ezek kiszivárgásának hatását a Dark Weben.

(C3.1) Megvizsgáljam a Dark Weben forgalmazott személyes adatok elterjedtségét és típusait. Elemezzem az adatvédelmi incidensek és a visszaélések egyénekre (felhasználókra) és szervezetekre gyakorolt gazdasági és társadalmi hatását. Javaslatot tegyek a személyes adatok védelmére vonatkozó továbbfejlesztett stratégiák implementálására, és javaslatokat dolgozzak ki a kiberbiztonsági gyakorlatok és irányelvek javítására a Dark Web-ről érkező kiberbiztonsági fenyegetések okozta kockázatok csökkentésére.

Kutatásmódszertan

A teljes kutatási ciklus alatt ötvözötten használtam kérdőíves kutatási módszert, dokumentumelemzést, valamint Dark Weben végrehajtott mintavételezési eljárás utáni mélyebb elemzést és esettanulmányozást. [4] A Dark Web-es vizsgálat során empirikus megfigyelést is végeztem. A Dark Webes kutatáshoz azért alkalmaztam ezt a módszert, mivel az empirikus megfigyelés közvetlenül a valóságra (gyakorlatra) alapoz, ami lehetővé teszi a tényleges események, adatok és jelenségek pontos megismerését. Az empirikus megfigyelés során gyűjtött adataim függetlenek saját véleményemtől vagy előítéletemtől, ami növeli a tudományos eredmények megbízhatóságát. Hátrányként említhető a Dark Webes kutatások tekintetében, hogy annak ellenére, hogy az empirikus megfigyelések általában megismételhetők, ami azt jelenti, hogy más kutatók is hasonló eredményeket érhetnek el, ha ugyanazokat a módszereket alkalmazzák, ez a Dark Web esetében már nem áll fent.

A kérdőíves kutatás során meghatároztam a célokat, felvázoltam a kutatás céljait, valamint azt, hogy milyen információkat kívántam gyűjteni. Első lépésként listát készítettem azokról a kérdésekről, amelyek elősegítik a kutatási célok elérését. A kérdések részben nyílt végűek és zárt végűek keveréke lett. Törekedtem arra, hogy egyértelmű, releváns és egyszerű legyen, viszont a téma komplexitása miatt ez nem minden esetben volt teljes mértékben kivitelezhető.

Elvégeztem a kérdőív előzetes tesztelését kis mintával[7], majd azonosítottam a problémákat és a félreértéseket. Ezt követően módosítottam a kérdőívet a közvetlen visszajelzések alapján.

A kitöltés után összeállítottam a válaszokat, és elemeztem az adatokat. Ebben az esetben kvantitatív módszereket a zárt végű kérdéseknél és kvalitatív módszereket a nyílt végű kérdéseknél tudtam használni. Az elemzett adatok alapján levontam a következtetéseket.

A kitűzött célok megvalósításához részt vettem a kiberbiztonsággal, információ- és nemzet biztonsággal, valamint az adatvédelemmel kapcsolatos tudományos rendezvényeken, konferenciákon, gyakorlatokon, majd ezt követően feldolgoztam, elemeztem, és értékeltem az ott szerzett tapasztalatokat. Emellett folyamatosan nyomon követtem a kiberbiztonsággal, információbiztonsággal és adatvédelemmel kapcsolatos sajtó és tudományos cikkeket a

[7] 14 fő személyes felügyelet melletti kitöltés, amely során a kérdéseket részletesen, tételesen ismertettem. A kitöltő személyeknek minden pont után lehetőségük volt kérdéseket feltenni, valamint abban az esetben, ha a kérdés nem volt egyértelmű, akkor a kérdés azonnali átdolgozásra került. Ezt követően a pilot csoport újra kitöltötte a kérdőíveket. Az eredményt a pilot vizsgálat alatt ellenőriztem, majd a megkérdezettek részletesen tájékoztattak arról, hogy az egyes kérdésekre milyen választ adtak, és miért azt válaszolták.

releváns szakfolyóiratok tanulmányozásával, valamint a hírközlési célú médiumokon keresztül a napi fejleményeket.

A témakörben előadásokat tartottam a KNBSZ Doktorandusz Konferencia állománya részére, a Batthyány Lajos Alapítvány ösztöndíjprogramjában, az NKE-HHK-KMDI képzése során, valamint a NKE-ÁNTK hallgatói részére is. Részt vettem nemzetközi kiber, hibrid- és nemzetbiztonsági konferenciákon is (NATO Intelligence Fusion Centre (NIFC), NATO Civilian Intelligence Committee (CIC), CYB PANEL stb.).

Az értekezés szerkezete és jelölésrendszere

Az értekezés szerkezete döntően három fő témakört (a hipotézisek köré szervezve) fog össze, amelyek szorosan összefüggenek egymással.

Az 1. fejezetben az adatvédelmi fogalmak ismeretének mérésének eredményét mutatom be, valamint az adatvédelem társadalmi megítélését elemzem, kitérve annak alapjaira, célkitűzéseire és hatásaira. Vizsgálom a GDPR vállalkozások és szervezetek munkavállalóira gyakorolt hatását, az egyének adatvédelmi jogainak saját megítélését, valamint a közvélemény és szakmai vélemények alakulását.

A 2. fejezetben a Surface Weben és a Dark Weben megtalálható személyes adatok előfordulási formáit és kockázatait mutatom be. Bemutatom a Dark Weben a személyes adatok szempontjából az adatlopás és adatszivárgás mechanizmusait, valamint a személyes adatok illegális kereskedelmét és a kiberbűnözési módszereket. E fejezet kitér a jogalkotási és rendészeti kérdésekre is bemutatva a szabályozási és bűnüldözési erőfeszítéseket, valamint a kutatás során felmerült új tudományos problémákat is megfogalmazom, illetve javaslatot teszek kezelésükre.

A 3. fejezetben a személyes adatok megjelenését vizsgálom a kibertérben, kiberbiztonsági stratégiákban és néhány jelentősebb új/már alkalmazott technológia esetében. E részben meghatározom a személyes adatok fontosságát a digitális korban, a kiberbiztonsági kihívásokat és az ezekre adott válaszokat, valamint az új technológiák (mint például a generatív mesterséges intelligencia, blokklánc és IoT stb.) adatvédelmi kérdéseit és problémáit.

A három fő tartalmi részt általános keretrendszerbe foglaltam, ahol bemutatom a kutatás célját, hipotéziseit, a kutatás módszertanát. A téma nagysága és szerteágazott rendszere miatt lehatárolásokkal éltem. Mivel a digitális korban folyamatosan jelennek meg az új technológiák, így a terjedelem kontrolálása végett szűkíteni kellett a kutatást a vizsgált technológiák tekintetében. Kutatásomat 2024. szeptember 30-án zártam le.

Minden fejezet elején bemutatom a kutatás fejezethez tartozó hipotézisét, a felhasznált kutatási módszertant, valamint 1. és 3. fejezetben a kapcsolódó szakirodalmat is. Majd bemutatom a hipotézis igazolására szolgáló részkutatást és annak részeredményeit.

A felhasznált irodalom a törzsszövegben IEEE szabvány szerint sorszámozott hivatkozással szerepel. Ez a disszertáció végén külön fejezetben található irodalomjegyzékben kerül megjelölésre.

A dőlt szövegrészek a szó szerinti idézéseket jelzik. A disszertációban található ábrák és táblázatok saját szerkesztésűek, amelyeket jeleztem, kivéve amennyiben a forrás egyértelműen fel van tüntetve.

Bevezetés

Az adatvédelem minden eddiginél fontosabbá vált, hiszen a digitális világ folyamatos fejlődése új kihívásokat hoz. A személyes adatok védelme az adatvédelem egyik központi eleme, amely biztosítja, hogy az egyének magánszférája sértetlen maradjon. Az adatvédelem kulcsfontosságú a bizalom fenntartásában, legyen szó magánszemélyekről vagy szervezetekről. Megfelelő védelem nélkül a személyes adatok visszaélések és illetéktelen hozzáférések áldozatává válnak. Ezért mindenki felelőssége, hogy tudatosan kezelje, és védje az adatokat a digitális térben.

Mindennapi életünket, a társadalmat, a gazdaság működését döntően és meghatározóan befolyásolják az internet segítségével összekötött hálózatok, valamint a rajtuk továbbított vagy tárolt személyes adatok. Ez a függés azonban kiszolgáltatottságot is jelent. A digitális ökoszisztéma gyors elterjedése miatt a személyes adatok védelme egyre fontosabbá válik kiemelten a külső fenyegetések tekintetében. Ezt alátámasztja az is, hogy *„A kibertér mindennapjaink meghatározó dimenziójává vált. Életünk minden szegmensére kihatással van, legyen szó gazdaságról, politikáról, kultúráról vagy akár a magánéletünk egyes elemeiről. Azonban azok a szolgáltatások, amelyek a kiberteret alkotják, és az ezeket lehetővé tevő eszközök egyre nagyobb függőséget jelentenek számunkra”.* [5]

Digitális jelenlétünk nyomot hagy a kibertérben, amely tartalmazza a személyes adataink jelentős részét. Személyes adatinkhoz vagy egyéb információkhoz történő illetéktelen hozzáférés komoly kockázatot jelent a felhasználókra. Ezek az adatok jellemzően az internetezési élmény javítására, kényelmi szolgáltatások fenntartására szolgálnak. 2024-ben viszont már olyan mértékű lábnyomot hagyunk, hogy ezeket a szolgáltatók „nagy adatként” kezelik, ezek kikerülése vagy illetéktelenek általi felhasználása komoly adatvédelmi kockázatot jelent. [6]

Személyes adatainkat napjainkban már szinte mindenhol elektronikus úton kezelik és tárolják, ezek egy részét a mindennapi ügymeneteink során osztjuk meg (banki, pénzügyi, egészségügyi stb.) önkéntesen, egy része automatikus módon keletkezik (keresési előzmények, internetes sütik, meglátogatott weblapok stb.), és egy részét illegális módon szerzik meg tőlünk illetéktelen felhasználók.

A személyes adatok kezelésének kérdése nemcsak a polgári szférában értelmezhető, hanem a honvédelmi szektorban és a létfontosságú infrastruktúrák vonatkozásában is. Ezek a típusú adatok megjelennek a kereskedelmi rendszerekben, egészségügyben, információs

technológiában (IT[8]) és az Információs és Kommunikációs Technológia (ITC[9]) rendszerekben, kormányzati hálózatokon egyaránt.

A személyes adatok kezelésének és kockázatkezelésének kérdései az új technológiák tekintetében is megjelentek napjainkra. A blokklánc technológia (kriptopénzek okosszerződések stb.), a felhő szolgáltatások, okoseszközök (Dolgok Internete és okos rendszerek) esetében is már szinte minden esetben felmerül az adatkezelés kérdése és a személyes adatok védelme is. *Alátámasztja ezt az, hogy „A kibertérben lévő szolgáltatások, események és incidensek összetett szempontok szerint meghatározható kiberbiztonságot eredményeznek. A szervezeti feladatok sokszínűsége, a szolgáltatások változásai nem teszik lehetővé, hogy a fenyegetések, sebezhetőségek hosszabb távra érvényes biztonsági szinten legyenek kezelhetők."* [7]

A kibervédelem és a személyes adataink védelme pedig kiemelten fontos mind társadalmi, mind személyes tekintetben egyaránt. Az Európai Unió intézményei és szakhatóságai, az Európai Bizottság, Európai Uniós Kiberbiztonsági Ügynökség (ENISA[10]), az Unió számítógépes eseménykezelő központja (CERT-EU[11]), vagy az EUROPOL[12] is kiemelten kezeli már a személyes adatok védelmét, mivel a kiberbűnözői csoportok kiemelt célpontjai között vannak személyes adataink. Az internet több rétegében fellelhető személyes adatokat napjainkban már illegális módon értékesítik, majd pedig ezt követően ezekkel további bűncselekményeket követnek el.

Például egyre emelkedő tendenciát mutat a több rétegű zsarolási modell a kiberbűnözés területén, amely már megjelenik az EUROPOL IOCAT[13] 2024 jelentésében is. [8]

Az ENISA Threat Landscape 2024 elemzése a személyes adatok védelmét a legfrissebb kiberfenyegetések és technológiai trendek kontextusában elemzi és tárgyalja. A személyes adatok védelme az adatkezelési szabályozások betartásától kezdve az új technológiai kihívásokig (pl. mesterséges intelligencia, Zero Trust[14], adatvédelmi hatásvizsgálatok) széles

[8] Information Technology - Olyan tudományágat és iparágat jelent, amely az információk tárolásával, feldolgozásával és továbbításával foglalkozik, és magában foglalja a számítástechnikát, szoftvereket, hardvereket, adatbázisokat, hálózatokat és egyéb technológiai rendszereket.
[9] Information and Communications Technology - Az ITC azokat a technológiai rendszereket foglalja magában, amelyek az információk kezelését és a kommunikációs folyamatokat segítik elő.
[10] European Union Agency for Cybersecurity - https://www.enisa.europa.eu/
[11] The Computer Emergency Response Team for the EU institutions, bodies and agencies https://cert.europa.eu/
[12] European Police Office
[13] Internet Organised Crime Threat Assessment
[14] Egy kiberbiztonsági modell, amely elve szerint senkiben és semmiben nem szabad automatikusan megbízni, még a belső hálózaton belül sem – minden hozzáférést folyamatosan ellenőrizni és hitelesíteni kell.

spektrumot ölel fel. Az ENISA hangsúlyozza ezen területek fontosságát a biztonsági intézkedések és jogi megfelelőség szempontjából is. A dokumentumban a személyes adatok védelme is megjelenik olyan szempontból, hogy említésre kerülnek a zsarolóvírusokkal kapcsolatos fenyegetések [9], a személyes adatok kezelésével és feldolgozásával (GDPR 4. cikk 12. pontja szerint) kapcsolatos fenyegetések, a pszichológiai manipuláció, adathalászat, a mesterséges intelligencia (MI) is. [7]

Ebben az esetben persze nemcsak a kibertámadásokat kell megemlíteni, hanem a kiberbiztonsági incidenseket is. A kiberbiztonsági incidens olyan esemény vagy eseménysorozat, amely a digitális rendszerek, hálózatok vagy adatok biztonságát veszélyezteti. A kiberbiztonsági incidensek eltérő jellegűek lehetnek. Így például az adatlopás, adathalászat, rosszindulatú szoftver támadások (malware), adathozzáférési hibák, szolgáltatás megtagadással járó támadások (DoS[15] vagy DDoS[16]) vagy egyéb kártékony tevékenységek is ide tartoznak. [10] [11] Ezek az incidensek jelentős károkat okoznak globálisan is.

Kutatásom során megvizsgáltam azokat a jelentősebb kiberbiztonsági incidenseket, amelyeket 2024. január, február és március hónapban publikáltak, és összefüggésbe hozhatóak a személyes adatokkal. Megvizsgáltam a LoanDepot, a Cybernews, az Inspiring Vacations támadás, a Malajzia Telekom újabb adatszivárgását, a Lurie Children's Kórházat ért kibertámadást, a California Union, a A Zenlayer, a Viamedist és az Almeryst, a Pure Incubation Ventures, a France Travail incidenseit. [12]

Mivel a disszertációm nem csak a Surface Web területén értelmezendő, annak érdekében, hogy még jobban látható legyen mennyire aktuális a probléma, ezért a Dark Web blogjain is egy rövid idejű mintát vettem arról, hogy 2024. április 10-11-én milyen adatszivárgásokról lehetett információkat fellelni.

[15] denial-of-service
[16] distributed denial-of-service

Időpont	Weboldal	Feltételezett támadó	Kiszivárgott mennyiség	Szektor
2024. április 11.	crelan.be	BlackSuit	ismeretlen	Bank szektor
2024. április 11.	dubuisson.com	BlackSuit	ismeretlen	**Szórakoztató ipar**
2024. április 11.	ecobati.com	BlackSuit	ismeretlen	Technológia
2024. április 11.	fairoils.com	BlackSuit	ismeretlen	Szépségipar
2024. április 11.	g-pack.be	BlackSuit	ismeretlen	Logisztika
2024. április 11.	generationelec.be	BlackSuit	ismeretlen	Technológia
2024. április 11.	**mylord.be**	**BlackSuit**	**ismeretlen**	**Vendéglátás**
2024. április 11.	nexperia.com	DunghillLeak	1TB	Technológia
2024. április 11.	**inszoneinsurance.com**	**Hunters**	**213GB**	**Szolgáltatás (biztosítás)**
2024. április 11.	okigolf.com	Rhysida	ismeretlen	Szórakoztató ipar
2024. április 11.	oliwoodtoys.be	BlackSuit	ismeretlen	Technológia
2024. április 11.	samartcorp.com	Akira	300GB	Technológia

2024. április 11.	specialoilfield.com	LockBit	ismeretlen	Energia
2024. április 10.	arch-con.com	BlackBasta	2TB	Építőipar
2024. április 10.	atlascontainer.com	BlackBasta	200GB	Logisztika
2024. április 10.	**centralcarolina.com**	**BianLian**	**500GB**	**Szolgáltatás (biztosítás)**
2024. április 10.	consilux.com.br	Akira	ismeretlen	Tanácsadás
2024. április 10.	homeocan.ca	BlackSuit	ismeretlen	Technológia
2024. április 10.	kadushisoft.com	DragonForce	ismeretlen	Szolgáltatás (IT)
2024. április 10.	online.majuhome.com.my	DragonForce	6,84 GB	Könnyűipar
2024. április 10.	multi-fill.com	BlackSuit	ismeretlen	Könnyűipar
2024. április 10.	npcitaly.com	DragonForce	19,23GB	Könnyűipar
2024. április 10.	**panaceahcs.com**	**BianLian**	**ismeretlen**	**Tanácsadás**
2024. április 10.	**roomzzz.com**	**BlackBasta**	**ismeretlen**	**Vendéglátás**
2024. április 10.	**saintcecilias.london**	**DragonForce**	**6,77 GB**	**Oktatás**
2024. április 10.	**schlesingerlaw.com**	**BlackBasta**	**2,2TB**	**Szolgáltatás (jogi)**
2024. április 10.	sermo.com	BlackBasta	700GB	Közösségi hálózat
2024. április 10.	siemensmfg.com	BlackBasta	800GB	Technológia
2024. április 10.	**swansea.com**	**DragonForce**	**5,17GB**	**Tanácsadás (pénzügy)**

1. ábra Kiszivárgások Forrás: saját eredmények

A fenti lista jól mutatja, hogy az adatvédelmi incidensek számos szektort érintenek. Az ábrán kiemelt adatszivárgások esetében nem csak üzleti adatok kerültek nyilvánosságra. Az adatszivárgás érintette például a szolgáltatás, oktatás, tanácsadás területét, ahol feltehetően név, lakcím, elérhetőségek, családi állapot vonatkozásában kerülhettek ki személyes adatok.

A téma aktualitása, kapcsolódása a katonai műszaki tudományokhoz, honvédelmi ágazathoz

A személyes adatok védelme és a katonai műszaki tudományok közötti kapcsolat több szinten is értelmezhető, és jelentős összefüggések azonosíthatóak. A két terület közötti összefüggések különösen a modern digitális technológiai fejlődés és a digitalizálódó korszak előrehaladásával válnak egyre nyilvánvalóbbá. Napjainkban nincs se a privát, se a szakmai életünknek olyan szegmense, amelyben ne kezelnék mások az adatainkat. A honvédelmi ágazatban is több esetben kezelik ezeket a személyes adatokat:

- belépünk a szolgálati helyünkre;

- mozgunk a munkahelyünkön felszerelt kamerarendszer kameráinak látószögében, vagy jelentést írunk;
- éves lövészeten veszünk részt, illetve éves szabadságot szervezünk;
- illetményünk bérszámfejtésénél;
- a szolgálati gépjármű igénybevételénél;
- nemzetbiztonsági ellenőrzés során, illetve nemzetbiztonsági ellenőrzés végzői vagyunk;
- új munkakörbe helyeznek minket, külföldi vagy belföldi szolgálati útra megyünk (útlevél szám, foglalás, útiterv),
- használjuk a szolgálati helyünk számítógépét és a számunkra kiadott e-mail címet;
- humán ügyek intézése során;
- élelmezési anyag rendelése során (ételallergia, ételintolerancia), (éves) egészségügyi ellenőrzés;
- vendéglátóipari szolgáltatás igénybevétele a szolgálati helyen (kantin – pénzügyi adatok), béren kívüli juttatások igénybevétele (tanévkezdési támogatás, nevelési segély), temetéssel és születéssel kapcsolatos támogatások.

Információbiztonság és kiberbiztonság

A katonai műszaki tudományok egyik kulcsfontosságú és napjainkban meghatározó területe az információbiztonság, adatvédelem és kiberbiztonság. A különböző haderőnemek és a honvédelmi ágazatban működő nem katonai szervezetek számára létfontosságú a titkosított kommunikáció, az érzékeny információk védelme, az adatlopások, illetve a kibertámadások elleni hatékony védelem. [13]

A Magyar Honvédség állományának adatai, mint például a katonák személyes és különleges személyes adatai, különleges védelmet igényelnek. A honvédelmi ágazat kiberbiztonsági intézkedéseinek egyik célja ezeknek az adatoknak a védelme az illetéktelen hozzáféréstől. Ma már a honvédelmi ágazat is gyakran szerepet játszik az olyan új technológiák fejlesztésében és alkalmazásában, melyek később a polgári szférában is elterjednek. Az adatvédelmi technológiák, például a titkosítási módszerek, gyakran a katonai kutatások eredményeként jelennek meg először.

Adatkezelés és elemzés

A katonai műszaki tudományokban jelentős szerepe van az adatok kezelésének és elemzésének, különösen a hírszerzés és felderítés szakágait illetően. [14] Természetesen ezeken felül a kommunikációs szolgáltatások fejlődése szükségessé tette az elektronikus információvédelmi rendszabályok honvédelmi fejlesztését. A biztonsági célkitűzések, biztonsági követelmények,

védelmi rendszabályok és mechanizmusok naprakész szabályozása kulcskérdés. Erről Kassai Károly *Az elektronikus információvédelem szabályozási kérdései a közelmúltban* című cikkében részletesen olvashatunk. [15] A személyes adatok védelme kiemeleten fontos kérdés, mivel a begyűjtött adatok gyakran tartalmaznak érzékeny személyes adatokat. A katonai hírszerzési tevékenységek, katonai műveletek során rengeteg információt gyűjtenek, beleértve a civil lakosság adatait is. Ezek védelme, valamint a jogi és etikai normák betartása kulcsfontosságú. A katonai műszaki tudományok egyre inkább támaszkodnak a nagy adathalmazok (Big Data[17]) elemzésére és a mesterséges intelligencia alkalmazására. Ezek az adatok gyakran személyes információkat is tartalmaznak, így a megfelelő adatvédelmi intézkedések elengedhetetlenek. [16]

Szabályozások

Mind a honvédelmi (2022. évi XXI. törvény a honvédelmi adatkezelésekről, 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról) mind a polgári szektorban a személyes adatok védelmére vonatkozó szabályozások és jogszabályok szigorú betartása szükséges. A katonai szervezeteknek is alkalmazkodniuk kell a személyes adatok védelmét szabályozó nemzetközi és nemzeti jogszabályokhoz, mint például a GDPR. A katonai műszaki tudományok fejlődése során felmerülő etikai kérdések, például a megfigyelés és adatgyűjtés vonatkozásában, szorosan kapcsolódnak a személyes adatok védelméhez. Emellett már egyes tudományos művek azt is vizsgálják például, hogy mi adhat mentességet[18] a rendelet alkalmazása alól a haderőnek. Így a honvédelmi, bűnüldözési és nemzetbiztonsági célú adatkezelések esetében az Infotv. az irányadó, míg az ettől eltérő célú adatkezelések esetében a GDPR. Mivel ez is egy kiemelt kérdése a haderő és az adatvédelmi szabályozás összefüggésének, [17] [18] fokozott kockázatot jelent a honvédelmi ágazatban a személyi állomány adatainak kiszivárgása. Számos ilyen esetet publikáltak a különböző médiafelületeken is. Például az amerikai Pentagon 2023-ban több mint 26 000 alkalmazottjának adatai kerülhettek ki egy adatvédelmi incidens során. [19] Hasonló eset történt 2024-ben a BBC tájékoztatása szerint, amikor az Egyesült Királyság Védelmi Minisztériumánál tevékenykedő személyi állomány egy részének az adatai szivárogtak ki. [20]

[17] A nagy adat kifejezés olyan adatállományokra utal, amely túl nagy, túl gyorsan keletkezik, vagy túl sokféle formában jelenik meg ahhoz, hogy a klasszikus adatfeldolgozási módszerekkel hatékonyan kezelhető legyen. A Big Data definícióját gyakran a 3V vagy 5V modell alapján magyarázzák. Volume (Mennyiség), Velocity (Sebesség), Variety (Változatosság), Veracity (Hitelesség) és a Value (Érték).

[18] A GDPR 23. cikke tartalmaz korlátozásokat. Ez nem mentesség, azonban az érintett jogokat jelentősen lehet korlátozni pl. nemzetbiztonsági és honvédelmi érdekre hivatkozva.

Jogszabályok

Számtalan ágazati jogszabályunk tartalmaz adatvédelmi rendelkezéseket, mint a munka törvénykönyve (Mt.) [21], a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló törvény [22], az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló törvény [23], a panaszokról és a közérdekű bejelentésekről szóló törvény, a nemzeti köznevelésről [24] és a nemzeti felsőoktatásról szóló törvény [25], az elektronikus hírközlésről szóló törvény [26] és a személyszállítási szolgáltatásokról szóló törvény is [27]. Fontos azt kihangsúlyozni, hogy amennyiben az ágazati törvény adatkezelésre vonatkozó szabálya ütközik a GDPR előírásaival, az uniós rendeletben megfogalmazottak az irányadók.

2. ábra Jogi keret

Kutatásom során a szakértői megbeszélések, interjúk és kérdőívek kitöltése esetében kérdésként merült fel az, hogy a GDPR és az Infotv. milyen módon lehet elhatárolni. Erre esettanulmányként jó példa a rendvédelmi, honvédelmi szervezeteknél rendszeresített mobiltelefonokra telepített elektronikus levél postafiókja. Ebben az esetben az a helyes eljárás, ha a személyes elektronikus postafiókunkat nem telepítjük a szolgálati telefonunkra, illetve a szervezetek által alkalmazott Exchange kiszolgálót egy másik készülékre telepítjük. Gyakorlatban viszont egyes esetekben az Android operációs rendszerrel ellátott eszközök csak

Gmail fiók telepítésével működnek üzemszerűen, így ezek alkalmazása nem kívánatos a rendvédelmi szervezeteknél. Megoldás lehet, ha ilyen esetben egy kizárólag erre a célra elkülönített Gmail fiókkal hajtjuk végre a készülékregisztrációt, ennek azonban hátránya, hogy ilyen esetben egy rendvédelmi dolgozóhoz minimálisan két privát fiók (GDPR) és egy szolgálati fiók (Infotv.) tartozik.

Gyakorlati alkalmazások

A korszerű biztonsági rendszerek és hálózatok tervezése és kivitelezése során alapvető fontosságú a személyes adatok védelme. A katonai személyzet által használt okoseszközök, alkalmazások és kommunikációs rendszerek fejlesztésekor is figyelembe kell venni a személyes adatok védelmét, így akár a kiképző rendszerek esete is ide sorolható. [28]

Ebben az esetben pedig ki kell emelni a honvédelmi ágazatban alkalmazott IoT eszközök okozta kockázatot is. A katonai IoT-piac várhatóan 2032-re eléri a 18,22 milliárdos forgalmat, és a Komponens Éves Növekedési Ütem (CAGR[19]) 6,20%-os lesz 2022-2032-re. Ennek oka, hogy a globális katonai IoT-piac drasztikus ütemben fejlődik. [29]

Napjainkra a védelempolitikai nyilatkozatokban, stratégiákban és elgondolásokban alapvetővé vált az, hogy a jelenlegi és jövőbeli katonai műveletekben a fizikai csapásmérő erőkkel együtt vagy akár önállóan alkalmazott kiber- és hibrid hadviselési módszereket alkalmaznak. A személyes adatok védelmének fontosságát mutatja az is, hogy ez megjelenik már a különböző kiberbiztonsági stratégiai dokumentumokban. [30]

A személyes adatok védelmét a katonai műveletek területén is lehet értelmezni. A NATO álláspontja szerint a kibertér már a negyedik dimenziója a hadviselésnek. De már 2007-ben is kiemelt figyelmet fordított a szervezet a kibervédelem és kiberhadviselés területére.

2012-ben a kibervédelem bekerült a szövetség védelmi tervezési folyamatába, majd ezt követően a 2014. évi walesi csúcson elfogadásra kerültek a NATO kibervédelmi szakpolitikai irányai.

Ezután a szövetség Walesben deklarálta, hogy a kibertérben is érvényesnek tekinti a nemzetközi jogot, emellett pedig a kibervédelem területét beemelte a NATO kollektív védelmi feladatai közé[20]. 2016-ban a Varsói Csúcs záródokumentumában[21] a szövetségesek amellett, hogy

[19] Compound Annual Growth Rate - Jelzi, hogy egy adott érték (például bevétel, piac vagy eszköz értéke) évente hány százalékkal nőtt egy adott időszak alatt, figyelembe véve a növekedés kumulált hatását.
[20] Wales Summit Declaration, p 72., p 73.
[21] Warsaw Summit Communiqué, p 70-71.

megerősítették a NATO védelmi jellegét, az operatív hadviselés területét – a tengerek, a szárazföld és a levegő mellett – kiterjesztették a kibertérre is. Emellett deklarálták, hogy a NATO egy tagországa elleni kibertámadást a szövetség egésze elleni támadásnak tekinthet, és szükség esetén kollektív válaszlépéseket tehet. [31]

Mint minden katonai műveletet, a kiberműveleteket is fegyverekkel vívják meg. Ilyen eszközök a rosszindulatú szoftverek is, amelyek napjainkra a kiberhadviselés egyik alapeszközeivé váltak, amelyekkel az egyes reguláris vagy irreguláris erők sikeres műveleteket képesek végrehajtani a katonai információs rendszerek ellen.

Az információs műveletek során végrehajtott kiberműveleteknek több célja lehet. Ezek közé tartozik a megtévesztés, amelynek része lehet akár a katonai rendszerekben tárolt információk megváltoztatása, a katonai hálózatok üzemszerű működésének megakadályozása, az informatikai rendszerek ideiglenes megbénítása, valamint ugyanezen rendszerek fizikai rombolása és az információ gyűjtése (például a személyes adatoké).

Az érzékeny adatok gyűjtése honvédelmi vonatkozásban az információgyűjtés esetében értelemszerűen csak a honvédelemmel kapcsolatos információk tekintetében értelmezhetőek. Az adatgyűjtésnek több ismert módszere létezik, viszont katonai viszonylatban a legcélravezetőbb az, ha nagy mennyiségű adatot begyűjtünk az ellenérdekeltségű célpontról, majd a megszerzett adatokat szintetizáljuk és szűrjük.

A klaszteranalízis során olyan dimenziócsökkentő eljárást alkalmaznak, amely által megpróbáljuk a klasztereket tartalmi relevanciájuk szerint csoportosítani. A tisztított adatot a későbbiekben relevancia szerint klaszterekbe rendezzük, vagy az általunk meghatározott struktúrába csoportosítjuk a gyors és hatékony kereshetőség érdekében. Ennek a folyamatnak a terjedése növekvő tendenciát mutat az elmúlt időszakban. Elég csak felfigyelni arra, hogy erre a tevékenységre szolgáltatási iparág is épült. A kártékony szoftverek üzemeltetését egyes hekkercsoportok már szolgáltatják is, és ezt általában a számítógépes támadások végrehajtására szolgáló szoftver és hardver bérbeadásaként is nevesítik (MaaS[22]). A MaaS-szerverek tulajdonosai fizetett hozzáférést biztosítanak egy rosszindulatú programokat terjesztő botnethez, amelynek segítségével hozzáférhetnek a kívánt adatokhoz, és letölthetik vagy kiszivárogtathatják azokat.

A MaaS szolgáltatás az egyik legjobb példa arra, hogy átlátható legyen az, hogy a személyes adatok megszerzése viszonylag egyszerű tevékenység is lehet. Hiszen a szolgáltatás bérlésével

[22] Malware-as-a-Service

könnyen célba juttathatnak kártékony szoftvereket abból a célból, hogy személyes adatokat szerezzenek meg a kiberbűnözők vagy ellenérdekeltségű szerveztek, majd könnyedén értékesíthetik a Dark Weben ezeket az adatokat. Mivel a MaaS egy úgynevezett kiberbűnözői modell, amely lehetővé teszi, hogy alacsony műszaki tudással rendelkező támadók is könnyen hozzáférjenek, és használjanak kártékony szoftvereket. A MaaS szolgáltatások gyakran előre elkészített, bérelhető malware-eket, például trójaiakat, zsarolóvírusokat, botneteket vagy adathalász eszközöket kínálnak, amelyeket a támadók személyes adatok megszerzésére használhatnak. Arról nem beszélve, hogy a MaaS szolgáltatás is jellemzően a Dark Weben érhető el. [32]

Az ilyen szolgáltatások ügyfeleinek általában személyes fiókot kínálnak, amelyen keresztül irányíthatják a támadást, valamint technikai támogatást nyújtanak részükre.

Ilyen adatszerzésre kiválóan alkalmasak a kiberhírszerzés során használt kártékony szoftverek, amelyeket kémprogramoknak vagy más néven kémszoftvernek (spyware[23]) neveznek. A legtöbb spyware a felhasználó tudomása nélkül, valamilyen megtévesztésen alapuló módszerrel kerül bele az informatikai rendszerbe. A széles spektrumú adatgyűjtés a katonai rendszerek vonatkozásában az esetek túlnyomó többségében az alábbi információkra korlátozódik: – hadiipari és hadigazdasági vállalkozások üzleti adatai; – hadiipari beszállítók érzékeny adatai; – haditechnikai vállalatok műszaki megoldásai; – katonai létfontosságú rendszerek sérülékenysége; – létfontosságú információs infrastruktúra rendszerelemeinek sérülékenysége, személyi állomány és katonai vezetés személyes és érzékeny adatai.

A személyes adatok kezelése a honvédelmi ágazatban is számos kockázatot rejt magában. A személyes adatok illegális kezelésének formái az orosz-ukrán konfliktus tekintetében is felmerültek. A különféle fegyveres konfliktusok, a hagyományos és az új típusú biztonsági kihívások és fenyegetések dinamikus és gyors váltakozása, illetve kölcsönhatása új, eddig nem látott mértékben növelték meg a kiberbiztonsági kockázatokat az élet számos területén, ami közvetve és közvetlenül is érinti a személyes adtok kezelését.

Az orosz-ukrán konfliktus során kiszivárgott és felhasznált személyes adatok tovább mélyítik/mélyítették az orosz-ukrán konfliktust a kibertérben. Mivel várhatóan a szembenálló felek a konfliktus diplomáciai rendezése alatt, vagy a katonai konfliktus közben célirányos

[23] Olyan rosszindulatú szoftver, amely titokban figyeli, és rögzíti a felhasználó tevékenységét anélkül, hogy az érintett erről tudna, vagy beleegyezését adta volna.

támadásokat hajtanak végre katonák, kormánytisztviselők, politikusok, vagy akár a háború elől menekülők ellen, ezen adatok felhasználása segítségével.

Meg kell említeni még azt is, hogy a személyes adatok kezelése és annak bizalmassági kérdései a fegyveres harcok során életét vesztett áldozatok hozzátartozóinak és a háborús bűntettek elszenvedőinek, valamint tanúinak tekintetében is felmerült a kutatás során. Ezt abban a viszonylatban lehet vizsgálni, hogy az orosz-ukrán konfliktus során folyó kiberműveletek alatt számos személyes adatot szivárogtattak ki egymásról a szembenálló feleket támogató hekkerek. Emiatt például az ukrán fél a háborús bűntettek vizsgálta során minimális személyes adatot dokumentálnak annak érdekében, hogy a tanúk azonosítását megakadályozzák, illetve pszeudoanonimizálást[24] is alkalmaztak szintén a tanúk védelme érdekében.

Kutatásom során több esettanulmányt is megvizsgáltam annak érdekében, hogy bemutassam azt, hogy a személyes adatok milyen célokra használhatók fel a fegyveres konfliktusok során. Ilyen esettanulmány volt az az incidens, amely során személyes adatok nagyméretű gyűjtésének kérdése több esetben felmerült. Sajtóinformációk szerint a Sberbanktól kerültek ki személyes adatok a konfliktus kitörését követő időszakban. A sajtóban megjelent információk alapján a Google engedélyezte egy szankcionált orosz reklámcégnek, hogy hónapokig gyűjtsön felhasználói adatokat. A Google a Sberbank tulajdonában lévő RuTarget-nek egyedi mobiltelefon-azonosítókról, IP-címekről, helyadatokról, valamint a felhasználók érdeklődési köréről és online tevékenységéről információkkal adott át. A feltehetően június 23-án történt adat átadással kapcsolatosan kockázati tényezőként a következőket azonosítottam:

- a felhasználók személyes adatai (név, cím, pénzügyi adatok, keresési előzmények, érdeklődési kör stb.) kiszivárogtak, és ismeretlen felhasználókhoz kerültek;
- a reklámcég a személyes adatokat továbbította a Sberbank rendszerébe, és onnan kiegészítve banki adatokkal esetleg orosz kormányzati rendszerbe került az információ.

Az esemény annak ellenére bekövetkezett, hogy 2022. április 6-án United States Department of the Treasury, Office of Foreign Assets Control (OFAC) számos orosz entitást felvett a különlegesen kijelölt állampolgárok (SDN[25]) listájára. Konkrétan az amerikai

[24] Olyan adatvédelmi technika, amely során a személyes adatokat úgy módosítják, hogy azok ne legyenek közvetlenül azonosíthatóak, de a módosított adatok és az eredeti adatok között visszafejthető kapcsolat maradjon fenn. Ezáltal az adatok továbbra is használhatók, de nem kapcsolhatók egyértelműen egy adott személyhez, anélkül hogy az adatkezelőhöz hozzáférne a kulcs vagy az információ, amely lehetővé tenné a visszafejtést.

[25] Specially Designated Nationals and Blocked Persons List – Olyan személyeket, szervezeteket és vállalatokat tartalmaz, akikkel az amerikai állampolgárok és vállalatok nem folytathatnak üzleti tevékenységet, mivel

Pénzügyminisztérium fokozta az orosz kormánnyal szembeni szankciókat az ukrajnai atrocitások miatt. Így a Pénzügyminisztérium szankcionálta a „webalapú automatizált oroszországi reklámszoftver-fejlesztőt”, a „RuTarget”. [33]

Hasonló eset volt az Orosz Központi Bank incidense is, amikor ukrán hekkerek sajtóközleményben kijelentették, hogy az Orosz Központi Banktól több ezer belső dokumentumot loptak el, pontosabban egy 2,6 GB-os adatcsomagot szereztek meg illetéktelenül, amely 27.000 fájlt tartalmazott. Ezek az adatok elvileg a bank munkatársainak (volt munkatársak és aktív munkavállalók) a személyes adatait is tartalmazták. [34]

A támadást az ukrán érdekeltségű IT Army egyik eddig ismeretlen tagja (csoportja) hajtotta végre. A támadó a Telegramm csatornáján kiemelte azt, hogy ha az orosz központi bank a saját adataira sem tud vigyázni, akkor hogyan tudná szavatolni a rubel árfolyamának stabilitását.

A támadás ténye és sikerességének kérdése azért jelentős, mivel a jegybank Oroszország egyik legfontosabb pénzintézete, az állami monetáris politika kidolgozója és a nemzeti valuta szabályozója. Az orosz média tagadta, hogy feltörték volna a rendszerét, és sajtóközleményükben kijelentették, hogy minden kiszivárgott dokumentum már fent volt a nyílt interneten. Ez a példa is kitűnően mutatja, hogy a személyes adatok illetéktelen eltulajdonítása kiválóan alkalmas arra, hogy a konfliktus során egyes intézmények reputációját negatívan befolyásolják. [35]

Azt is érdemes a konfliktus tekintetében kiemelni, hogy az ukrán hekkerek orosz érdekeltségű zsoldosok személyes adatait szerezték meg az orosz Wagner Katonai Magánvállalattól. Ennek következtében ez egy kiemelten jó esettanulmány arra, hogy nyomon követhessük azt, hogy a személyes adatok illetéktelen felhasználása a konfliktus után is további konfliktusokat okozhat. [36]

Összességében a személyes adatok védelme és a katonai műszaki tudományok közötti kapcsolat alapvetően az információbiztonságra, a szabályozások betartására és az etikai normák figyelembevételére épül. Ahogy a technológia fejlődik, ez a kapcsolat egyre inkább előtérbe kerül, és mindkét terület számára fontos kihívásokat és lehetőségeket jelent. Természetesen ide sorolható még az is, hogy a honvédelmi ágazat a működése során a saját állománya személyes adatait is kezeli, de erre a kutatás nem terjedt ki.

kapcsolatban állhatnak terrorizmussal, kábítószer-kereskedelemmel, pénzmosással vagy más nemzetbiztonsági kockázatokkal.

A katonai kiberműveletek során a személyes adatok hatékony felhasználása károkozás céljából többféle módon valósulhat meg. Ezek a módszerek gyakran kifinomultak és műszakilag már fejlettek, és céljuk lehet az ellenfél demoralizálása, információs hadviselés, vagy közvetlen anyagi károkozás.

Ilyen módszer lehet a személyre szabott adathalász-támadás. A személyes adatok alapján hiteles, személyre szabott adathalász e-mailek küldése lehetséges, amelyekkel bizalmas információk megszerzése a cél a honvédelmi ágazat munkatársaitól. Hasonlóak továbbá a magas rangú katonai vagy kormányzati személyek ellen indított támadások, melyek révén érzékeny információkhoz lehet hozzájutni. Ilyen eset például a belorusz érdekeltségű UNC1151 hekkercsoport, amely ukrán katonák ellen indított adathalász kampányt. A kampányra az ukrán Számítógépes Eseménykezelő Központ hívta fel a figyelmet. [37]

Emellett kockázatként értékelhető a személyazonosság-lopás is, amely során katonai vagy kormányzati személyek személyazonosságát eltulajdonítják, hogy hozzáférjenek bizalmas rendszerekhez vagy információkhoz, elsősorban belépési adatokhoz. Illetve idetartozik még a hamis identitások létrehozása és felhasználása dezinformációs kampányokban. [38]

A pszichológiai manipuláció[26] során a személyes adatok felhasználása a célpontok manipulálására, bizalmas információk megszerzésére vagy kártékony tevékenységek befolyásolására is alkalmas. Ennek segítségével lehetséges a beépülés szervezetekbe vagy csoportokba. A pszichológiai manipuláció célja, hogy az áldozatokat a lehető legkisebb ellenállással, gyakran szakszerűen személyre szabott módon próbálják manipulálni. Ennek érdekében a kiberbűnözők gyakran az áldozatok közvetlen környezetéből, illetve nyilvánosan elérhető adatbázisokból szerzik be az információkat. Ennek a módszernek alkalmazása magas kockázatot jelent az áldozatokra, valamint egyre több esetben használják kiegészítő/előkészítő tevékenységnek kibertámadások során. Az Aura mérése szerint 2023-ban ezek a támadások az éves kibertámadások 20%-át tették ki. [39] A katonai pszichológiai hadviselés során a megfélemlítés és dezinformáció esetében is jelentős szerepet játszanak a személyes adatok.

A honvédelmi ágazat létfontosságú infrastruktúrái ellen végrehajtott célzott támadások során a személyes adatok felhasználása kulcsfontosságú, hiszen ezek segítségével azonosítják az informatikai rendszerhez hozzáférő kulcsfontosságú felhasználókat a támadók. 2015-ben az ukrán energetikai hálózatot kibertámadás érte. A támadást a Sandworm elnevezésű orosz hekkercsoport hajtotta végre, bár a támadási módszerek inkább a kiberbiztonsági rendszerek és

[26] Social Engineering

az infrastruktúra sérülékenységeire összpontosultak, azonban a támadók nemcsak sérülékenységeket, hanem személyes adatokat is felhasználhattak, hogy sikeresebbé tegyék az inzultust. Az esemény során a kiberbűnözők valószínűleg pszichológiai manipulációt használtak, hogy hozzáférjenek a célpontok érzékeny adatihoz, például az ukrán energetikai cég munkatársaiét. Az ukrán elektromos hálózati támadás hátterében egyes szakértők úgy vélik, hogy a támadók kihasználták a külső beszállítók, alvállalkozók vagy szervizcégek kapcsolatát is a hálózathoz. Ebben az esetben a támadók a személyes adatokat felhasználhatták, hogy megtévesztő kéréseket küldhessenek az alvállalkozók felé, amelyek így lehetővé tették a hozzáférést a rendszerekhez. Összességében tehát a személyes adatok nem voltak közvetlenül az alapvető támadási eszközök, de hozzájárulhattak ahhoz, hogy a támadók hatékonyabban juthassanak hozzá a kritikus rendszerekhez és az érzékeny információkhoz.

A fentiek tükrében a katonai kiberműveletek során a személyes adatok védelme kiemelt fontosságú, és mind a katonai, mind a civil ágazatban szigorú adatvédelmi intézkedésekre van szükség a biztonság érdekében.

1. Az adatvédelmi fogalmak ismeretének mérése, az adatvédelem társadalmi megítélése

1.1 Áttekintés

Az adatvédelem és a mai társadalom információs térben megjelenő tevékenysége közötti összefüggés számos aspektusban megnyilvánul. A GDPR 2016-ban lépett hatályba és 2018. május 25-től alkalmazandó az Európai Unióban, és célja a személyes adatok védelmének megerősítése és egységesítése volt. Ez a rendelet jelentős hatással van a mai társadalomra, különösen a digitális világban de a társadalmi életben is. [40]

Az adatvédelem és a társadalom összefüggéseinek kérdőíves kutatása növelheti az emberek tudatosságát és ismereteit az adatvédelem fontosságáról, mivel számos új kérdésre világít rá a megkérdezetteknek is.

A kutatási eredmény hozzájárulhat a felelős adatkezelési gyakorlatok terjedéséhez, mind az egyének, mind a szervezetek körében. A társadalom és az adatvédelem összefüggéseinek kutatása több okból is kiemelt fontosságú és releváns. Az alábbiakban felsorolás szerint a legfontosabb szempontok:

Az MI és a Big data elemzése robbanásszerű fejlődést mutat jelenleg. Ezek a technológiák óriási mennyiségű adatot gyűjtenek és elemeznek, amelyek közül sok a személyes adat. Az ilyen technológiák alkalmazása új adatvédelmi kihívásokat vet fel, amelyeket meg kell érteni a társadalomnak, és kezelni is kell.

Az IoT eszközök és az okoseszközök használata széles körben elterjedt, és folyamatosan növekszik számuk a háztartásokban. Ezek az eszközök folyamatosan adatokat gyűjtenek rólunk, amelyek személyes és érzékeny információkat tartalmazhatnak. Az adatvédelem kutatása szükséges annak biztosítására, hogy ezek az eszközök biztonságosan működjenek. Így a kutatások során meg kell ismeri azt, hogy a társadalom mennyire van tisztában az ebben rejlő kiberbiztonsági kockázatokkal.

Az adatvédelmi jogszabályok folyamatosan fejlődnek, és szigorodnak globálisan az elmúlt évek során. A GDPR jelentős hatást gyakorolt az adatvédelmi gyakorlatokra az Unióban, és más országok is hasonló szabályozásokat vezettek be. A kutatás segít megérteni ezeknek a jogszabályoknak a társadalmi hatásait és a megfelelés biztosításának módjait, hiszen maga a magyar társadalom minden szintje érintett ebben a kérdésben. Viszont szükségessé vált a kutatás annak érdekében, hogy megismerjük azt, hogy a társadalom milyen mélyen ismeri az említett jogszabályokat.

Az adatvédelmi kérdések nemzetközi dimenzióval is bírnak, mivel az adatok határokon átnyúló áramlása egyre gyakoribb. A globális adatvédelmi szabályozások harmonizációja és az ezekből eredő kihívások kutatása fontos a nemzetközi együttműködés és az adatvédelem javítása érdekében.

Az adatvédelemi tevékenység közvetlen hatással van az egyének magánszférájára és alapvető jogaira. A kutatás segített feltárni, hogy hogyan érinti az adatkezelés és a technológiai fejlődés az egyének életét, és hogyan lehet egyensúlyt teremteni az innováció és a magánélet védelme között.

Bár a kutatás célirányosan nem vizsgálta azt, hogy a személyes adatok felhasználása diszkriminációhoz is vezethet, különösen az MI rendszerek esetében, amelyek előítéletes algoritmusokat használhatnak. Az adatvédelem és az etika kutatása segít azonosítani és kezelni ezeket a problémákat.

Az adatvédelem és a társadalom összefüggéseinek kutatása növelheti az emberek tudatosságát és ismereteit az adatvédelem fontosságával kapcsolatban. Ez hozzájárulhat a felelős adatkezelési gyakorlat terjedéséhez mind az egyének, mind a szervezetek körében.

Összességében a társadalom és az adatvédelem összefüggéseinek kutatása 2024-ben kulcsfontosságú ahhoz, hogy megértsük, és kezeljük az adatvédelemmel kapcsolatos kihívásokat, elősegítsük a technológiai- és jogszabályi fejlődést, és biztosítsuk az egyének jogainak és magánéletének védelmét egy egyre digitálisabb világban.

1.2 Hipotézis

Hipotézisem szerint: „***Jelenleg a magyar társadalom jelentős része nem rendelkezik megfelelően mély ismeretekkel az adatvédelem, valamint az újonnan felmerült kiberbiztonsági kockázatokról, amelyek a személyes adatok kiszivárgása vagy illetéktelen felhasználása tekintetében jelentkeznek, emellett nem is bíznak a szolgáltatók adatvédelmi megoldásaiban.”***

Kutatás módszertana

Kérdőívek és felmérések:

A hipotézis igazolásához kérdőíves kutatási módszert alkalmaztam. Ennek oka, hogy a kvantitatív kutatási módszer deduktív jellegű vizsgálati típus, mivel jelentős mennyiségű adat gyűlt össze, meghatározott logikai ív mentén bizonyítani tudtam az előre meghatározott hipotézisemet. Emellett a módszertan mellett szóló érv volt, hogy a metódus alapvető jellemzői a számszerűsíthetőség és a mérhetőség.

A kérdőívek kitöltése minden esetben felügyelet mellett zajlott, valamint klasszikus értelemben véve nem alkalmaztam online (elektronikus) kérdőívet. Ennek oka, hogy a témakör eleve komplex, valamint az egyszavas válaszok, eldöntendő kérdések nem adtak volna értékelhető eredményt, valamint azokból nem lehetett volna ismereteket szerezni arról, hogy a gyakorlatban milyen ismeretanyag áll a megkérdezettek rendelkezésére. Emellett álláspontom szerint a személyes kérdőíves kutatás számos előnnyel rendelkezik az online kérdőíves kutatással szemben:

- Várhatóan magasabb a válaszadási arány, mivel a személyes interakció révén a válaszadók nagyobb valószínűséggel töltötték ki a kérdőívet, mivel közvetlen kapcsolatban álltunk, így lehetőség volt bátorítani, és emlékeztetni a megkérdezetteket a kitöltésre.
- Hatékonyabb és részletes válaszminőség, hiszen a személyes kérdezés során tisztáztam a kérdéseket, magyarázatokat adtam, így pontosabb és részletesebb válaszokat kaphattam.
- A személyes interakció során összetettebb és hosszabb kérdőíveket tudtam használni, mivel segíthettem a válaszadóknak a szövegértésben, és végigvezethettem őket a kérdéseken.

- A személyes kérdőíves kutatás során a környezet jobban kontrollálható volt, így a válaszadók kevésbé voltak a külső tényezők által befolyásolva, így jelentősen megbízhatóbb eredményeket kaptam.
- A személyes interakció során megfigyeltem a válaszadók metakommunikációját, arckifejezéseit és egyéb nonverbális jeleket, amelyek további információkat nyújtottak a válaszok értelmezéséhez.
- A személyes kérdezés lehetősége is biztosított volt, így mélyebb kérdéseket tudtam feltenni, így megalapozottabb információkat gyűjtöttem be. [41]

1.3 Kapcsolódó szakirodalom áttekintése

Ahhoz, hogy a téma átlátható és egyértelmű legyen magát az adatvédelem fogalmát is pontosítani kívánom. Az adatvédelem definícióját számos tudományos forrás tárgyalja különböző formában és kontextusban. Az adatbiztonság alapvetően a személyes és érzékeny adatok bizalmasságának, integritásának és rendelkezésre állásának biztosítását jelenti, annak érdekében, hogy megvédjék azokat a jogosulatlan hozzáféréstől vagy illegális felhasználástól[27].

Az adatvédelemhez hasonló, ami a természetes személyek személyes adatainak kezelése során alkalmazott elvek, jogok és intézkedések összessége, amelynek célja az érintettek jogainak és szabadságainak védelme, különösen a magánélethez való joguk tiszteletben tartása mellett.

A fogalom szorosan kapcsolódik az értekezésemben tárgyalt GDPR-hoz, amely meghatározza a személyes adatok feldolgozására vonatkozó alapelveket.

A GDPR tekintetében is számos értelemző szakkönyv készült, ezek az ismertető tanulmányok szerint az adatvédelem a jogi szabályozáson túl kiterjed a technológiai megoldásokra, mint például a Privacy-Enhancing Technologies (PETs) alkalmazása. Ezek az eszközök segítik az adatbiztonság növelését az anonimizálás és a hozzáférés-szabályozás révén, miközben elősegítik az adatok biztonságos megosztását is. Az adatvédelem elveit az Egyesült Nemzetek Emberi Jogok Egyetemes Nyilatkozata is rögzíti, amely szerint minden egyénnek joga van személyes adatainak védelméhez.

[27] Egyes szakértői vélemények ezzel szemben azt mondják, hogy ez így egyedül a GDPR 5. cikk (1) bekezdés f) pontjában meghatározott alapelve szűkíti az adatvédelmet.

Az alaptörvény VI. cikk (2) bekezdése rögzíti a személyes adatok védelméhez való jogot, és ugyanennek a cikknek a (3) bekezdése előírja, hogy adatvédelmi törvényt kell alkotni. Az általános szabályokat a Polgári törvénykönyv is megfogalmazta már.

Az Alaptörvény alapján született meg az információs önrendelkezésről és az információszabadságról szóló 2011. évi CXII. törvény, amely célként fogalmazza meg, hogy személyes adataival mindenki maga rendelkezzen. A nemzetközi normákkal összhangban meghatározza a személyes adatok gyűjtésének és feldolgozásának feltételeit.

Az adatvédelmet szabályozó törvény értelmében mindenkinek joga van megtudni, hogy milyen nyilvántartást vezetnek róla, és mindenki kérheti téves adatai törlését, amennyiben esetleg ez felmerül. A személyes adatokat az arra jogosult szervezetek is csak meghatározott célból és csak a feltétlenül szükséges mértékben és ideig kezelhetik. Az adatfelvétel előtt a kérdezett személyt tájékoztatni kell, hogy az adat szolgáltatása önkéntes vagy kötelező. Amennyiben az adatszolgáltatás kötelező, meg kell jelölni az azt elrendelő jogszabályt is. Személyes adatot harmadik fél számára továbbítani csak az érintett beleegyezésével lehet. Kivételt e szabály alól – meghatározott indokból – csak törvény határozhat meg.

1. A definíciók közös vonása, hogy az adatvédelem nemcsak technikai, hanem etikai és jogi megközelítést is magában foglal, hangsúlyozva az egyén jogainak tiszteletben tartását az adatkezelés során. Az egyének személyes adatainak védelmét ebben az esetben például név, cím, születési dátum jelenti.
2. Adatbiztonság: Az adatok fizikai és digitális védelme a jogosulatlan hozzáférés ellen.
3. Adatkezelési gyakorlatok: Az adatkezelők és adatfeldolgozók által alkalmazott eljárások az adatok védelme érdekében.

Az adatvédelem társadalmi hatásairól, különösen a GDPR által kiszabott bírságokról és azok okairól számos cikk született, amely az MI és az adatvédelem összetett kapcsolatával is foglalkozik, Molnár Nikolett cikke például rávilágít a technológiai szabályozások szükségeségének kérdésére is. [42] A kérdőíves kutatásomnak előzményeit, jogszabályi és társadalmi szempontból dr. Sziklay Júlia vizsgálta „Az információs jogok kialakulása, fejlődése és társadalmi hatása” című doktori értekezésében. [43]

Egyes tanulmányok, mint például Hielke Hijmans és Charles Raab cikke a GDPR etikai dimenzióival is foglalkozik. Cikkükben megállapítják azt, hogy a GDPR és maga az adatvédelem ma már túlmutat a jogi kérdéseken, azaz erre utal a GDPR 5. cikk (1) bekezdés a) pontja, miszerint az adatkezelés során tisztességesen kell eljárni. Az etikai döntéshozatalhoz

számos új kritériumot kell meghatározni ahhoz, hogy a jogszabályi megfelelés mellett milyen adatvédelmi döntéseket kell vagy lehet meghozni, ebben viszont a társadalmi szereplők nem feltétlenül értenek egyet. [44] A személyes adatok védelme és annak a társadalomra gyakorolt hatása nemzetközi vonatkozásban is megjelenik. Az Egyesült Nemzetek Fejlesztési Programja (UNDP[28]), kiemelten kezeli azt, hogy az egyes egyéneknek személyes adatai és jogai biztosítva legyenek. [45] A legfontosabb azt figyelembe venni, hogy a részkutatás egyik célja rávilágítani arra, hogy a megfelelő tudás nélkül az egyes személyek alapvető jogai is sérülhetnek. A személyes adatok védelme az Európai Unió Alapjogi Chartájában is szerepel, pontosabban az EU Alapjogi Chartája **7**. cikkében. Ez az alapvető jogokat biztosítja a személyes adatok védelmére az EU-ban, és alapot ad a személyes adatok kezelésére vonatkozó jogi szabályozásoknak is. [46]

1.4 A célcsoport meghatározása

Magyarországon különböző célcsoportok tölthetnek ki kérdőíveket, attól függően, hogy az milyen célból készült. A kutatásom esetében az alábbi csoportok kerülhettek kizárólag a kutatás fókuszába, az alábbi csoportosítások szerint:

Felnőtt lakosság: Általános társadalmi, gazdasági, politikai, egészségügyi vagy egyéb felmérések esetén a célcsoport általában a felnőtt lakosság. Ezen kérdőív célja esetében a kiskorúak[29] nem számítottak olyan felhasználóknak, akik releváns információval rendelkeztek volna.

Oktatási intézményekben gyakran végeznek kérdőíves felméréseket a diákok és hallgatók körében. A jelenleg felsőoktatásban tanuló hallgatók több esetben találkoznak az adatvédelmi kérdésekkel, így véleményük releváns a felmérés szempontjából. Az is elmondható, hogy összességében a GDPR és az adatvédelem fogalma számos módon és kontextusban jelenik meg a felsőoktatásban, biztosítva, hogy a hallgatók alaposan megismerjék, és megértsék ezen fontos szakterületek alapjait, gyakorlati megjelenését, valamint a felmerült kockázatokat. Adatvédelmi kurzusok során egyetemen és főiskolán külön megjelenik ez a tárgykör, amelyek kifejezetten a GDPR és az adatvédelem témakörére fókuszálnak, így a hallgatók véleménye releváns

[28] United Nations Development Programme - Az UNDP több mint 170 országban és területen működik, és olyan projekteket indít, amelyek a gazdasági fejlődést, a társadalmi egyenlőséget és a környezet védelmét célozzák.
[29] Magyarországon a kiskorúság meghatározása a Polgári Törvénykönyv (Ptk.) alapján történik. A magyar jog szerint kiskorúnak számítanak azok a személyek, akik még nem töltötték be a 18. életévüket. Kiskorú**:** Az a személy, aki még nem töltötte be a 18. életévét. Cselekvőképtelen kiskorú**:** Az a személy, aki 14 évesnél fiatalabb. Ők jognyilatkozatot (például szerződést) nem tehetnek, helyettük törvényes képviselőjük jár el. Korlátozottan cselekvőképes kiskorú**:** Az a személy, aki már betöltötte a 14. életévét, de még nem töltötte be a 18. életévét. Ők bizonyos jognyilatkozatokat önállóan is megtehetnek, de más esetekben törvényes képviselőjük hozzájárulása szükséges.

információkat tartalmazhat. Ezek a kurzusok lehetnek részben jogi, informatikai, gazdasági és társadalomtudományi jellegűek is, ahol megjelenik a személyes adat védelme. A joghallgatók esetében különösen fontos az adatvédelem, így a jogi karokon szinte minden esetben találkoznak a GDPR és az Infotv. szabályaival és azok alkalmazásával. Ha tovább vizsgáljuk, akkor az is megállapítható, hogy az informatikai szakokon a hallgatók adatbázis-kezelés, kiberbiztonság, és információbiztonság témakörében ismereteket szereznek a GDPR és az adatvédelem alapelveiről.

Emellett a közgazdasági és üzleti képzések során, kiemelten a marketing, online értékesítés, webshopok esetében, menedzsment és emberi erőforrás szakokon, szintén kiemelt szerepet kap az adatvédelem, mivel az üzleti szektorban az ügyfelek és munkavállalók személyes adatainak védelme prioritást élvez.

Napjainkban a jogi és informatikai szakismeretek egyre több esetben fonódnak össze, ennek következtében egyre több egyetem kínál olyan interdiszciplináris programokat, amelyek kombinálják a jogi, informatikai és gazdasági tudományokat, és ezek keretében az adatvédelem és a GDPR is már több esetben is megjelenik. A felsőoktatási intézmények kutatási projektjeiben is gyakran érintik az adatvédelem témakörét, különösen akkor, ha a kutatás során személyes adatokat gyűjtenek vagy dolgoznak fel. Egyetemek és főiskolák gyakran szerveznek szemináriumokat, workshopokat és konferenciákat, ahol a GDPR és az adatvédelem aktuális kérdéseit tárgyalják. Ezeken az eseményeken a hallgatók szakértőktől tanulhatnak, és naprakész információkat szerezhetnek. Számos oktatási intézmény kínál online kurzusokat és e-learning tananyagokat az adatvédelem és a GDPR témakörében, amelyek rugalmas tanulási lehetőséget biztosítanak a hallgatók számára. Sok képzés során esettanulmányokon és gyakorlati feladatokon keresztül ismerkedhetnek meg a hallgatók a GDPR gyakorlati alkalmazásával, ami segít a tanultak mélyebb megértésében és alkalmazásában. Vállalatok és szervezetek belső felméréseket készíthetnek a munkavállalók számára, hogy mérjék a munkavállalói elégedettséget, a munkahelyi környezetet, a képzési igényeket vagy a vállalati kultúrát. Sok kutatás és felmérés célja lehet az online közösségek és a közösségi média felhasználói véleményének és viselkedésének megismerése. Ezek a kérdőívek gyakran online platformokon keresztül kerülnek kiküldésre. Egyes felmérések speciális célcsoportokat céloznak meg, például bizonyos szakmák (honvédelem és rendvédelem) képviselőit, különböző korosztályokat.

A kérdőíves kutatás során törekedtem arra, hogy a magyar társadalom szemszögéből reprezentatív adatokkal tudjak dolgozni. Ennek tükrében a kérdőíveket a honvédelmi és polgári szférában egyaránt alkalmaztam. A megkérdezettek alapvetően gépjárműipar, emberi erőforrás

szervezés, IT és ITC szakterület, honvédelmi[30], rendvédelem[31], nemzetbiztonsági szektorból kerültek ki. Figyelembe vettem azt, hogy a megkérdezettek a társadalom teljes egészét lefedjék, így végzettség tekintetében nem alkalmaztam lehatárolásokat.

1.5 Lehatárolás

A megkérdezettek tekintetében lehatárolás a következő esetben történt. A kérdőívek kitöltése önkéntes alapon történt, és a válaszadóknak joguk van megtagadni a részvételt vagy bármikor visszavonni hozzájárulásukat. Emellett a személyes adatok védelme érdekében a kérdőívek kitöltésekor a GDPR előírásait is be kell tartani.

Kizárólag olyan személyek töltötték ki a kérdőíveket, akik:

- legalább betöltötték a 18. életévüket;
- közügyektől jogerősen nem voltak eltiltva;
- nem álltak gyámság alatt;
- kizárólag saját döntésük szerint, önkéntesen töltötték ki a kérdőívet.

1.6 Adatvédelmi ismeretek mérésének célja

Az adatvédelmi ismeretek mérése Magyarországon elsősorban a jogszabályi megfelelés biztosítását, a tudatosság növelését, az adatvédelmi incidensek megelőzését, a belső folyamatok fejlesztését, a vevői és partneri bizalom növelését, a versenyelőny megszerzését, a kockázatkezelést, valamint az oktatási programok hatékonyságának értékelését szolgálja, de abból a szempontból, hogy van-e valamilyen ismereti alapja a társadalomnak/egyénnek.

A kutatásom egyik alapvető kérdése, hogy a magyar társadalom milyen alapvető ismertekkel rendelkezik az adatvédelem vonatkozásában. Ismeri a kérdéskörben az alapvető fogalmakat? Ehhez az alábbi kérdéseket használtam annak érdekében, hogy a fent említett kérdésre választ kapjak:

- Véleménye szerint mik tartoznak a személyes adatok közé? (alapvető tudás méréséhez);
- Véleménye szerint mik tartoznak a különleges személyes adatok közé? (alapvető tudás méréséhez);
- Ön szerint melyik a legérzékenyebb személyes adat[32]? (Csak egy típust nevezzen meg) (mit tartanak a megkérdezettek a legnagyobb kockázatnak);

[30] MH 2. Vattay Antal terület védelmi ezred, MH Klapka György 1. Páncélos dandár, Katonai Nemzetbiztonsági Szolgálat.
[31] Budapest II. Kerületi Rendőrkapitányság
[32] A kérdés esetében felmerült további kérdésként, hogy milyen módon definiálható az érzékeny adat fogalma.

- Az ön által ismert személyes adatok közül melyeket tartja a legfontosabbnak? (mit tartanak a megkérdezettek a legnagyobb kockázatnak);
- Véleménye szerint kerültek-e már illetéktelen kézbe az ön adatai?;
- Véleménye szerint a kiberbűnözők tevékenysége valós veszélyt jelent a személyes adatok vonatkozásában?

1.7 A GDPR-ral kapcsolatos ismeretek mérésének célja

A GDPR-ral kapcsolatos ismeretek mérésének célja az alábbiak szerint fogalmazódnak meg. A GDPR szigorú követelményeket támaszt az adatvédelmi gyakorlatokkal kapcsolatban. Az ismeretek mérése segített abban, hogy átláthatóvá váljon az, hogy a vállalatok és szervezetek hogyan felelnek meg ezeknek a jogszabályoknak, elkerülve ezzel a bírságokat és egyéb jogi következményeket. A mérés során elsődlegesen a fókuszban a felhasználók törléshez való jogának biztosítását vizsgáltam meg.

A kérdőíves kutatás során az ismeretek mérésével felmértem, hogy a munkavállalók (felhasználók) mennyire vannak tisztában a GDPR-ral kapcsolatos előírásokkal és elvárásokkal, alapfogalmakkal. Ez segíthet az oktatási programok fejlesztésében és a tudatosság növelésében, valamint az ismeretek mérése alátámasztotta azt is, hogy a felhasználóknak szüksége van alapvető oktatásra, aminek jellemzően példák bemutatásán alapuló összefoglaló tanulmánynak kell lennie.

A megfelelő adatvédelmi ismeretek birtokában a munkavállalók hatékonyabban tudják védeni a személyes adatokat, csökkentve ezzel az adatvédelmi incidensek kockázatát. A kutatás célja közt volt az is, hogy a felhasználók mennyire vannak tisztában azzal, hogy mi az incidens fogalma, vagy hogy esetleg már estek-e áldozatul ilyen eseménynek.

A GDPR-megfelelés és az adatvédelem iránti elkötelezettség növelheti a vállalatok és szervezetek esetében az ügyfelek és partnerek bizalmát, mivel biztosak lehetnek abban, hogy adataikat biztonságban kezelik. A kutatás sarkalatos pontja volt az, hogy kvalitatív módon mérjük azt, hogy a felhasználók megbíznak-e az adatkezelőkben? Bíznak-e abban, hogy adataikat biztonságosan, a GDPR szabályai szerint kezelik.

Az ismeretek mérése révén azonosítottam azokat a területeket, ahol hiányosságok vagy gyengeségek vannak az adatvédelem, különösen a személyes adatok védelme területén. Ezek alapján fejlesztési intézkedések vezethetők be a belső adatkezelési folyamatok javítására.

Összességében az ismeretek mérése alapvetően hozzájárul a GDPR követelményeinek betartásához és az adatvédelem kultúrájának kialakításához a szervezetben.

Fontos azonban kiemelni, hogy a kutatás döntően honvédségi közegben zajlott. A kérdőívet kitöltők túlnyomó többsége a Magyar Honvédség kötelékéből került ki – tehát olyan személyek, akik szoros kapcsolatban állnak a szervezet biztonsági és információvédelmi gyakorlatával. A civil szférából származó válaszadók száma korlátozott volt, így a minta nem tekinthető teljes mértékben reprezentatívnak a magyar társadalom egészére vonatkozóan.

Ennek ellenére a kutatás kiemelkedő értéke, hogy egy specifikus, magas szabályozottságú környezet – a honvédelem – adatvédelmi kultúrájába enged betekintést. Az itt szerzett tapasztalatok és tanulságok azonban hasznos kiindulópontként szolgálhatnak a civil szektor számára is, különösen azokban az ágazatokban, ahol a biztonságos adatkezelés hasonlóan kritikus fontosságú (pl. egészségügy, pénzügyi szektor, közigazgatás). A kutatás tehát nemcsak belső fejlesztést szolgálhat, hanem hozzájárulhat a társadalmi szintű adatvédelmi kultúra erősödéséhez is.

Ehhez az alábbi kérdések kerültek be a kérdőívbe a méréshez:

- Hallott-e már az EU általános adatvédelmi rendeletéről? (GDPR). (alapvető tudás méréséhez)
- Soroljon fel 5 esetet, ahol már találkozott a rendelettel!
- Munkahelyén/beosztásában találkozott-e az adatvédelmi rendelettel?
- Magánéletében hol találkozik legtöbbször a GDPR fogalmával?
- Az ön véleménye szerint a rendelet szabályai könnyen értelmezhető az adatvédelmi nyilatkozatokban/ adatkezelési tájékoztatókban?
- Részt vett-e korábban a GDPR rendeletről szóló oktatáson? Ha igen, akkor milyen módon?

A kutatás során vizsgáltuk, hogy a megkérdezettek a rendelet szabályait az adatkezelési tájékoztatókban tudják-e értelmezni.

Az iskolai végzettség tekintetében elmondható, hogy jellemzően a magasabban végzetséggel rendelkező személyek ismerték az általános adatvédelmi rendeletet, míg az alacsonyabb végzettséggel rendelkezők nagyobb számban válaszoltak nemmel. Ebből az eredményből az következik, hogy az adatvédelemmel, kiemelten a személyes adatok védelmével kapcsolatos oktatást (ismeretterjesztést) már általános iskolai szinten meg kell kezdeni. Emellett a magasabb iskolai végzettséggel rendelkező személyek jellemzően érdeklődnek, vagy rendelkeznek alapismeretekkel az adatvédelemről. Ennek oka feltételezhetően az, hogy a felsőoktatásban

több esetben találkoznak adatvédelmi kérdésekkel, valamint tanulmányaik során rálátást szereznek arra, hogy a személyes adatok védelme kiemelt prioritással bír.

Bebizonyosodott, hogy a felhasználók kevesebb, mint fele rendelkezik ismeretekkel a GDPR-ról. Emellett a felhasználók vagy nem értik vagy el sem olvassák az adatvédelmi tájékoztatókat.

A kutatás során vizsgáltuk, hogy a megkérdezettek a rendelet szabályait az adatkezelési tájékoztatókban tudják-e értelmezni. A 141 fő válaszadó közül 41 fő válaszolt „igen-nel", 56 fő pedig „nem-el", 44 fő pedig saját bevallása szerint nem olvassa el ezeket a tájékoztatókat. Az arányokból arra lehet következtetni, hogy a megkérdezettek közel 29%-a tudja csak értelmezni az adatvédelmi tájékoztatókban foglaltakat, közel 40% pedig nem érti ezeket a szabályokat, 31% pedig el sem olvassa azokat.

1.8 A felhasználók bizalmának mérése

A felhasználói bizalom tudományos módszerekkel történő mérése létfontosságú volt az adatvédelem és a GDPR szempontjából 2022-ben, mivel segítette a szervezeteket a megfelelőség biztosításában, a bizalom növelésében.

Hiszen az adatvédelem és az információbiztonság alapvetővé vált a digitális korban. A felhasználók adatainak megfelelő kezelése és védelme alapvető elvárás a szolgáltatók fele, valamint a felhasználói bizalom jelentős hatással van a szervezetek hírnevére és későbbi tevékenységére.

Tudományos módszerekkel végzett bizalomfelmérésekkel pontos képet adtam arról, hogy a felhasználók mennyire bíznak/vagy nem bíznak meg egy adott szervezetben vagy szolgáltatásban az adatvédelem szempontjából.

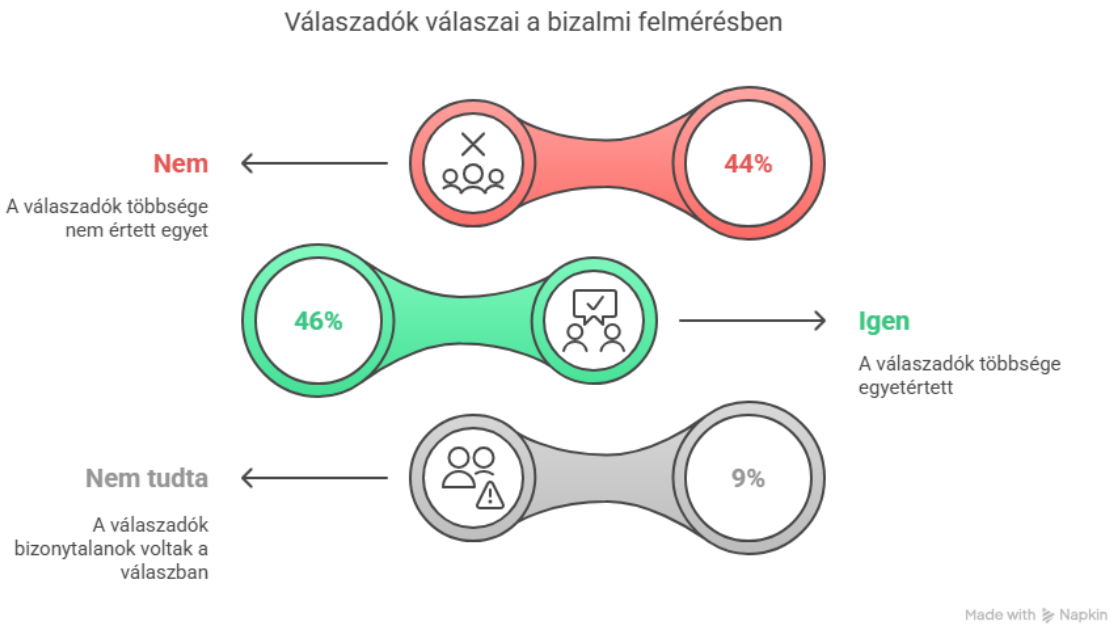
A GDPR szigorú előírásokat tartalmaz az adatok kezelésére, és új irányelveket adott a védelmére vonatkozóan. Az egyik alapelv a felhasználó önkéntes beleegyezése, amely csak akkor tekinthető érvényesnek, ha az informált és gyakorlatilag is önkéntes. A felhasználók bizalmának mérése tudományos módszerekkel segíthet biztosítani, hogy a felhasználók valóban megértették, és elfogadták az adatkezelési gyakorlatokat, ami elősegíti a GDPR előírásainak való megfelelést, azaz tisztában vannak-e azzal, hogy mit is fogadtak el, és teljes bizalommal írták-e azt alá. Ha a vállaltok és szerveztek szempontjából nézzük, akkor a GDPR kiemeli/elősegíti a transzparencia és elszámoltathatóság fontosságát. A tudományos módszerekkel végzett felmérések objektív és megbízható adatokat szolgáltattak a felhasználói bizalomról, ami későbbiekben elősegítheti majd a szervezetek számára, hogy nyilvánosan és hitelesen kommunikálják adatvédelmi gyakorlatukat.

Tágabban értelmezve a felhasználói bizalom közvetlen hatással van a felhasználói érzelmeire és a szervezethez vagy vállalathoz való hűségre is. Ha a felhasználók bíznak egy szervezetben, nagyobb valószínűséggel maradnak annak rendszerében, és könnyebben osztják meg adataikat. A tudományos módszerekkel végzett bizalomfelmérések segíthetnek azonosítani a bizalom növelésének lehetőségeit javítva ezzel a felhasználói élményt és lojalitást. Leglényegesebb pont, hogy a rendszeres bizalomfelmérések lehetővé teszik a jelentősebb problémák korai felismerését és kezelését. Ha egy szervezet/rendszer időben felismeri, hogy a felhasználói bizalom csökken, gyorsan beavatkozhat és módosíthatja adatvédelmi gyakorlatát, hogy helyreállítsa a bizalmat.

A bizalom méréséhez az alábbi kérdéseket tettem fel a megkérdezetteknek.

- Véleménye szerint ön találkozott már adatvédelmi incidenssel, vagy hanyag adatkezeléssel? Ha igen hol?
- Önnek mi jelentene garanciát személyes adatának védelme érdekében egy adatkezelőtől?
- Véleménye szerint kerültek-e már illetéktelen kezekbe az ön személyes adatai?
- Véleménye szerint a szolgáltatók betartják saját adatvédelmi előírásaikat?

Példaként kiragadva az utolsó kérdésre a válaszadók az alábbi módon válaszoltak. A 300 feldolgozott kérdőív esetében erre a kérdésre 118-an válaszoltak az alábbi eloszlásban.



3. ábra Bizalom mérése (kivonat) Forrás: saját kutatási adatok

Továbbá a kérdések direkt módon céloznak a probléma felmérésére, valamint felhasználói megoldást is keresnek. Természetesen a felhasználók megoldásai megállapítható, hogy a szervezet/vállalkozás szempontjából műszaki, vagy jogszabályi, vagy adatvédelmi okokból nem megvalósíthatóak.

A kutatás során kitértünk arra a kérdésre, hogy a megkérdezettek miként értékelik azt, hogy érintettek voltak-e már adatvédelmi incidensben. A 300 feldolgozott kérdőíven a megkérdezettek csak 15 esetben válaszoltak „igen”-nel, a többi megkérdezett nem írt választ, feltehetően a kiberbiztonsági, illetve az adatvédelmi incidens fogalma nem volt ismert a számukra. Valószínűsíthető, hogy a fő probléma az, hogy az érintettek gyakorlatilag fel sem tudják mérni azt, hogy a tárolt adataikat bárki illetéktelenül megszerezheti tudtukon kívül, és emiatt kialakul bennük egy „hamis” biztonságérzet.

Kutatásunk során bizonyítást nyert az a tény, hogy a megkérdezettek (a megkérdezettek közel 90%) alapvetően a retorziót említették, mint egyetlen olyan garanciát, amely biztosítja a személyes adataik megfelelő szintű védelmét, leginkább azért, mert jelenleg nincs lehetőségük arra, hogy az adatkezelőket ellenőrizni tudják (erre jelenleg megállapításunk szerint technológiai megoldás nem áll rendelkezésre).

A kutatás során a személyes elbeszélgetések tekintetében. viszont megállapítottam, hogy a megkérdezettek azzal egyáltalán nem voltak tisztában, hogy a GDPR felhatalmazza a tagállamok felügyeleti hatóságait, hogy közigazgatási bírságot szabjanak ki, amelynek nagysága attól függ, hogy a rendelet mely cikkeit sértette meg az adatkezelő, illetve az adatfeldolgozó. A bírság összege legfeljebb 20 millió euró, illetve vállalkozások esetében azok teljes éves világpiaci forgalmának legfeljebb 4%-át kitevő összeg lehet attól függően, hogy melyik érték magasabb. A felmérés során erre mindösszesen négy személy tudott választ adni pontosan, de ez nem volt emiatt mérhető a teljes megkérdezettek tekintetében (1%).

1.9 Mérési eredmények összefoglalása

Adatvédelmi ismeretek mérésének eredménye (részletesen az 1. sz. melléklet)

Hipotézisem igazoltam az eredményekből, hogy a megkérdezettek jelentős része rendelkezik információval arról, hogy milyen adatok tartozhatnak a személyes adatok körébe. Viszont senki sem tudta hibátlanul felsorolni a jogszabályban megfogalmazott személyes adatok mindegyikét egyszerre. Alapvetően a megkérdezettek 93,20%-a válaszolt a kérdésre, ahol az általuk

személyes adatnak vélt adattípusokat sorolták fel. Ennek feltételezhető oka, hogy a megkérdezettek egy konkrétumra asszociálnak ilyenkor, és nem egy komplex összefüggésre. Ebben az esetben ez az lenne, hogy a személyes adat minden olyan információ, amely valamely azonosított vagy azonosítható élő személlyel kapcsolatos. Mindazon információk, amelyek összegyűjtése egy bizonyos személy azonosításához vezethet, ugyancsak személyes adatnak minősül. Ehelyett jellemzően 35 személyes adat típust említetek a megkérdezettek.

Több esetben tárgyi tévedések merültek fel a részletesebb ellenőrzés során. Jól látható, hogy egyes esetekben konkrétan adatcsoportokat neveztek meg a megkérdezettek, és nem személyes adattípusokat soroltak fel. Emellett további kiértékelési problémát okozott az, hogy egyes adattípusokat tovább bontottak, például:

- név-családnév,-vezetéknév-keresztnév-születési név;
- bankkártya adatok – bankkártya számok;
- Jelszavak – PIN kódok.

A részletesebb kimutatás szerint alapvetően az adat típusok közül legtöbb esetben a név és lakcím kombinációja merült fel. Feltételezhetően azért, mert ezekkel az adatokkal találkoznak legtöbbet a felhasználók. Azt is érdemes megfigyelni, hogy egyes felhasználók már személyes adatnak minősítik a kibertérben megjelenő adatokat, mint az e-mail cím vagy a böngészési előzmények, de ezek a számok elenyészőek. A hipotézisemet alátámasztja az is, hogy a megkérdezettek 6,9%-a fogalmazta meg azt, hogy az adat akkor minősül személyes adatnak alapvetően, ha ennek segítségével beazonosítható egy személy. Bebizonyítottam, hogy a társadalom egy jelentősebb része nem ismeri ténylegesen a személyes adat fogalmát és összefüggését.

1.10 A GDPR-ral kapcsolatos ismeretek mérésének eredménye

Kérdőíves kutatásom célja annak feltérképezése volt, hogy a megkérdezettek mennyire ismerik a GDPR-t, illetve milyen mélységben tudják értelmezni annak alapfogalmait. A felmérés eredményei azt mutatták, hogy a válaszadók túlnyomó többsége – több mint 90%-a – már hallott a GDPR-ról, és helyesen az adatvédelem témaköréhez tudta kötni. Ugyanakkor a válaszok mélyebb elemzése során kirajzolódott, hogy a jogszabályhoz kapcsolódó alapvető fogalmak, mint például a „jogalap”, „adatkezelő”, „adatfeldolgozó”, „hozzájárulás”, vagy a „törléshez való jog”, nem egyértelműek sokak számára.

Kutatásommal párhuzamosan a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) is több tanulmányában és éves jelentésében rámutat arra, hogy bár a GDPR-ról való hallomás elterjedt, a mélyebb ismeretek hiányoznak a lakosság jelentős részéből. A NAIH 2021-es jelentésében például megállapítják, hogy a panaszok nagy része félreértésekből, illetve az adatkezelési jogok nem megfelelő ismeretéből fakadtak.

Hasonló eredményekre jutott a 2020-as Eurobarométer felmérés is, amely szerint az európai polgárok 73%-a hallott már a GDPR-ról, viszont csak 20%-uk érzi úgy, hogy teljes mértékben érti is, milyen jogok illetik meg önmagukat, mint érintettet.

A fogalmi zavar különösen az adatkezelés jogalapjainál volt jellemző a saját kutatásomban. A megkérdezettek úgy vélték, hogy minden adatkezeléshez szükséges írásos hozzájárulás, miközben a GDPR több jogalapot is megenged (pl. szerződés teljesítése, jogi kötelezettség, jogos érdek), ahol a hozzájárulás nem szükséges, sőt nem is megfelelő. Ez a félreértés gyakorlati következményekkel járhat – például olyan esetekben, amikor egy szervezet feleslegesen kér hozzájárulást, ezzel saját magát adatvédelmi kockázatnak teszi ki.

A fenti eredmények alapján egyértelmű, hogy a GDPR kommunikációs és oktatási stratégiáját nemcsak a jogszabály ismertségére, hanem a fogalmak pontosítására és értelmezésére is ki kell terjeszteni. Célzott lakossági kampányokat, oktató videókat, valamint az iskolai oktatásba illesztett adatvédelmi modulokat be kell vezetni, hogy már fiatal korban lefektessük az adatvédelmi tudatosság alapjait.

Összességében tehát a kutatás megerősítette azt a gyakorlati tapasztalatot, hogy a GDPR-ról szóló diskurzus felszíni ismeretekben gazdag, de mélységi tudásban még hiányos. A jogszabály valódi céljainak – vagyis az egyének adatainak hatékonyabb védelmének – eléréséhez elengedhetetlen a fogalmi világ közérthetőbbé tétele és a társadalom jogtudatosságának fejlesztése.

1.11 A felhasználók bizalmának mérésének eredménye.

Kutatásom szerint a GDPR 2018-as hatálybalépése óta a természetes személyek adatainak védelme jogi szinten kiemelt figyelmet kapott. Ennek ellenére a közvélemény bizalma az adatkezelő vállalkozások irányába nem növekedett érdemben – sőt, sok esetben inkább lecsökkent teljes mértékben. Az érintettek bizalmatlansága több összefonódó tényezőből ered, amelyek nemcsak jogi, hanem társadalmi és pszichológiai szempontokat is tartalmaz.

Az adatvédelmi tájékoztatók jellege vált a bizalmatlanság egyik legfőbb forrásává. Ezek a dokumentumok hosszúak, túlságosan részletezőek, és olyan jogi nyelvezetet használnak, amely a hétköznapi felhasználó számára nem értelmezhetőek. Bár elvileg ezek célja az átláthatóság biztosítása lenne, a gyakorlatban sokszor inkább elrettentik az olvasót, aki nem olvassa el teljes egészében, vagy ha el is olvassa, nem biztos benne, hogy pontosan tudja, vagy érti, mit vállal. Ez az információs aszimmetria könnyen vezethet ahhoz az érzéshez, hogy a vállalkozások valójában elrejtik az adatkezelés valódi természetét.

További problémát jelent a digitális térben tapasztalható gyakori visszaélésekkel kapcsolatos információk nagy száma, amire magában az értekezésben is rámutatok. Az utóbbi években számos, nagy médiavisszhangot kiváltó adatvédelmi incidens történt – adatlopások, jogosulatlan adatmegosztások, illetve olyan üzleti modellek, amelyek a felhasználók adatainak piacosítására épülnek. Ezek az esetek megingatják a közbizalmat, hiszen látható az értekezés harmadik bekezdésében tárgyalt adatok szerinti mekkora mértékű már a személyes adatok illegális felhasználása, és megerősítik azt az általános vélekedést, hogy a vállalkozások elsősorban üzleti érdekeiket követik, és csak másodsorban vagy formálisan törődnek az adatvédelemmel. A probléma az is emellett, hogy egy vállalkozást nem feltétlenül tántorít el a tevékenységétől, és hiányos vagy téves adatvédelmi rendszabályainak alkalmazásától a hatósági büntetés.

Emellett az érintettek számára gyakran nem világos, hogy milyen jogokkal rendelkeznek, és hogyan tudnák probléma esetén azokat érvényesíteni. A GDPR számos jogot biztosít – így például a hozzáférés, törlés vagy tiltakozás jogát –, de ezek gyakorlati alkalmazása sokszor nem is alkalmazható, és az érintettek nem mindig érzik úgy, hogy érdemben tudnák befolyásolni az adatkezelést.

Végül, a bizalom alapvetően nemcsak szabályozás, hanem a gyakorlati tapasztalat kérdése is. Ha az érintettek úgy érzékelik, hogy adataikkal nem kezelik felelősen – például ha kéretlen reklámokat kapnak, vagy célzott tartalmakat küldenek nekik egy korábbi online aktivitásuk alapján –, akkor ez közvetlenül gyengíti a bizalmukat abban, hogy a vállalkozások betartják az adatvédelmi előírásokat. Ebben az értelemben a bizalom hiánya nem pusztán előítélet, hanem egyre inkább megtapasztalt valóság.

Összességében tehát elmondható, hogy az érintettek bizalmatlansága a vállalkozások GDPR-megfelelésével kapcsolatban több, egymást erősítő okra vezethető vissza: az adatvédelmi

tájékoztatók bonyolultságára, a nyilvánosságra került visszaélésekre, a jogérvényesítés nehézségeire és a mindennapi digitális élményekre. A szabályozás önmagában nem elegendő – valódi bizalom csak akkor épülhet ki, ha a vállalkozások következetesen, átláthatóan és empatikusan kezelik az adatvédelmet, és ezt a felhasználók saját tapasztalataikon keresztül is érzékelik.

1.2.1 Következtetések

A kérdőíves felmérés és a hozzá kapcsolódó szakirodalmi adatok egyértelműen rámutatnak arra, hogy bár a GDPR ismertsége magas, a rendelet értelmezése és gyakorlati alkalmazása komoly kihívásokba ütközik, különösen a fogalmi szintű ismeretek hiányosságai miatt. Ez a probléma azonban nem kizárólag a laikus (átlagos ismeretekkel rendelkező) állampolgárokat érinti, hanem a szakmai oldal, jellemzően a kutatási környezet adatai szerint az informatikai és mérnöki területen dolgozók is hasonló nehézségekkel szembesülnek.

A GDPR szabályozás hossza és jogi nyelvezete a műszaki szakemberek számára gyakran átláthatatlan, nehezen értelmezhető. Mivel a rendeletet alapvetően jogászok dolgozták ki, ugyanakkor annak implementálása, gyakorlati kivitelezése elsősorban informatikusokra, rendszermérnökökre és más műszaki szakemberekre hárul, ez a szakadék komoly problémákat eredményez. A mérnöki habitus – amely a gyakorlati megvalósítást, logikai rendszerek működtetését és optimalizálását helyezi előtérbe – nem kedvez a jogszabályokkal való elmélyült foglalkozásnak, kiemelten, ha azok túl hosszúak, vagy ellentmondásosnak tűnnek az új lehetséges műszaki megoldásokkal.

Ennek következtében a GDPR-t sok mérnök nem segítő keretként, hanem inkább akadályként vagy korlátozó tényezőként értelmezi, ami gátolja a jogszabály célkitűzéseinek teljesülését. Ez a hozzáállás nem feltétlenül rosszindulatból fakad, hanem inkább abból, hogy hiányzik a jog és a technológia közötti fordítói szerep, amely segítené a rendelet átemelését a jogi nyelvezetből a műszaki gyakorlatba.

A megoldás kulcsa részben a kommunikáció újra tervezésében rejlik. Szükség van a jogi és műszaki szakmák közötti párbeszédre (bridge-men képzés), közös képzésekre, és olyan értelmező anyagokra, amelyek hidat képeznek e két világ között. Emellett érdemes lenne a

rendeletet – vagy annak gyakorlati alkalmazását – mérnöki szemlélethez igazított útmutatókkal, sablonokkal, döntési fákkal, esetpéldákkal támogatni.

A GDPR célja, hogy megvédje az emberek személyes adatait illetve az érintettet, de ehhez nemcsak jogi akarat, hanem technikai együttműködés is szükséges – ehhez pedig az értelmezés és alkalmazhatóság javításán keresztül vezet az út.

1.2.2 Hipotézis igazolása

Hipotézisemet alátámasztják kérdőíves kutatásom eredményei is, amelyek egyértelműen rámutatnak arra, hogy a válaszadók többsége nemcsak bizonytalan az adatvédelemmel kapcsolatos jogairól és a kockázatok természetéről, hanem gyakran nem is bízik abban, hogy a szolgáltatók megfelelően és felelősségteljesen kezelik személyes adataikat.

A kutatás célja éppen ezért az volt, hogy feltérképezze a lakosság adatvédelmi tudatosságának szintjét, valamint a digitális biztonsággal kapcsolatos attitűdjeit, és választ adjon arra, milyen tényezők állnak a bizalmatlanság és a tudáshiány hátterében.

Különösen szembetűnő, hogy a megkérdezettek csupán 6,9%-a tudta pontosan megfogalmazni a személyes adat jogi definícióját, miszerint az minden olyan információ, amely valamely azonosított vagy azonosítható természetes személyre vonatkozik. Ez az alacsony arány arra utal, hogy az adatvédelemhez kapcsolódó alapvető fogalmak sem közismertek.

További jelzésértékű eredmény, hogy a „Véleménye szerint mik tartoznak a személyes adatok közé?” kérdésre a megkérdezettek 87,65%-a válaszolt ugyan, de közülük csak 78,82% adott érdemi, felhasználható választ. Ez azt jelenti, hogy minden ötödik válaszadó vagy nem tudta a választ, vagy nem volt képes azt értelmezhető módon megfogalmazni. Ez is alátámasztja, hogy a társadalom jelentős része nincs tisztában azzal, milyen típusú adatokra terjed ki az adatvédelem. Mindez azt jelenti, hogy a digitális környezetben való biztonságos részvételhez szükséges ismeretek nem elégségesek, ami fokozott kockázatot jelent a személyes adatok védelme szempontjából. Ez a tudáshiány könnyen vezethet a szolgáltatókba vetett bizalom megingásához is, hiszen ha a felhasználók nem értik, hogy adataik hogyan és miért kerülnek kezelésre, nagyobb eséllyel érzik magukat kiszolgáltatottnak. A hipotézis tehát — miszerint a társadalom nemcsak tájékozatlan az adatvédelem és kiberbiztonság területén, hanem bizalmatlan is a szolgáltatókkal szemben — a bemutatott kutatási eredmények alapján egyértelműen igazolható.

1.2.3 Ajánlások

A kutatási eredmények miatt szükségszerűvé vált egy oktatási anyag elkészítése annak érdekében, hogy az érintettek példákon keresztül értelmezni tudják az adatvédelemmel kapcsolatos alapfogalmakat.

Az „Adatvédelem alapfokon” című könyvben a kérdőíves kutatás részeredményei is feltüntetésre kerülnek. A könyv célja, hogy olvasmányos módon bevezesse az olvasót az adatvédelem és GDPR világába. Gyakorlati példák segítségével mutatja be az adatvédelmi alapelveket azok számára, akik a témában kevésbé jártasak. A könyv szakosodott társszerzője biztosítja az olvasmány szakmai színvonalát, a tudományos kutatás pedig kiegészíti a gyakorlati állapot bemutatásával a könyvet. [47]

Alapvetően az oktatás során törekedni kell arra, hogy már az alapvető fogalmakat tisztázzuk az érintetteknek, mivel a kutatás során bebizonyosodott, hogy ezekkel sincsenek tisztában a megkérdezettek. A legsarkalatosabb probléma az, hogy a személyes adatok vonatkozásában a megkérdezettek jellemzően adattípusokra gondolnak és nem összefüggésre. Azaz nem rendelkeznek arról információval, hogy a személyes adatok tekintetében azt az összefügést kell figyelembe venni, hogy az adatok akkor válnak személyes adattá, ha valakit egyértelműen tudunk azonosítani.

2. A Dark Weben és a Surface Weben megtalálható személyes adatok előfordulási formái és kockázatai

2.1 Áttekintés

Az interneten számos személyes adat fellelhető. Internetes tevékenységünk során számos személyes adatot és egyéb információt osztunk meg magunkról, sokszor nem is tudva erről. Ezek az adatok alkotják a digitális lábnyomunkat, amely információkat tartalmaz például az általunk meglátogatott weboldalakról, a közösségi médiában közzétett bejegyzéseinkről, a vásárlási szokásainkról, sőt akár a földrajzi helyzetünkről is. A digitális lábnyom és a személyes adatok szorosan összefüggenek, hiszen a lábnyomunk egy része közvetlenül azonosítható adatokat, például nevünket, e-mail címünket vagy bankkártyaadatainkat is tartalmazhatja. Ezek az információk értékesek lehetnek adatgyűjtő cégek számára, de sajnos a Dark Web szereplői és használói is élénken érdeklődnek irántuk.

Az internet több rétegében különböző módon jellenek meg személyes adataink. Míg a Surface Web a teljes internetnek csak egy kis része, addig a Deep Web egy sokkal nagyobb réteget

képvisel, amely rejtett, de nem feltétlenül illegális. A Dark Web pedig a Deep Web egy elzártabb, speciális része, amely a névtelenséget és általában a rejtett tevékenységeket támogatja.

A Dark Web tartalmának teljes kereskedelmi célú forgalma nem megbecsülhető. Az úgynevezett Dark Web árindex[33] átlagolt árakat vizsgál, vagyis az évente megjelenő kutatások képesek megmutatni a trendekben beállt változásokat. A táblázatban szereplő adatok a Dark Weben elérhető különböző típusú lopott adatok és szolgáltatások átlagos árait mutatják be röviden. Ezek az információk több, a Dark Web árindexével foglalkozó forrás elemzéséből származtatható természetesen csak becsülve.

Tétel	Átlagár (USD)	Megjegyzés
Hitelkártya adatok (CVV-vel)	$10–$110	Ár függ a számlaegyenlegtől és a régiótól
Online banki belépési adatok	$30–$100	Minimum $100 egyenleggel rendelkező számlákhoz
PayPal fiók (min. $1,000 egyenleg)	$120	Átutalási szolgáltatásokkal együtt drágább lehet
Kriptovaluta fiókok (Coinbase, Kraken)	$610–$810	Ellenőrzött fiókok

4. ábra 2023-2024 pénzügyi adatok értéke (kivonat) Forrás: PrivacyAffairs és a SOCRadar kutatása

Tétel	Átlagár (USD)	Megjegyzés
Teljes személyazonosság (név, SSN, születési dátum, e-mail, telefon)	$0.50–$10	Gyakran "Fullz" néven említik
Orvosi nyilvántartások	$250 vagy több	Értékes a biztosítási csalásokhoz
E-mail adatbázis (pl. 10 millió USA e-mail cím)	$120	Nagy mennyiségű adat privacyaffairs.com

5. ábra 2023-2024 személyhez köthető adatok értéke (kivonat) Forrás: PrivacyAffairs

[33] Az árindexet úgy állítják össze, hogy a darknet piacokon elérhető adatokat elemzik, és majd azokat kategóriák szerint rendszerezik és átlagolják. Az indexet rendszeresen frissítik, mivel az árak gyorsan változhatnak a kereslet, a kínálat és a kiberbiztonsági intézkedések változásai miatt. Ez egy olyan mutató, amely az illegális piactereken (darknet marketplace-eken) elérhető termékek és szolgáltatások átlagos árát követi. Ez az index segít megérteni a kiberbűnözők által kínált adatok és egyéb illegális szolgáltatások piaci értékét.

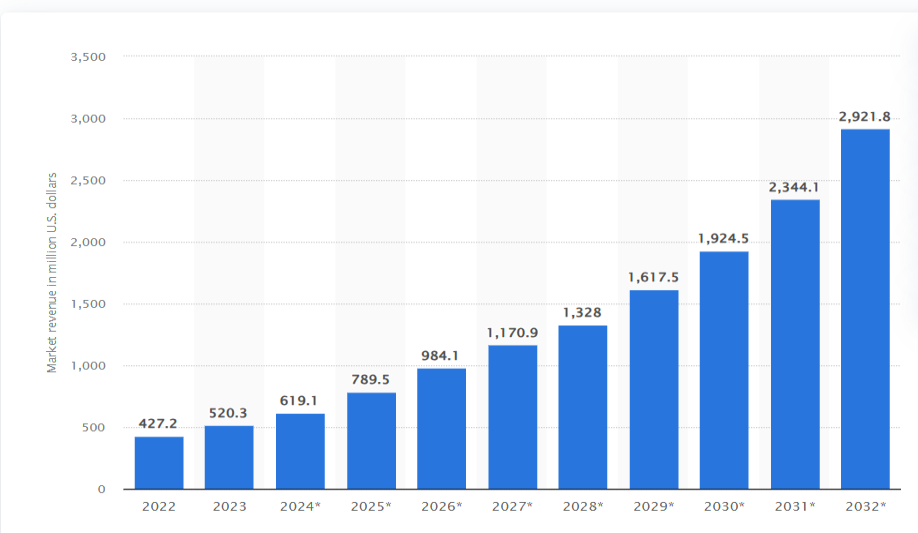
Tétel	Átlagár (USD)	Megjegyzés
Gmail fiók	$25–$80	Hozzáférés érzékeny információkhoz
Facebook fiók	$25	Használható adathalász támadásokhoz
Netflix fiók (1 éves előfizetés)	$1–$20	Előfizetéses szolgáltatásokhoz való hozzáférés
Uber sofőr fiók	$30	Jogosítvány és járműadatokkal együtt

6. ábra 2023-2024 szolgáltatásokhoz köthető adatok értéke (kivonat) Forrás: PrivacyAffairs

Tétel	Átlagár (USD)	Megjegyzés
Máltai útlevél (fizikai)	$4,000	Az egyik legdrágább hamis dokumentum
Francia útlevél	$3,000	Magas minőségű hamisítványok
EU vezetői engedély	$2,000	Különböző országokból származó példányok
USA jogosítvány	$150–$200	Államonként változó árak

7. ábra 2023-2024 dokumentumok értéke (kivonat) Forrás: PrivacyAffairs

A hitelkártyaadatok és az online banki belépési adatok, hamis amerikai zöldkártya vagy egy hamis európai uniós személyi igazolvány is könnyen beszerezhető ezeken a kereskedelmi platformokon. Az előbbiekben említett tételek mindegyike számos személyes adatot tartalmaz. [48] [49] [50] [51]



8. ábra Dark Web teljes éves becsült forgalma 2022-2032

A Staista információi szerint a Dark Web éves forgalmában 2027-től már drasztikus emelkedés prognosztizálható, ami 2032-re eléri az éves 2921 millió dollárt (körülbelül 1144 milliárd

forint). Ezen adatok alapján látható, hogy a személyes adatok kereskedelme is várhatóan hasonlóan fog emelkedni a Dark Weben, pontosabban a volumene leköveti a teljes növekedést. Az internet különböző rétegeiben különböző módon és számban találhatóak meg a személyes adatok. [52] [53]

A kiberbűnözők miatt a személyes adatok elektronikus kezelése napjainkban egyre nagyobb kockázattal jár. A digitális gazdaság és az e-társadalom átalakulása új kockázatokat teremtett. A kibervédelem, valamint a személyes adataink védelme pedig fontosabb mind társadalmi, mind személyes tekintetben is.

Egyre több esetben látjuk, hogy az Európai Unió intézményei és szakhatóságai, mint például az Európai Bizottság, Európai Uniós Kiberbiztonsági Ügynökség (ENISA[34]), az Unió számítógépes eseménykezelő központja (CERT-EU[35]), vagy az EUROPOL[36] felhívják a figyelmet a lakosság és a vállalkozások kibervédelmének fontosságára.

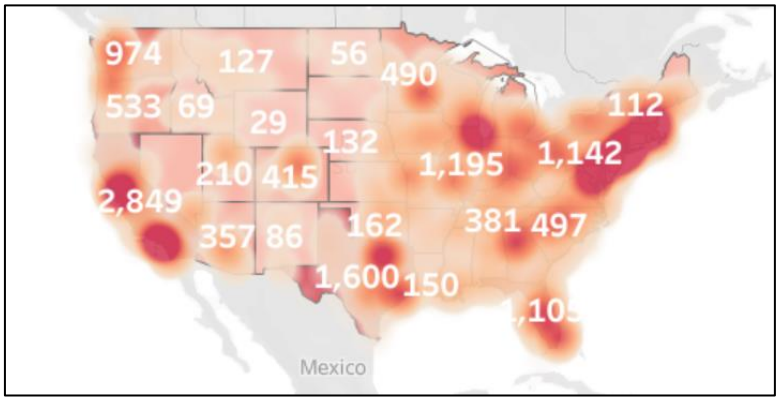
Fontos kiemelni azt, hogy a probléma egyre nagyobb méreteket ölt napjainkra. A történelem talán eddig ismert egyik legsúlyosabb adatvédelmi incidensének köszönhetően becslések szerint közel 2,9 milliárd személyes adat[37], köztük teljes nevek, címek és társadalombiztosítási számok kerültek fel a Dark Web piacterére. Egy amerikai közadatbázisból (adatbróker vállalkozás)[38] szerezték meg a jelentős mennyiségű adatot az elkövetők[39], akik az első lépésben magas áron (3,5 millió dollár) próbálták értékesíteni az adatbázist, majd ezt követően ingyenesen és nyilvánosan hozzáférhetővé tették. Ebben az esetben a vállalkozás az eset következményeként csődöt jelentett, mivel nem tudta kezelni az adatvédelmi kötelezettségekből származó anyagi kiadásokat. [54] [55]

Az AT&T[40] szintén hasonló incidenst jelentett 2024-ben. Első lépésben elkezdte értesíteni azon ügyfeleit, akik érintettjei voltak a kiberbiztonsági incidensnek. Az incidensnek az volt a jellemzője, hogy nem egy elszigetelt esetről volt szó, hanem minden ügyféltől kiszivárgott

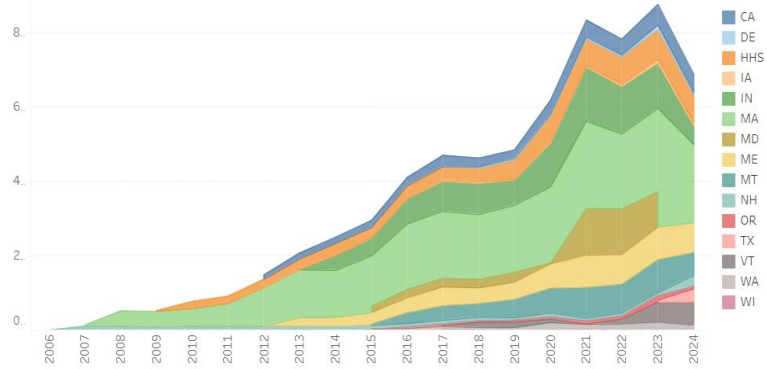
[34] European Union Agency for Cybersecurity - https://www.enisa.europa.eu/
[35] The Computer Emergency Response Team for the EU institutions, bodies and agencies https://cert.europa.eu/
[36] European Police Office
[37] 277 GB adat, összesen 2,9 milliárd rekorddal
[38] National Public Data adatkezelő vállalkozás másnéven adatbróker cég volt, amely alkalmazottak háttérellenőrzését végezte. Elsődleges szolgáltatásuk az volt, hogy nyilvános adatforrásokból információkat gyűjtsenek, beleértve a bűnügyi nyilvántartásokat, címeket és foglalkoztatási előzményeket, és ezeket az információkat eladásra kínálják.
[39] USDoD SXUL hekkercsoportot jelölték meg médiaforrások elkövetőknek.
[40] Az AT&T Inc. amerikai telekommunikációs vállalat. Gyökerei 1875-ig nyúlnak vissza, amikor is Alexander Graham Bell feltalálta a telefont. A 19. század folyamán az AT&T a Bell System anyavállalatává vált. Monopolhelyzetbe került az amerikai telefonpiacon, emiatt az Amerikai Igazságügyi Minisztérium 1984-ben nyolc vállalatra (Baby Bell) bontotta szét az anyavállalatot.

valamilyen adat. Az illetéktelen kezekbe került rekordok között telefonszámok, hívásnaplók és szöveges üzenetek voltak. A szolgáltató szerint a hívások és üzenetváltások tartalma nem kompromittálódott, tehát a támadók csak annyit tudtak, hogy interakció volt két ügyfél között egy adott csatornán. Viszont a metaadatok között szerepelt a kapcsolatfelvétel száma, valamint hívás esetén annak időtartama. Egyes esetekben az SMS-hez kapcsolódó cellaadatokat is tartalmazták a megszerzett információk, melyekkel hozzávetőlegesen megállapítható, hol tartózkodott a hívás/üzenet kezdeményezője és fogadója. [56]

Azt is figyelembe kell venni, hogy a személyes adatok kiszivárgása nemcsak globálisan mérhető, hanem szűk spektrumban (országonként/államonként) is látható napjainkban. A Privacy Rights adatai szerint is drasztikus adatvesztés/adatszivárgás észlelhető az Amerikai Egyesült Államokban a vállalkozások és a magánszemélyek esetében is. [57]



9. ábra Adatszivárgás eloszlási kép – Amerikai Egyesült Államok 2024. december



10. ábra Adatszivárgás 2006-2024. 15 amerikai állam tekintetében

A 3. ábra szerinti diagramm az adatvédelmi incidensek kronológiáját mutatja 15 amerikai államban. A diagramm csak azért 15 állam forrásadataira korlátozódik, mivel ezekben az államokban kötelező az adatszolgáltatás a bekövetkezett incidensek tekintetében. Az ábrán jól látható, hogy a szivárgások növekedésének volumene jelentős a számok tekintetében, és ez

várhatóan további növekvő tendenciát mutat majd, ami természetesen leköveti az 1. ábra emelkedését is.

Month, Day, ..	Org Name	Organizatio..	Breach Type	Total Affect..	Residents A..	Breach Loca..	Source	
December 7, 2024	Amergis Healthcare Staffi..	MED	HACK	11329	75	MD	ME	More Information...
December 6, 2024	Tactical Wealth Managem..	UNKN	UNKN	363	363	TX	TX	More Information...
December 5, 2024	Acadia Pharmaceuticals I..	UNKN	UNKN	UNKN	0	CA	TX	More Information...
	Anna Jaques Hospital	MED	HACK	316342	637	MA	ME	More Information...
	Ferring Pharmaceuticals I..	UNKN	UNKN	UNKN	2	UNKN	MA	More Information...
	Medical Affiliates of Cape ..	MED	UNKN	UNKN	12	UNKN	MA	More Information...
	Pathward, N.A.	UNKN	UNKN	375	375	SD	TX	More Information...
	Rebound Communications	BSO	UNKN	UNKN	1	UNKN	MA	More Information...
	Stryker Corporation	MED	UNKN	810	810	MI	TX	More Information...
December 4, 2024	Acadia Pharmaceuticals I..	MED	DISC	UNKN	UNKN	CA	CA	More Information...
	Acadia Pharmaceuticals, I..	MED	DISC	1	UNKN	CA	DE	More Information...
	American Engineers, Inc.	BSO	UNKN	UNKN	8	UNKN	MA	More Information...
	Brown, Gruttadaro, & Pra..	BSO	UNKN	UNKN	2	UNKN	MA	More Information...
	Compassionate Care Hosp..	MED	UNKN	1	1	TX	TX	More Information...
	Greater Lowell Technical ..	EDU	UNKN	UNKN	910	UNKN	MA	More Information...
	Metropolitan Council	UNKN	HACK	1	1	MN	NH	More Information...
December 3, 2024	Adams Community Bank	BSF	UNKN	UNKN	1	UNKN	MA	More Information...
	Ariel Corporation	UNKN	HACK	4	4	UNKN	NH	More Information...
	Bob's Discount Furniture	BSR	HACK	UNKN	UNKN	CT	CA	More Information...
			UNKN	UNKN	417	UNKN	MA	More Information...
	Bob's Discount Furniture, LLC	BSR	HACK	87	87	CT	NH	More Information...
				5222	72	CT	ME	More Information...
	Cardiology Associates of ..	MED	HACK	1514	1	AL	ME	More Information...
	CASTO	BSO	UNKN	UNKN	5	UNKN	MA	More Information...
	Central Carolina Insuranc..	BSF	HACK	3	3	NC	NH	More Information...
	Chemonics International, Inc.	BSO	HACK	26	26	UNKN	NH	More Information...
		NGO	HACK	263136	30	DC	ME	More Information...
		UNKN	UNKN	UNKN	179	UNKN	MA	More Information...
	Christine C. Shubert, Chap..	UNKN	UNKN	129514	129514	NJ	TX	More Information...
	DanceBUG INC	BSO	UNKN	UNKN	227	UNKN	MA	More Information...
	Joanne Symons, Inc. dba ..	BSR	UNKN	450	450	UNKN	TX	More Information...
	Keesal, Young & Logan	UNKN	UNKN	6642	6642	CA	TX	More Information...
	Kelsey-Seybold Medical G..	MED	UNKN	462	462	TX	TX	More Information...
	Kulicke and Soffa Industri..	BSO	HACK	1	1	UNKN	NH	More Information...

11. ábra Adatszivárgás rövid minta 2024. december 3-7.

A személyes adatok szivárgásának nagyságát jól ábrázolja a 4. ábra is, ahol látható, hogy egy szűk keresztmetszetben vizsgálva viszonylag rövid cikluson belül (4 nap) is hány entitást ért kiberbiztonsági incidens. Ha ebből még részletesebb vizsgálatot végzünk (incidens adatlapja szerint) láthatjuk például a Amergis Healthcare Staff esetében 11,329 személy elektronikus levélcíme került ki egy február 6-i adatszivárgás során, amelyről végleges jelentést december 7-én publikálta ki a hatóság[41]. A fenti viszonylag szűk kitekintésű adatszivárgások mértékéből is látható, hogy globálisan ennél nagyságrendekkel nagyobb a globális adatszivárgás mértéke.

2.2 Hipotézis

Az illegális és hanyag adatkezelés miatt a személyes adatok jelentős számban, folyamatos jelleggel kikerülnek a Surface Webre és a Dark Webre, ezzel egyre jelentősebb biztonsági kockázatot okoznak, és ez emelkedő tendenciát mutat majd a következő években is.

[41] Main Állam Főügyészség

Elgondolásom szerint, a Surface Weben a személyes adatok az esetek túlnyomó többségében emberi hanyagságból jelennek meg, vagy az adatvédelmi/információbiztonsági ismeretek hiánya miatt kerülnek ki a különböző adatbázisokból.

A Dark Weben kikerült/értékesített vagy előre megtervezett módon kiszivárogtatott személyes adatok viszont kiemelt kockázatot jelentenek mind a vállalkozások, mind pedig a magánszemélyek (természetes személyek) részére. Alapvetően a személyes adatok adatcsoportokban vagy adatkombinációk formájában jelennek meg, mivel illegális felhasználásuk csak így lehetséges. Hiszen elég belegondolni abba, hogy a legnagyobb kockázat akkor keletkezik, ha a támadók kombinálni tudják ezeket az adatokat, és azt részletes információkkal vagy pénzügyi lehetőségekkel párosíthatják, így közvetlenül kihasználhatják a sértett pénzügyeit, identitását vagy személyes biztonságát. A személyes adatok titokban tartása és biztonságos kezelése elengedhetetlen ahhoz, hogy elkerüljük ezt a kockázatokat.

Az internet különböző szintjein (rétegeiben) különböző módon és számban találhatóak meg a személyes adatok. A nyílt interneten[42] kevés és pontatlanabb adat lelhető fel, addig a Deep Web[43] és a Dark Weben[44] már nagy mennyiségű aktív adat is megtalálható, illetve akár illegálisan meg is vásárolható.

2.3 Eddigi kutatások

A Dark Webbel kapcsolatos eddigi kutatások átfogó képet nyújtanak annak technológiai alapjairól, az ott zajló illegális tevékenységekről, a felhasználói magatartásról, a pénzügyi rendszerekről és a jogi szabályozási kihívásokról. Ezek az eredmények hozzájárulnak a Dark Web megértéséhez és a hatékonyabb szabályozási és rendészeti intézkedések kidolgozásához. [58]

A témában számos tudományos cikk készült, hiszen a probléma nem most jelentkezett. Már 2010-ben is jelent meg tanulmány a témában, ahol a szerző hangsúlyozza azt, hogy az elektronikus kereskedés során az Amerikai Egyesült Államokban hogyan szükséges megvédeni személyes adatainkat. Valamint az elektronikus kereskedelemre milyen hatással van a személyes adatok védelme. Következtésében kihangsúlyozza azt, hogy a személyes adatok

[42] Surface web, visible web avagy az internet felületét vagy látható részét jelenti. Ez az internet azon része, amit a keresőmotorok meg tudnak találni, azaz indexelt oldalak.
[43] A deep web része olyan terület, amihez valamilyen regisztráció, azonosítás során lehet hozzáférni. A privát online banki oldalunk, a jelszóval védett felhő tárhelyünk a legjobb példa erre.
[44] Ahhoz, hogy hozzáférjünk az itt található tartalomhoz anonim böngészőre van szükségünk, ami lehetetlenné teszi valós identitásunk beazonosítását, kódolja üzeneteinket és tevékenységünket.

megfelelő védelme nagy mértékben hozzájárul a megfelelő digitális kereskedelem működéséhez. [59]

Egyes kutatások már vizsgálták a pénzügyi visszaélések, személyes adatok relációját. Ennek a 2019-es tanulmánynak a következtetése szerint személyes adataink eladóvá válnak a Dark Weben, és ezt már nem, mint lehetőség, hanem mint tényt kell kezelni. Elemzésük bizonyítékai azt mutatják, hogy egyesek ezeket az adatokat a vállalkozásuk bővítésére használják, mások pedig csak továbbadják. A tanulmányon keresztül végzett elemzés rávilágít arra a tényre, hogy egyre nagyobb az igény a személyes adatokra a különböző internetes illegális kereskedelmi fórumokon. A piac nagyobb szereplői egyre több szolgáltatást és árut nyújtanak illegális tevékenységek végzésére. Ezeknek a következményeknek a megértése nagy gyakorlati jelentőséggel bír a személyes adatok védelme és az érzékeny adatok biztonságának megőrzése szempontjából. Ezenfelül az illegális piac folyamatos nyomon követése létfontosságú a kiberbiztonsági szakértők és a rendvédelmi munkatársak részére, hogy tisztában legyenek az online fenyegetések egyre nagyobb mértékével. [60]

Számos összefoglaló tudományos munka készült arról is, hogy alapvetően a Dark Web fogalmával jellemzően az emberkereskedelemet, terrorizmust, kiberbűnözést kötik össze. [61]

Ez az állítás viszont a gyakorlatban téves képet is adhat, hiszen, ha egy Dark Weben használt keresőt használunk az nem ad feltétlenül illegális tartalmat, sőt a gyakorlatban elsősorban olyan nyílt releváns eredményeket kapunk, mintha a Surface Weben keresnénk.

2.4 Fogalmak egyértelműsítése

A kutatásom és elemzésem során, valamint az értékeléshez szükségessé vált néhány fogalom pontosítása és egyértelműsítése, mivel ezek a fogalmak a cikkekben több esetben egymás szinonimájaként vagy gyűjtőfogalomként jelent meg.

A Dark Web és a Deep Web tekintetében is készült számos tudományos mű, bár ezekben több esetben keverednek fogalmak, főleg a Deep Web és a Dark Web-en fellelhető információk esetében arról, hogy ezek törvényes/törvénytelen úton kerültek fel az említett rétegbe. [62] [63] [64]

Egyes tanulmányokban a Dark Web-et a Deep Web egy részének tekintik, ahol egyértelműen illegális tevékenység folyik. Vagy a Dark Web lehetőséget ad arra, hogy fedett műveleteket hajtsanak végre egymás ellen különböző szervezetek, nemzetbiztonsági szolgáltok.

Más kutatásokban a Dark Web és a Dark Net egymás szinonimái, és ez a terület egyértelműen a Deep Web része. Szó szerint idézve *„Az internetnek azonban vannak olyan részei, amelyeket a hagyományos keresőmotorok nem indexelnek, és rejtve maradnak a hétköznapi felhasználók elől. Ezt a rejtett részét nevezzük Deep Web-nek (mély web), amely becslések szerint a világháló körülbelül 96%-át teszi ki. A Deep Web-en belül található egy kisebb rész, amelyet leginkább illegális tevékenységekre használnak – ezt nevezzük Dark Web-nek vagy sötét hálónak.”*[45] [46]

A kutatás szempontjából a legfontosabb, hogy a Dark Web vagy más néven a Dark Net[47] az internet azon része, melyet nem indexelnek be a keresőrobotok. Ha egyszerűsíteni akarjuk akkor elmondható, hogy ha egy weboldal megtalálható a Google segítségével, akkor az a felszíni web vagy más néven Surface Web része, ha pedig nem, akkor az az oldal a mély web részét képezi.

A Surface Web fogalma az 1990-es évek elejére vezethető vissza, amikor az első keresőmotorok és weboldalak megjelentek. A felszíni web az internetnek az a része, amelyet a hagyományos keresőmotorok, mint például a Google, indexelnek és elérhetővé tesznek a nagyközönség számára. Az internet kezdeti időszakában, az 1990-es évek elején, amikor az első keresőmotorok és webindexelési technológiák megjelentek, az internet túlnyomórészt felszíni weboldalakból állt.

A Dark Web az 1990-es évek végén kezdett kialakulni, a "Dark Web" kifejezés pedig a 2000-es évek közepén vált szélesebb körben ismertté. Az első dokumentált használata a "Dark Web" kifejezésnek a szélesebb közönség előtt a 2000-es évek közepén jelent meg, amikor a TOR hálózat és más hasonló technológiák kezdtek elterjedni és ismertté válni. A Dark Web kifejezés népszerűsége azóta nőtt, ahogy egyre több figyelem irányult a hálózaton elérhető illegális tevékenységekre.

Ezek a fogalmak tehát az internet fejlődésének és a technológiai változásoknak köszönhetően alakultak ki, és váltak elterjedtté.

[45] Saiba Nazah , Shamsul Huda , Jemal Abawajy, Mohammad Mehedi Hassan: Evolution of DarkWeb threat analysis and detection: a systematic approach. IEEE ACCESS Received August 19, 2020, accepted September 7, 2020, date of publication September 15, 2020, date of current version September 30, 2020. 171796 Introduction.
[46] Saiba Nazah , Shamsul Huda , Jemal Abawajy, Mohammad Mehedi Hassan: Evolution of DarkWeb threat analysis and detection: a systematic approach. IEEE ACCESS Received August 19, 2020, accepted September 7, 2020, date of publication September 15, 2020, date of current version September 30, 2020. 171796 Introduction.
[47] Egyes esetekben hívják még így is, hogy dark net, sötét web, esetleg sötét oldal.

12. ábra Internet rétegei, Forrás: https://kangadesign.hu/darknet-dark-web.html

A kutatásom során a Dark Weben végzett megfigyelés esetében megállapítható az, hogy ezek az adatkereskedések alapvetően valamilyen illegális cselekményhez köthetőek, de ezen felül természetesen van legális adatkereskedelem is.

Az Európai Unión belül az adatkereskedelmet több jogszabály és rendelet szabályozza, amelyek célja az adatok védelme, az átláthatóság biztosítása és a tisztességes adatfelhasználás előmozdítása.

Az EU-ban az adatkereskedelem szigorúan szabályozott terület, ahol a személyes adatok védelme mellett egyre nagyobb hangsúlyt kap az ipari és közadatok megosztásának jogszerűsége is. A GDPR a személyes adatok védelmét biztosítja, míg az Adatkormányzási Rendelet (DGA[48]) és a várhatóan 2025-től hatályos Data Act az adatpiacot szabályozza. A Digitális Szolgáltatásokról Szóló Rendelet (DSA[49]) pedig az online platformokon történő adatfelhasználást szabályozza, különösen a digitális hirdetések és adatkereskedelem szempontjából.

Emiatt szükségszerű pontosítani az adatbrókerek fogalmát is. Az adatbróker vállalkozások olyan vállalkozások, amelyek adatokat gyűjtenek, feldolgoznak, rendszereznek, és értékesítenek más vállalatok számára. Ezek az adatok lehetnek személyes vagy nem személyes (piaci trendek, üzleti adatok). Az adatbrókerek szempontjából a GDPR korlátozásokat fogalmaz meg, pontosabban az adatbrókereknek a GDPR összes előírását ugyanúgy be kell tartani, mint

[48] Data Governance Act – DGA, 2022/868/EU
[49] Digital Services Act – DSA, 2022/2065/EU

mindenki más adatkezelőnek, mind alapelvek, mind pedig az érintetti jogok tekintetében, mivel ennek következtében az adatbróker csak akkor dolgozhat fel személyes adatokat, ha az érintett személy hozzájárult, szerződéses kötelezettség vagy jogos érdek áll fenn, illetve az adatkezelés jogszabályi előíráson alapul. Ebben az esetben az érintetteknek joguk van tudni, hogy adataikat milyen célból gyűjtik és értékesítik, valamint az adatbrókereknek biztosítaniuk kell az érintettek hozzáférési-, törlési-, és helyesbítési jogát, továbbá, ha az adatokat egy harmadik féltől szerezték, akkor az érintettet erről értesíteni kell.

Kutatásomhoz szorosan nem kötődött, de azt is figyelembe kell venni, hogy az adatbrókerek nem adhatnak el személyes adatokat az EU-n kívülre, kivéve, ha az adott ország megfelelő védelmet biztosít. Az adatbrókereknek, amelyek vállalati vagy közadatokat értékesítenek, a DGA szabályai is relevánsak, függetlennek kell maradniuk az adatok vevőitől és eladóitól. Az adatok felhasználásáról átlátható feltételeket kell biztosítaniuk. Az állami szektor által generált adatok csak meghatározott feltételekkel értékesíthetők.

Az adatbrókerek az EU-ban egyre inkább a szabályozott adatmegosztás felé kell hogy elmozduljanak. A régi, „szürke zónás” adatkereskedelem (ahol a fogyasztók nem tudták, hogy az adataikat továbbadták) erősen korlátozottá vált, és helyette egy transzparensebb, jogilag szabályozott adatpiac kezd kialakulni.

A fogalmak egyértelműsítése miatt pontosítom az adatvédelmi incidens és a kiberbiztonsági incidens közötti eltéréseket, mivel a kutatás során e két fogalom szorosan kíséri egymást. Az adatvédelmi incidens bekövetkezhet kiberbiztonsági incidens következtében, de attól függetlenül is. Ha egy adatvédelmi incidensről beszélünk, akkor azt 72 órán belül jelenteni kell a magyar Nemzeti Adatvédelmi és Információszabadság Hatóságnak (NAIH), viszont az alacsony kockázatú50 adatvédelmi incidenseket nem kell jelenteni, csak regisztrálni kell az adatvédelmi incidens nyilvántartásban.

Adatvédelmi incidens bekövetkezhet önállóan is, például, ha valaki egy magánszemélynek szánt e-mailt, amely személyes adatokat tartalmaz véletlenül a szervezet központi e-mail címére küld meg, amit mindenki más is lát, illetve amikor valaki egy minősített dokumentumot nyílt minősítésű hálózaton továbbít. Ez nem csak adatvédelmi incidens, hanem minősített adat

[50] Az adatvédelmi incidenst jelenteni kell a hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, GDPR 33. cikk (1) bekezdés.

védelmére vonatkozó szabályok megsértése, amely a Büntető Törvénykönyv hatálya alá esik, amely a minősített adat és a nemzeti adatvagyon elleni bűncselekmények körébe tartozik.

Olyan adatvédelmi incidensek esetén, amikor felmerül, hogy kibervédelmi incidenshez kapcsolódhat, két kivizsgálási út lehetséges.

Az egyik, amikor egy kibervédelmi incidens és a kivizsgálás során felmerül annak a gyanúja, vagy be is bizonyosodik az, hogy a Infotv. vagy GDPR körébe tartozó személyes adatok szivárogtak ki, vagy kerültek illetéktelenek kezébe.

Ebben az esetben az eseménykezelő központnak értesítenie kell a kibervédelmi incidens bejelentőjét, aki általában az elektronikus információbiztonsági felelőst értesíti (a továbbiakban: EIRBF). A kijelölt EIRBF értesíti az adatvédelmi tisztviselőt, aki a 72 órás időkorlátot figyelembe véve értesíti a NAIH-ot.

Az olyan esetekben, amikor az adatvédelmi incidenst a kibervédelmi incidenskezelők fedezik fel, gyakran merül fel az a kérdés, hogy miért nem ők jelentik az adatvédelmi tisztviselőnek közvetlenül? Ilyenkor azt kell figyelembe venni, hogy a CSIRT[51]/CERT[52] feladatai közé nem tartozik az adatvédelmi incidensek kezelése, ez minden esetben az adatvédelmi tisztviselő dolga. És mivel a CSIRT/CERT az EIRBF-el van kapcsolatban, hivatalosan csak neki jelezhetik.

Van egy másik eset is, amikor bejelentésre kerül egy adatvédelmi incidens és a kivizsgálása során felmerül annak a lehetősége, hogy esetleg kibervédelmi incidens állhat a háttérben. Ebben az esetben az előbb már említett folyamat megfordul, és az adatvédelmi tisztviselő az EIRBF-en keresztül kéri az incidens kivizsgálását a CSIRT/CERT-től, aki a vizsgálatai során megállapítja, hogy történt-e kibervédelmi incidens amire vissza lehet vezetni az adatvédelmi incidenst vagy nem. Amikor az adatvédelmi tisztviselő kéri az eset kibervédelmi szempontból történő kivizsgálását, akkor abban az esetben nincs olyan határidő, mint az előző esetben, hogy a tudomására jutástól csak 24 óra áll rendelkezésére, hogy kérje a vizsgálatot.

Az említett folyamatokból is látszik, hogy lehet összefüggés a kibervédelmi incidens és az adatvédelmi incidens között, de a kettő nem keverendő össze. Az adatvédelmi incidens

[51] Computer Security Incident Response Team - informatikai szakemberek azon csoportja, amely egy szervezet számára szolgáltatásokat és támogatást nyújt a kiberbiztonsággal kapcsolatos vészhelyzetek értékelésével, kezelésével és megelőzésével, valamint az incidensek elhárítására irányuló erőfeszítések koordinálásával kapcsolatban.

[52] Computer Emergency Response Team - információbiztonsági szakértők csoportja, amely a szervezet kiberbiztonsági incidensek elleni védelemért, azok észleléséért és az azokra való reagálásért felelősek.

kivizsgálásába, amennyiben közepes vagy súlyos adatvédelmi incidens történik, akkor az azt kivizsgáló bizottságba a HM-nél már eleve bevonásra kerül az EIRBF, de az incidenskezelő központ nem. Őket az EIRBF-nek kell értesítenie, ha ilyen irányú kivizsgálást szeretne.

Fontos megjegyezni, hogy soha sem lehet evidenciaként kezelni, hogy az adatvédelmi és a kiberbiztonsági incidens együtt bekövetkezik. Külön-külön is bekövetkezhetnek, de az igaz, hogy sok esetben a kiberbiztonsági incidens során kiszivároghatnak személyes adatok is.

Megállapításom, hogy az adatvédelmi incidens és a kiberbiztonsági incidens között van összefüggés, de nem ugyanaz a definíciójuk.[53] Összefoglalva, hogy a kiberbiztonsági incidensnél az adatokat védjük, az adatvédelmi incidensnél viszont az érintettek jogaira és szabadságaira jelentett kockázatot.

2.5 Az Internet új architektúrája és a személyes adatok összefüggése

Az internet architektúrájának jövőbeli változásai jelentős hatással lesznek a személyes adatok továbbítására és kezelésére. Az adatvédelem integrálása az alapvető technológiai struktúrákba minimalizálhatja a személyes adatok felesleges továbbítását. Ennek következtében jobban illeszkedhet a GDPR követelményeihez, pontosabban a "minimális adatgyűjtés" és az "adatok célhoz kötöttsége" elveinek vonatkozásában könnyeb megfelelősséget biztosítanak majd. Az olyan technológiák, mint a blokklánc, elősegítik a személyes adatok decentralizált tárolását és kezelését, amelyben a felhasználók nagyobb kontrollt gyakorolhatnak adataik felett, ellenben viszont a törléshez való jogot nem tudják gyakorolni jelenleg. Ez a modell csökkentheti a központosított adatfeldolgozási kockázatokat, aminek következtében az adatlopások/szivárgások részben elkerülhetőek. Viszont új típusú kihívásokat generál a decentralizált adatok anonimizálásának vagy törlésének biztosítása terén.

Az IPv6 által biztosított egyedi IP-címek[54] és az IoT-eszközök elterjedése exponenciálisan növeli a hálózatba kapcsolt eszközök számát, így az adatforgalom is nő. [65] A megnövekedett adatforgalom kezelése során kiemelten fontos az adatvédelem biztosítása, például az érzékeny

[53] Interjú Király Ágnes őrnaggyal, 2025.02.28

[54] A protokoll az IPv4 hibáit megszüntette, emellett új szolgáltatásokat is tartalmaz. Ilyen például a megnövelt, nagyobb címtartomány és a közvetlen végponti címezhetősége. Az IPv6-címzés szerves része az IPsec, ez hálózati szinten nyújt lehetőséget arra, hogy a kommunikációban részt vevő felhasználók hitelesen azonosítsák egymást, valamint az egymás közt zajló adatforgalmat titkosítsák tunnel-en keresztül. A 128 bites címtartomány több ezer milliárd eszköz számára biztosíthat IP-címet, így gyakorlatilag kimeríthetetlen a kapacitása. Lefordítva ezt a háztartásokra, az otthonokban minden internetképes eszköz önálló IP-címet kaphat, így azok zavar nélkül kommunikálhatnak egymással.

illetve különleges adatok titkosítása, a helyi adatfeldolgozás (edge computing) előtérbe helyezése. Az adatkezelés, ezen belül különösen az adattovábbítás optimalizálásában egyre nagyobb szerepet kapnak az MI-alapú rendszerek, amelyek gyorsabban tudnak adatokat továbbítani és elemezni. Az MI alapú rendszerek által gyűjtött és továbbított adatok potenciálisan új adatvédelmi kockázatokat teremtettek meg, mivel az MI működésének alapját adó algoritmusok átláthatósága korlátozott (fekete doboz). Az adatlokalizáció követelményei miatt az adatok globális továbbítása komplexebbé válhat.

Az adatlokalizáció szempontjából a követelmények az MI és a személyes adatok összefüggésében kulcsfontosságú szerepet játszik a globális adatáramlásban, és az adatvédelmi szabályozások egyre szigorúbb szabályokat állítanak a személyes adatok védelme érdekében. Az adatlokalizáció az a gyakorlat, hogy az adatokat a feldolgozáshoz vagy tároláshoz egy adott országban vagy joghatóság területén kell elhelyezni, így azok nem kerülhetnek át más ország területére, ha azok nem biztosítanak megfelelő védelmet ezeknek.

A GDPR az Európai Gazdasági Térségen (EGT)-ben irányadó szabályozás, és az adatkezelési tevékenységek során szigorúan szabályozza, hogy hogyan lehet személyes adatokat külföldre továbbítani. Az adatlokalizációs követelmények különösen fontosak a mesterséges intelligencia alkalmazásoknál, mivel az MI rendszerek gyakran nagy mennyiségű adatot használnak, amelyek gyakran személyes adatokat is tartalmaznak.

A személyes adatok nem kerülhetnek az EGT kívüli országokba, kivéve, ha az adott ország biztosítja a GDPR által elvárt szintű adatvédelmet. A harmadik országok adatvédelmi szintjét az EU Bizottság értékeli.

Az EGT-országokba történő adatátvitel belföldi adattovábbításnak számít, de más országok esetében megfelelő biztosítékokat kell alkalmazni. Ez lehet például Adatvédelmi szerződések (SCCs[55]). Bizonyos esetekben az EU szabályozásai megkövetelik, hogy az adatokat lokálisan, vagyis az EU-n belül tárolják, hogy megakadályozzák a személyes adatok harmadik országba történő kiszivárgását vagy nem megfelelő védelmét. Ha az MI alkalmazások érzékeny személyes adatokat kezelnek (pl. egészségügyi adatok), akkor különösen fontos a lokális tárolás és feldolgozás, hogy az adatokat megfelelő védelmi előírások [56]mellett kezeljék.

[55] Standard Contractual Clauses

[56] Az új kibervédelmi törvény erre vonatkozóan tartalmaz rendelkezéseket, illetve a visszaélés-bejelentésről szóló tv. is állít fel korlátokat.

Az új architektúrák interoperabilitási problémái adatvédelmi kockázatokat jelentenek. Az adatok anonimizálása vagy törlése bonyolultabbá válhat decentralizált rendszerekben.

Kiemelet probléma, hogy a jelenlegi helyzetben a biztonsági követelmények csak utólagos rétegként kerülnek hozzáadásra, nem pedig a rendszer szerves részeiként. Ez különösen jelentős hatással van a személyes adatok továbbítására, mivel ezek biztonsága gyakran az infrastruktúra gyenge pontjain múlik.

Az új architektúrák – például tartalomorientált hálózatok – előtérbe helyezhetik az adatbiztonságot, például az adatok tartalom alapú azonosításával és titkosításával. Ez azt eredményezheti, hogy az adatforgalom során nem az eszközök vagy a hálózati útvonalak, hanem maguk az adategységek határozzák meg a védelmet.

Az új architektúrák kísérleti tesztkörnyezetekben való kipróbálása (például az amerikai GENI[57] vagy az európai FIRE[58] projektek) lehetőséget ad arra, hogy a személyes adatok kezelését érintő technológiai megoldásokat valós körülmények között értékeljék. Ezek a teszterületek segíthetnek a biztonság, az interoperabilitás, valamint az adatkezelés szabályozási és technikai feltételeinek finomhangolásában.

A GENI és a FIRE két jelentős kutatási és kísérleti infrastruktúra-projekt, amelyek célja az internet lehetséges jövőjének kutatása és a hálózati technológiák fejlesztésének támogatása. Mindkettő olyan tesztkörnyezetet biztosít, ahol új hálózati protokollokat, architektúrákat vagy szolgáltatásokat lehet valós környezetben kipróbálni.

Az új várható internetes környezet (Web 3.0) nemcsak technológiai szinten hoz új megoldásokat, hanem alapvető változásokat vezet be az adatvédelmi megközelítések területén. Az architektúra tervezésében a biztonság és a felhasználói adatok feletti kontroll már nem utólagos kérdés lesz. Az említett biztonsági és adatvédelmi követelményeknek az alapokba integrálva kell megjelenniük. Ez a szemléletváltás elengedhetetlen ahhoz, hogy a jövő internete hatékonyan és etikusan tudjon működni a személyes adatok kezelésének növekvő kihívásai közepette, mivel a fő jellemzője, hogy decentralizált technológiákra épül, például a blokkláncra, és célja, hogy a felhasználók visszanyerjék az irányítást a saját adataik felett. Az adatok nem központi szervereken, hanem elosztott hálózatokon tárolódnak. A felhasználók digitális

[57] Global Environment for Network Innovations - A National Science Foundation (NSF) indította, és célja a hálózati és elosztott rendszerek új generációjának fejlesztése és tesztelése.
[58] Future Internet Research and Experimentation – Az Európai Bizottság az FP7 és Horizon 2020. keretprogramokon belül indult, és a kutatás célja a egy Kutatási és tesztelési infrastruktúra létrehozása a jövő internettechnológiái számára.

pénztárcákkal jelentkeznek be, nem adnak meg e-mail címet vagy jelszót. Így maga az érintett dönt arról, milyen adatot oszt meg, kinek és mikor.

2.6 Kutatás módszertana

Az empirikus kutatási módszer kiválasztására azért került sor a részkutatás során, mert a téma konceptuális kerete ezt követelte meg. Pontosabban a hipotézis igazolásához gyakorlati életből vett eredmények szükségesek, mivel a rendelkezésre álló ismeretanyag megbízhatatlansága alapján a felmerült problémára nem tudtam volna választ adni. Ez azonban nem jelentette azt, hogy a kutatás az elméleti meghatározottság nélkülözésével elkezdhető lett volna. Valamint ezzel a kutatási módszertan segítségével az eredményeket leíró jelleggel tudtam közölni.

Gyakorlatban a kutatás során személyes adatokat kerestem az internet kettő előzetesen említett rétegében. A keresés során a jogszabályi keretek figyelembevételével a személyes adatokhoz köthető fogalmakat is kerestem. A fellelt információkat elemeztem, és értékeltem majd ebből vontam le a következtetéseket, továbbá esettanulmányokat végeztem annak érdekében, hogy hipotézisemet igazolni tudjam. [66]

2.7 Kutatás környezete

2.7.1 Kutatás jogszabályi környezet

Az interneten végzett tudományos kutatást jogszabályi környezet határolja be. Kutatásom környezetét elsősorban az általános adatvédelmi rendelet GDPR[59] és az Infotv.[60], valamint a Btk.[61] határozzák meg, amelyeknek maradéktalanul meg kell felelni. Kutatásom során számos alkalommal nagy mennyiségű személyes adatot leltem fel, ahol alapvetően olyan visszaélésekről beszélünk, amikor az elkövető szándékosan megszegi a személyes adatok védelméről szóló jogszabályi rendelkezések valamelyikét. Haszonszerzési célból vagy jelentős érdeksérelmet okozva jogosulatlanul vagy céltól eltérően személyes adatot kezel. Itt hozzá kell fűzni azt is, hogy akkor is bűncselekmény vagy szabálysértés történik, ha elmulasztja az adatbiztonsági intézkedéseket betartani vagy betartatni az elkövető.

Az adatvédelem általános kereteit az EGT-tagállamok területén a GDPR szabályozza, kivéve a bűnügyi irányelv[62], honvédelmi és nemzetbiztonsági adatkezeléseket, amelyek esetében –

[59] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről
[60] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
[61] A Büntető Törvénykönyvről szóló 2012. évi C. törvény
[62] Nem teljesen tagállami hatáskör, az EDPB ennek is a végső felügyeleti szervezete.

mivel ez a terület tagállami szabályozási hatáskör – az Infotv. az irányadó jogszabály, hiszen műveleti adatokról beszélünk, azok jellegétől függetlenül.

Meg kell azonban jegyezni, a bűnügyi adatkezelések esetében szintén egységes uniós alapok érvényesülnek.[63] Amennyiben ezen jogszabályok megszegésére kerül sor, elsősorban a személyes adatokkal visszaéléssel kapcsolatos Btk. 219. §-a merül fel, mint alkalmazandó jogszabály.

A műveleti – bűnüldözési, honvédelmi, illetve nemzetbiztonsági célú – tevékenységek esetében a Btk. 219.§-át az Infotv. tölti meg tartalommal, azaz az Infotv. szabályait kell megszegnünk ahhoz, hogy ezen törvényi tényállás alapján minősüljön a tettünk. Amennyiben különleges adatokkal kapcsolatban történik a cselekmény elkövetése (például egészségügyi vagy bűnügyi adattal kapcsolatban), abban az esetben súlyosabb a megítélés, illetve akkor is, ha mindez hivatalos személyi minőségben történik. A büntethetőség alól a kutatásra hivatkozás nem felmentő indok, ezért a hipotézis igazolásához is minden adatot anonimizálni kellett annak érdekében, hogy ne okozzon jelentős sérelmet azzal, hogy a Dark Weben talált személyes adatot elemzünk. A kutatásban minősített adatokat sem használtam fel, mivel a kutatási tevékenység nem számít nemzetbiztonsági munkának, valamint nem is volt annak célja. Az anonimizált adatokat azért mutatom be, hogy az olvasó jobban megérthesse a kockázat jelentőséget.

Amennyiben az adott személyes adat kezelése nem az Infotv. hatálya alá tartozik (azaz nem bűnüldözési, honvédelmi, illetve nemzetbiztonsági célú tevékenységgel kapcsolatos), abban az esetben a GDPR szabályai alkalmazandók a közzétételre. Ebben az esetben a GDPR 5. cikkében foglalt alapelvek betartásával kezelhető a személyes adat a kutatásunk során (célhoz kötöttség) és a 6. cikk (1) bekezdésében található jogalapok egyikére kell tudni jogszerűen hivatkozni azért, hogy ezen személyes adatok kezelése (gyűjtése, tárolása, közzététele) megfeleljen a jogszabályi követelményeknek. Természetesen kutatásom során tárolni vagy közzétenni nem kellett az adatokat. Ebben az esetben a kutatásunk során vagy az érintettek hozzájárulását kell kérni (kevés az esélye annak, hogy a Dark Weben árult személyes adatok érintettjei ilyet adnának), illetve a jogos érdekünkre hivatkozva kezelhetjük még ezen adatokat. Ebben az esetben kétséges, hogy a személyes adatok közzététele esetén a kutatási érdekünk felülírná az érintettek érdekeit, valamint jogait és szabadságát, különösen arra tekintettel, hogy a kutatásunk

[63] Személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/680 európai parlamenti és tanácsi irányelv (bűnügyi adatvédelmi irányelv, LED)

eredményét anonimizált adatokkal is be lehet mutatni. Így ennek következtében a kutatás során nem tároltam (nem mentettem merevlemezre további felhasználásra csak anonimizálás idejére) a megszerzett adatokat, kizárólag az anonimizálási eljárás során használtam őket, amennyiben az szükséges volt.

Különleges adatok esetében a GDPR 9. cikk (1) bekezdése egyértelműen tiltja az adatok kezelését, illetve ezen személyes adatok csak akkor kezelhetők, ha a 9. cikk (2) bekezdésében található kivételek egyikére jogszerűen tudunk hivatkozni, valamint megfelelünk a 6. cikk (1) bekezdésében felsorolt jogalapok egyikének is. A kutatásunk során ebben az esetben is azt a közzétételi módot választottam, hogy anonimizáltam a személyes adatokat.

Ezzel az eljárással egyrészt nem sértem meg az adatvédelemre vonatkozó rendelkezéseket, másrészről nem merítjük ki a Btk. 219.§-ban foglalt törvényi tényállást sem, mivel az anonimizált adatok nem tartoznak sem a GDPR, sem az Infotv. hatálya alá mindaddig, ameddig anonimizáltak maradnak. Éppen ezért nagyon fontos, hogy a kutatás során az anonimizálást úgy végeztem el, hogy az végleges legyen, azaz az érintettek újra azonosítása ne történhessen meg.

2.7.2 Kutatás műszaki környezete

Kiemelten fontos, hogy a Dark Weben végzett kutatást/keresést óvatosan közelítsük meg annak szabályozatlan, sajátos természete miatt. Ebben az esetben mindig ügyelni kell arra, hogy saját online biztonságunkat és az adatvédelmet helyezzük előtérbe.

- Alapvető feltétel egy teljesen erre a célra használható informatikai eszköz, ami semmi estre sem köthető névhez, azaz nem tartalmaz semmilyen személyes adatot;
- Biztonságos operációs rendszert kell alkalmazni, például a Tails vagy a Whonix, bár ez nem szigorú kritérium;
- A csatlakozáshoz a VPN használata alapvető kritérium, ahol figyelembe kell venni, azt hogy az adatvédelmet és a biztonságot részesítsük előnyben. A VPN segítségével elrejthetjük az IP-címünket, és titkosítjuk az internetkapcsolatot, ezzel is növelve az anonimitást. A VPN használata önmagában nem garantálja a teljes névtelenséget vagy védelmet természetesen. [67]
- A kutatáshoz alkalmazni kell a VPN mellett valamilyen anonimizálást biztosító hálózatot is (ACN[64]).

[64] Anonymous Communication Network

A TOR-ra alapvetően azért esett a választás, mert biztosítja az anonimitást a kutatás során. természetesen több ilyen ACN is működik, valamint ezzel egyidőben lehet McAfee VPN-t is alkalmazni. Ebben az esetben VPN over VPN kapcsolaton keresztül lépünk be a TOR rendszerbe. Az alábbi táblázatban feltüntettem azt is, hogy a TOR mellett más applikáció is alkalmazható erre a célra.

	Freenet	I2P	TOR
Domain/hozzáférés	CHK:SSK:	B32.i2p sites[65]	.onion sites
Rejtett hozzáférés	nem	nem	igen
Rejtett tárolás	igen	nem	nem
Arhitektúra	Elosztott	Decentralizált	Decentralizált

13. ábra Dark Web ACN-ek

2.7.3 Kutatás során felmerült problémák és megoldások

Alapvetően és döntően a kutatás során két jelentősebb problémakör merült fel. A Dark Weben végzett kutatás során felkeresett elektronikus felületek folyamatosan változnak[66]. A felületekhez a hozzáférés csak célszoftverekkel lehetséges. Emellett az anonimitás és a rendszer természete miatt az elektronikus felületek nem állandó címen szerepelnek. Ennek következtében hivatkozás két alapvető szabálya:

- a hivatkozott mű visszakereshetősége;
- illetve a választott hivatkozási forma következetes alkalmazása ebben az esetben nehezen alkalmazható.

További probléma, hogy az internetes források megadásánál szintén fontos az összes elérhető bibliográfiai adat megadása, pontosabban nem elégséges csak a hiperlink/URL azonosítása. A Dark Web esetében ez viszont nem is értelmezhető, mivel nem indexált és állandó web felületekről beszélünk.

[65] A Torhoz és a Freenethez hasonlóan az I2P-nek is van saját Dark Web tartománya, amely a számítógépén tárolt mikrowebhelyekből áll. Ebben az esetben a tartomány b32.i2p végződésű. Ez kizárólag anonim I2P hálózaton keresztül érhető el.

[66] Az Onion szolgáltatások és az IP cím el van rejtve, hogy minél nehezebben találják meg és azonosítsák a forrást, működtetőt. Az onion szolgáltatás címe automatikusan jön létre, így az operátoroknak nem kell domain nevet vásárolni. Az alkalmazott kriptográfia miatt a .onion URL-cím lehetővé teszi a Tor számára, hogy megbizonyosodjon arról, hogy a megfelelő helyre csatlakozik, illetve hogy a kapcsolatot nem manipulálják.

Természetesen megoldás lehet a tudományos hivatkozás kialakítása esetén, ha a Dark Web oldal alapvető adataival rendelkezünk, mint:

- szerző, vagy készítő (ami szintén fiktív és többnyire valótlan);
- weboldal esetlegesen feltüntetett neve, és az ehhez tartozó URL cím;
- képernyőfotó készítése.

További lehetőség BibTex alkalmazása, amely esetében hivatkozásunk az alábbi formátum lesz, mint például:

@misc{Darknet:****,

title={**** - The Better & Cheapest FUD Ransomware + C&C on Darknet},

howpublished={\url{http://****.onion}},

note={Accessed on 12.03.2017}

}

Kiemelt problémát jelent az, hogy a Dark Weben végzett kutatás nem reprodukálható újra, mivel nem kerül rögzítésre sehol sem az adott HTML felület. Természetesen ennek oka a Dark Web speciális természete, ahol az anonimitás a felhasználók alapvető elvárása.

A kutatási eredmények bizonyításához vagy visszakereshetőségéhez álláspontom szerint három lehetőség van.

A kutatási eredmények (oldalak) mentése helyileg. A legtöbb TOR böngésző lehetőséget kínál az oldalak helyi mentésére HTML formátumban. Ez a módszer egyszerű, és a mentett fájl offline is használható.

Az oldalról képernyőképet készítünk, amelyet később visszanézhetünk. Ez különösen hasznos, ha az oldalon található információk gyakran változnak, mint az én esetemben. Egyes böngészők lehetővé teszik, hogy egy oldalt PDF formátumba elmentsük. Ez megőrzi az oldal kinézetét és a legtöbb tartalmát is.

Továbbá, a HTTrack vagy wget programmal teljes weboldalakat letölthetünk helyileg. Azonban a nagy mennyiségű adat letöltése figyelmet vonhat magára, és bizonyos webhelyek ellenlépéseket tehetnek, ami ebben a környezetben jellemző.

2.7.4 Keresési ciklus és tapasztalatok, folyamatok

Kutatásom első lépcsőjében kulcsszavas keresést alkalmaztam annak érdekében, hogy megfigyeljem azt, hogy milyen keresési eredményeket adnak a Google, Bing, Yahoo kereső motorjai. A keresés során a „Stolen social security numbers", „ID card number", „ID number", „personal data" kulcsszavakra kerestem rá a nyilvánosan elérhető keresőmotorokkal. A vártnak megfelelően olyan eredményeket és szponzorált kiberbiztonsági cikkeket kaptam találatul, amelyek természetesen nem tartalmaztak személyes adatokat. Ebből megállapítható, hogy a nyílt interneten való kulcsszavas keresés teljesen eredménytelen módszer, mint ahogy az várható volt. Ennek oka, hogy a keresőmotor egy program vagy alkalmazás, amely egy adott felhasználó által szabott feltételek alapján információkat keres valamilyen internetes környezetben. Az internetes keresőmotorok jellemzően két részből állnak, az egyik összegyűjti az információt[67], a másik pedig rendszerezi. A rendszerezés során az előre indexelt oldalakat az indexelő elemzi majd ezután metaadatokat társít ezekhez, aminek a segítségével a keresési kritériumok alapján relevancia szerint sorrendet állít fel. Amikor a felhasználó elindít egy keresést, a kereső az index segítségével kiválogatja a kritériumoknak megfelelő oldalakat, a hozzájuk társított metainformációk alapján sorrendbe állítja őket, és az összes találat közül a relevancia szerint felsorolja azokat.

A kutatás második lépcsőjében egy közösségi hálózaton végeztem megfigyelést. A közösségi hálózatokon kiemelten sok feltöltött személyes adatot tárolnak vagy kezelnek magánszemélyek.

A fenti eredmények olyan adatok, amelyeket tulajdonosuk egyértelműen saját maga önállóan külső hatások nélkül osztott meg téves beállítások következtében vagy esetleg egy ellenérdekeltségű fél elleni lejáró kampány során. Nem vesszük ide azokat az adatokat, amelyek a közösségi portálok által üzemeltetett adatlapokon szerepelnek, mivel azok csak egy zárt csoport számára láthatóak. Valamint egyes magánszemélyek segítő szándékkal is feltöltenek személyes okmányokat annak érdekében, hogy esetlegesen felkutassák az említett okmányok tulajdonosát, miután elvesztette ezeket.

A harmadik lépcsőben olyan fogalmakat kerestem, mint „personal data breach", „personal data leak", amelyek személyes adatok kiszivárgásával kapcsolatba hozható eredményeket produkáltak. Bár hasonlóan az első lépcsős módszerhez a keresés nem adott konkrét eredményt

[67] Robot vagy web crawler.

viszont rámutatott azokra az incidensekre, amelyek esetében személyes adatok is érintettek voltak. Azaz ily módon az alábbi információk nyerhetők ki:

- incidens ideje (további kutatáshoz tájékoztató jellegű adat);
- melyik hekkercsoport vállalata fel, van-e azonosított elkövető (további kutatáshoz mérvadó adat);
- mi szivárgott ki pontosan, van e ProofPack[68] (további kutatáshoz relevancia indikátor);
- ki az érintett, ki jelentette az incidenst (további kutatáshoz mérvadó adat);
- kutatás során a hekkercsoportok képernyőfotók segítségével bizonyítják azt, hogy rendelkeznek az említett adatállományokkal. A vásárlók/érdeklődők a képernyőfotók segítségével értékelhetik előzetesen azt, hogy megvásárolják-e az említett adatállományokat.
- A Dark Web-en is lehetőségünk van személyes adatok megtalálására keresőmotorral annak ellenére, hogy nem indexelt weblapokat tartalmaz. Ebben az esetben a kutatás során azt vettem alapul, hogy a Surface Web mintához hasonlóan először a fórumokat célszerű felkeresni. Egy ilyen kulcsszavas keresés esetében egy esettanulmányon keresztül lehet jól látni, hogy könnyűszerrel lehet személyes adatokhoz hozzájutni ebben a rétegben. És az előzetesen végrehajtott Surface Web kereséssel szemben itt viszont konkrét adatokat találunk. Ebben az esetben alkalmazható a TheHiddenWiki[69], az Ahmia[70], a Torch[71], TorLinks[72], NotEvil[73], Grams[74], Candle[75] vagy a TOR OnionLand[76]kereső is.

2.7.5 Kutatási eredmények

A komplex kutatás során a Surface Web kerestem olyan híreket, amelyek eredménye vagy következménye megjelenik a Dark Webes felületeken, majd képernyőfotók segítségével mutatom be az eredményeket. A harmadik lépcsőben olyan fogalmakat kerestem „personal data

[68] A ProofPack a DarkWeb-en jellemzően árucikként jelenik meg, amelyet értékesítenek különböző bűnözők. Az illegális piacokon való jelenléte azért kockázat, mert lehetőséget ad a bűnözők számára arra, hogy a személyes adatokat, banki információkat és egyéb érzékeny adatokat könnyedén értékesítsenek, vagy felhasználják. Ezért az ilyen típusú adatcsomagok rendkívül fontosak a kibertámadások, csalások és más illegális tevékenységek szempontjából.
[69] http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion
[70] http://msydqstlz2kzerdg.onion
[71] http://xmh57jrzrnw6insl.onion
[72] http://torlinksge6enmcyyuxjpjkoouw4oorgdgeo7ftnq3zodj7g2zxi3kyd.onion
[73] http://hss3uro2hsxfogfq.onion
[74] http://grams7ebnju7gwjl.onion
[75] http://gjobqjj7wyczbqie.onion
[76] http://3bbaaaccczcbdddz.onion

breach”, „personal data leak”, amelyek személyes adatok kiszivárgásával kapcsolatba hozható eredményeket produkáltak. Bár hasonlóan az első lépcsős lépéshez, a keresés nem adott konkrét eredményt, viszont rámutatott azokra az incidensekre, amelyek esetében személyes adatok is érintettek voltak. Azaz ily módon az alábbi információk nyerhetők ki:

- incidens ideje (további kutatáshoz tájékoztató jellegű adat);
- melyik hekkercsoport vállalata fel (további kutatáshoz mérvadó adat);
- mi szivárgott ki (további kutatáshoz relevancia indikátor);
- ki az érintett (további kutatáshoz mérvadó adat).

A fent megszerzett adatok alapján ki lehet azt szűrni, hogy a vizsgált időszakaszban, milyen nagyobb vállalkozásnál merült fel kiberbiztonsági incidens és/vagy melyik hekkercsoportnak sikerült hozzájutnia nagy mennyiségű személyes adathoz egy incidens során. Ebben az esetben két lehetőségünk lenne. Az első esetben az érintettet/sértettet lehet megkeresni, és tájékozódni arról, milyen személyes adatok kerültek eddig nyilvánosságra. Viszont az innen megszerzett adat nem tekinthető primer adatnak, mivel nincs rálátásunk arra, hogy gyakorlatilag mi került ki valójában, mennyire hiteles, mikor keletkezett, és érvényes-e még egyáltalán a megtalált adat. Így lehetőség szerint a vizsgálatot tovább kell folytatni a hekkercsoport által üzemeltetett elektronikus felületen, ami alapvetően már az anonimitás miatt nem a nyílt interneten megtalálható adat. Arról nem beszélve, hogy feltehetően a sértett nem fogja megadni a kért adatokat, illetve elismerni az adatszivárgás tényét, mivel ezzel saját hitelességét és reputációját is rombolná.

Kutatásom során megállapítottam, hogy a hekkercsoportok képernyőfotók segítségével bizonyítják azt, hogy rendelkeznek e megszerzett adatállományokkal. A vásárlók/érdeklődők a képernyőfotók alapján értékelhetik, hogy megvásárolják-e az említett adatállományokat. [68]

Kihangsúlyozom, hogy ezeknek a csoportoknak általában Telegramm és Twitter fiókja is megtalálható a nyílt interneten, ahol támadásaikat egyes esetekben ki is posztolják. A legjobban látogatott telegramm csatornák az említett témakörben a LAPSUS$, az RF/RB Bases, a Null Leak, a vxunderground, az Ares, a „W BH”, a STORMOUS RANSOMWARE, az IT Army, a Kelvin Security és a Breached Data.

A hekkercsoportok esetében elhanyagolható előfordulási számmal megtalálható olyan eset is, amikor a rivalizálás során egymásról is kiposztolnak személyes adatokat. Egyik esetben például a BreachForums és az OmniForums tagjai egymást vádolták meg személyes adatok kiszivárogtatása miatt. Az elemzések után megállapítottam, hogy az Omni Forums posztjai

szerint bejelentkezési kulcsok, felhasználónevek, e-mail címek, IP-címek, jelszókivonatok, regisztrációs dátumok, a tagok utolsó látogatásai és bejegyzései, bejegyzések száma és utolsó tevékenysége került ki.

Az Onni Forums hivatalos Twitter-fiókjából származó tweetek alapján vállalták a felelősséget a támadásért. Ugyanezen fórum egy másik tweetje azt állítja, hogy részt vettek egy másik hackerfórum elleni támadásban is, amely az „Exposed" néven ismert csoport volt. Nevezetesen, 2022 májusában az ExposedForumon kiszivárgott egy részleges adatbázis, amely a lefoglalt RaidForums 460 000 tagjának adatait tartalmazta. A fenti eseményből jól látszik, hogy a riválisa csoportok gyakorlatilag folyamatos konfliktusban állnak egymással, ahol elsődleges cél a másik hitelrontása. A fenti információk hitelességét fenntartásokkal kell kezelni, mivel a motiváció a másik csoport lejáratása. Így nem zárható ki, hogy nem valós adatokat tartalmaznak ezek az adatbázisok.

A folyamatot tekintve elmondható, hogy a TOR over VPN kapcsolaton keresztül használtam a DucDuc keresőt. Kulcs szóként a „hacker forums" illetve a „hack forums" és „hack tools" kifejezést kerestem, mint releváns fogalom. Legrelevánsabb eredményként a HackForums oldal esetében kaptam használható eredményt.

Az oldal elemzése után a fórum felületről már át lehet navigálni az online kereskedelmi térbe (Buyers Bay), ahol egy részben változó kínálatot kapunk. A mintavétel időpontjában lehetőségünk lett volna feltehetően Instagram/Twitter, és Netflix élő kliensek megvásárlására is. Innen célirányosan lehetőség van továbbnavigálásra, a vásárlók területére, ahol már részleteiben is megtudjuk milyen adatokat/szolgáltatásokat/fiókokat értékesítenek ezen a felületen. A fórum vizsgálata során 250 megvizsgált bejegyzés (1-10 oldal) közül nyolc ajánlat (3,2%) volt közvetlenül a személyes adatokhoz köthető. Továbbá a 28 (11,2 %) pedig olyan ajánlat/megkeresés volt, amely közvetve köthető a személyes adatokhoz.

Ezekben az esetekben valamilyen érzékeny adatot értékesítettek a fórumon:

- szoftver, alkalmazáshoz köthető felhasználó név/jelszó;
- Xbox kliens belépő adatai;
- Google Play ajándékkártya adatok;
- NBA League Pass adatok;
- Adobe termékek termékkulcsai;
- Amazon ajándékkártya paraméterek, ahol névhez köthető szolgáltatási adatok vannak.

A vételre felajánlott adatokat ellenőrizni a jogszabályi keretek miatt nem volt lehetőség. Viszont hipotézisünket alátámasztja az, hogy a személyes adatok kereskedelme jelentős nagyságú (14,4 %) volt ebben a viszonylag szűk mintavételezési időben is[77], főleg hogy elég volt ehhez egy fórumot áttekinteni. A melléklet utolsó blokkjában feltüntettem néhány olyan, ajánlatot, amely jól mutatja, hogy mintavételi csoportban fellelhető adatok nem legális úton kerültek az értékesítőkhöz.

A Dark Web magját jelentő titkosítási eljárást az Amerikai Egyesült Államok hadereje fejlesztette, annak érdekében, hogy az itt folytatott kommunikáció visszakövethetetlen legyen. Ezt követően az egész felületet nyílt forráskódúvá tették. Ennek következtében a harmadik lépcsőben Onion TOR böngészőn (Ahmia) fellelhető linkeken folytattam a keresést az alábbi eredményekkel.

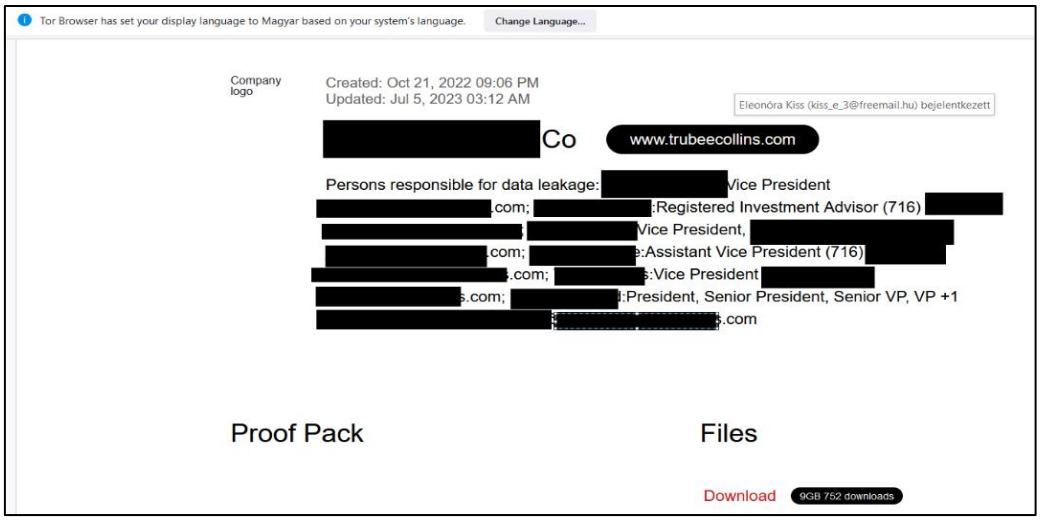
Ehhez ingyenesen és nyílt forrásból beszerezhető TOR keresőt[78] is lehet alkalmazni. A Hystak keresés során több a személyes adatokhoz köthető fogalmat használtam.[79] A kutatás során fellelt eredmények, ahol a Dark Weben a személyes adatok az alábbi kombinációkban jelennek meg jellemzően:

- 1. csoport bankkártya számok;
- 2. csoport CC's számok, lejárat dátuma, tulajdonos személyi igazolvány száma;
- 3. csoport Facebook ajándékkártya adatok;
- 4. csoport SIM kártya adatok (hamis ID számokkal);
- 5. csoport útlevél számok, vezetői engedélyek, Személyi Azonosító Igazolvány számok, Születési anyakönyvi kivonatok, Zöldkártya számok.

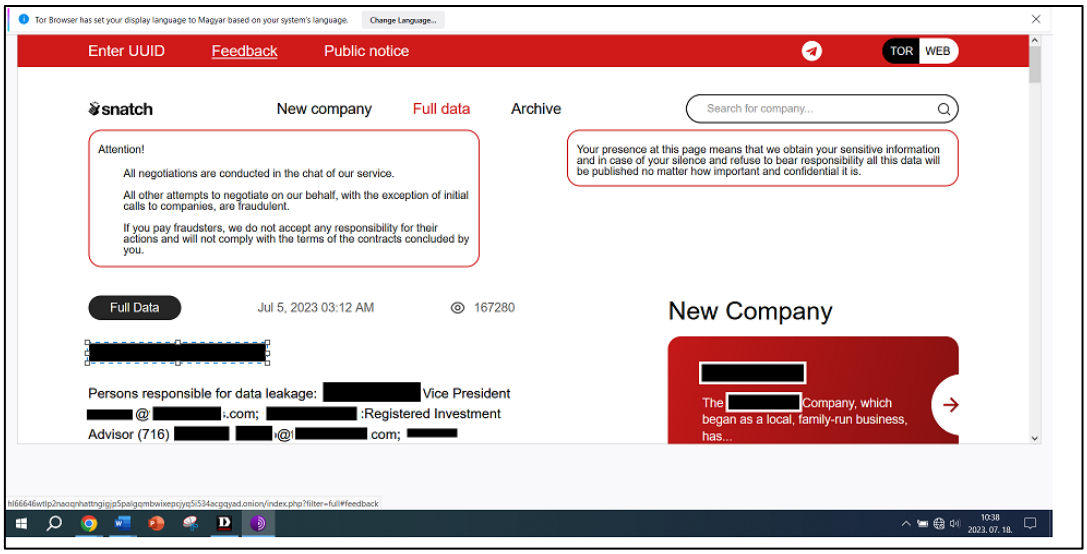
Kutatásom során a „Snatch” elnevezésű csoport oldalát figyeltem meg elemzés és értékelés céljából. A csoport oldalán már a nyitólapon megjelenik az az üzenet, ha ezt az oldalt meglátogattuk, akkor feltehetően saját vállalkozástól vagy érintett szervezettől adatok szivárogtak ki, és ezzel feltételezhetően rendelkezik a csoport.

Látható az esettanulmányban, hogy a felületen bemutatják, hogy ki volt a felelős a szivárgásért, valamint annak elérhetőségét, a vállalkozás nevét és a kiszivárgott adatok típusát. A weboldalon láthatóak az új vállalkozások, ahol adatszivárgás történt, valamint egy rövid vállalati bemutatót is kaphat az olvasó.

[77] Folyamatosan végzett 180 perces megfigyelés.
[78] http://haystak5njsmn2hqkewecpaxetahtwhsbsa64jom2k22z5afxhnpxfid.onion/?q=id+card+number
[79] „Personal data”, „stolen personal data”, „SIM card number”, „E-card number”, „ID number”.



14. ábra Snatch oldala forrás: saját kutatás



A kezdő oldalon beléphetünk az egyes vállalkozások kiszivárgott adatait tartalmazó oldalakra, ahol már részletesebb leírást kapunk a vállalatról (tevékenységi kör, létszámadatok stb.). A megszerzett információkat itt még nem láthatjuk, de lehetőségünk van bizonyíték „Proof Pack” beszerzésére is.

A vizsgálat során - egyes vállalkozások esetében, ahol feltehetően nem került sor a váltságdíj megfizetésére – a weboldal alján lehetőségünk van direkt módon hozzáférni az adatállományhoz is. Emellett tájékoztatást nyújtanak arról, hogy a letöltött állomány milyen méretű, és eddig hányan töltötték le.

A Snatch oldalát elemezve az alábbi táblázatba gyűjtöttem az összesített eredményeket. Az „érintett iparág” típusát tüntetem fel annak érdekében, hogy az egyes vállalkozásokat ne

nevesítsem. Emellett látható, hogy az adott csoportokat hányszor töltötték le (vagy vásárolták meg), valamint azt, mekkora adatmennyiség érintett a kiszivárgásban. A megtekintések száma nem egyezik értelemszerűen a letöltések számával, ebben az esetben a megtekintés csak azokra az információkra korlátozódik, ami bemutatja a megszerzett személyes adatok kivonatát.

Megtekintések száma	Feltöltés ideje	Letöltött adatmennyiség (GB)	Letöltések száma	Érintett iparág
317466 db	2021. december 26.	3 GB	89 db	Turizmus
167441 db	2022. augusztus 18.	297 GB	3100 db	Egészségügy
197266 db	2022. január 17.	17 GB	67 db	Turizmus
252631 db	2022. november 20.	119 GB	95 db	ITC
390690 db	2022. október 20.	38 GB		ITC/védelmi ipar
167441 db	2022. október 21.	9 GB	756 db	Pénzügy
180136 db	2022. október 21.	7,2 GB	1282 db	Szórakoztatóipar
1484 db	2023. július 05.	20000 GB		ITC
1450 db	2023. július 05.	500 GB		ITC
1483 db	2023. július 11.			Élelmiszer ipar/szolgáltatás
30878 db	2023. június 21.	25,9 GB	1253 db	Egészségügy
64821 db	2023. május.23.	28,8 GB	3120 db	Kormányzat
108821 db	2023. március 8.		11490 db	Kormányzat

Kutatási eredményem szerint a fenti táblázat alátámasztja azt a hipotézisemet, hogy a személyes adatok kiszivárgása kiemelt kockázatot jelent jelenleg. Fontos megjegyezni azt, hogy ez az adat egy 24 órás ciklusból keletkezett, egy hekkercsoport által illegálisan megszerzett adatait tartalmazza csak. Ennek tükrében megállapítható, hogy a kockázat kiemelten magasnak minősíthető, hiszen a fenti adatok többszöröse tárolódik a Dark Web háttértárakon.

Személyes adat akkor is kikerülhet, ha az elkövető a zsarolás következtében nem kapja meg a követelt összeget. Ebben az esetben szinte azonnal kipublikálják kereshető és rendszerezett módon a megszerzett adatokat.

2.7.6 Fórumok

A Dark Web-es keresések során másik módszer a már előzetesen említett fórumokon keresztüli klasszikus manuális keresés. Erre lehetőségünk van, hiszen számos ilyen fórum létezik mint például a Nulled. A Nulled egy online fórum, amely 2020-ban több mint három millió tagot számlált, és többnyire kiberbűnözők használják kiszivárgott információk kereskedelmére és vásárlására. Itt 2016-ban a hekkerek tevékenysége miatt közel 9,45 GB-nyi felhasználói személyes adat került nyilvánosságra. [69]

Egy másik hasonló a Dread fórum, amely a darkneten funkcióját tekintve megegyezik a Reddittel. Ismerős közösségi vitalapokat biztosít. A fórum sok ötletet átvesz a Reddittől, például az alközösségekről és a felhasználói moderálási kötelezettségekről. A Dread fő célja, hogy egy cenzúramentes fórumot kínáljon, de néhány szolgáltatást is kínál, például a penetrációs tesztet is. A Dread fórumot a felhasználók gyakran használják információcserére a különböző illegális tevékenységekről, tapasztalatok megosztására, és olyan témákról egyeztetnek, amelyek a legtöbb mainstream internetes platformon tiltottak. Ezenkívül itt több esetben megjelennek hírek és értesítések a Dark Web piacokkal kapcsolatban is, abban az esetben például, ha egy piacot megszüntetnek, vagy ha egy új piac indul. A fórum népszerűsége annak köszönhető, hogy a felhasználóknak anonimitást biztosít, és ezt moderátorok felügyelik, akik igyekeznek biztosítani a fórum biztonságát és megbízhatóságát. [70]

A Cracking King egy olyan közösségi fórum, amelyen jelenleg oktatóanyagokat és program-eszközöket kínálnak az illegális tevékenységek kivitelezéséhez. Információkat találhatunk az adatszivárgásokról, valamint hozzáférhetünk a piacterükhöz is. 2024-től a számítógépes bűnözéssel kapcsolatos különféle tiltott tevékenységek elősegítésével szerzett hírnevet magának a fórum. Elsősorban a hekkerek és a kiberbűnözők piactereként szolgál információcserére, valamint ellopott adatokat is terjesztenek. A fórum különösen népszerű a feltört szoftverek, a kiszivárgott hitelesítő adatok és a különböző rendszerek sérülékenységeinek kihasználására vonatkozó részletes útmutatók megosztása miatt is. Az elmúlt években az olyan fórumokon, mint a Cracking King, jelentősen megnőtt a rosszindulatú programokkal kapcsolatos bejegyzések száma, különösen az olyanokkal, mint a Redline, amelyek célja érzékeny információk, például bejelentkezési adatok és pénzügyi adatok

gyűjtése. Ezek a fórumok más típusú kiberbűnözési szolgáltatások népszerűsítésére is alkalmasak, például a kripto-drainerek[80] és a rosszindulatú programbetöltők, amelyek népszerűsége a kriptovaluták iránti növekvő érdeklődés és a kifinomultabb támadási módszerek iránti igény miatt nőtt meg feltételezhetően. [25];

A 2017-ben indult a CryptBB. privát hekkerfórumként indult, amely szigorú jelentkezési elvárásairól volt ismert, és csak azokat a tagokat fogadta, akik megfeleltek az interjún. Ez a fórum 2024-ben továbbra is aktív, és meghatározó szerepet játszik a kiberbűnözői közösségben. A fórum mostanra kiterjesztette célközönségét, és már nemcsak a tapasztalt hekkerekre fókuszál, hanem az újonnan belépő tagokra is, olyan személyekre, akik érdeklődnek az illegális informatikai tevékenységek iránt. Ez a lépés valószínűleg a fórum adminisztrátorainak szándéka volt, hogy szélesebb közönséget vonzzanak, és biztosítsák a fórum hosszú távú fennmaradását. [71]

Emellett változatlanul különböző szolgáltatások is elérhetőek, a fórumon lehetőség van például különböző rendszerekhez kapcsolódó Távoli Asztali Protokoll (RDP[81]) hozzáférés megszerzésére, hekkerek felbérlésére, valamint penetrációs tesztelési és hibabejelentési szolgáltatásokat is biztosít a tagoknak. A fórum adminisztrátorai különösen nagy hangsúlyt fektetnek arra, hogy megtartsák a közösséget, és magas színvonalú szakértői vitákat folytassanak. Ez a változás a fórum népszerűségét növelheti, különösen a versenytársak, például a Torum fórum[82] kihívásaival szemben. [72] A Torum egy angol nyelvű, nonprofit kiberbiztonsági fórum volt, amely 2017 májusában indult. A fórum célja a kiberbiztonsági témák megvitatása és a hackelési módszerek megismerése volt. Azonban 2020. augusztus 9-én az adminisztrátor bejelentette a fórum bezárását, mivel elvesztette az érdeklődését annak fenntartása iránt. A bezárás előtt a fórum több mint 130 000 felhasználóval rendelkezett, és aktív közösséget alkotott. A Torum bezárása után a felhasználók alternatívákat kerestek, például a CryptBB fórumot. [73]

A RaidForums egy olyan webhely, amely feltört adatbázisok és szoftvereszközök megosztására szolgál, illetve elmondható, hogy a hitelesítő adatokkal való feltöltési támadások végrehajtására

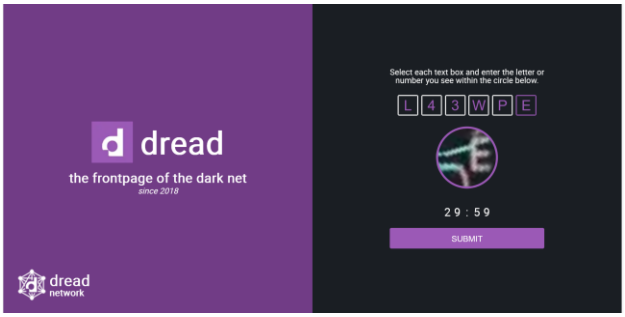
[80] A crypto drainer egy adathalász eszköz, amelyet a web3 ökoszisztémára rendszeréhez optimalizáltak. Ahelyett, hogy ellopnák az áldozatok felhasználónevét és jelszavát, a drainerek üzemeltetői gyakran web3-projekteknek álcázzák magukat, és arra csábítják az áldozatokat, hogy kriptopénztárcájukat csatlakoztassák és jóváhagyják azokat a tranzakciós kéréseket, amelyek a pénztárcában lévő pénzeszközök feletti ellenőrzést biztosítják a kezelőnek. Azaz önként átadják személyes pénzügyi adataikat.
[81] Remote Desktop Protocol
[82] https://onion.live/site/torum

(credential stuffing[83]) specializálódott. Webhelyük nyílt webes verziójával is rendelkeznek, ami viszont emiatt egyedivé tette őket, egészen az oldal felszámolásáig. [74] Az oldalt 2022-ben az Europol és az FBI közös akciója során lekapcsolták, és az üzemeltetőjét letartóztatták.

A FreeHacks az egyik legnépszerűbb és az egyik legnagyobb hekkerfórum az interneten. A hekkerek és kiberbűnözők orosz közössége üzemelteti a rendszert, ahol alapvetően az egyik cél a közös tudás megosztása.

Természetesen számos fórum talaláható meg a Dark Weben. Ezek a fórumok közösségi térkén funkcionálnak, a kutatás során ezekből a gócpontokból lehetett különböző irányokban kereséseket végezni. Alapvetően olyan fórumot kerestem, ami ismert és ahol fellelhetőek személyes adatok is, nem csak oktatási/szolgáltatási céllal jöttek létre.

A jelen kutatás során a Dred fórumot figyeltem meg az elemzés céljából. A belépéshez több hitelesítési folyamaton keresztül lehet bejutni. Alapvetően olyan programokat használnak, ami az illegális célból írt robotprogramokat szűri, és csak embereknek teszi lehetővé az űrlapok használatát a weboldalon. Ezek alapvetően kép vizsgálat alapú időzítővel ellátott programok voltak.



15. ábra Dred forum belépés

A keresés során kulcsszóként a „Personal Data” és az ID CARD” kifejezést alkalmaztam annak érdekében, hogy megfelelően releváns adatokat kapjak meg. A „Personal Data” kifejezés túl széles körűnek bizonyult, így használható eredményt itt nem kaptam.

Ellenben az „ID CARD” kulcsszóra már generált használható találatot a fórum. Alapvetően bankkártyákkal kapcsolatba hozható pénzügyi visszaélésekkel kapcsolatos cikkek, eljárások érhetőek el. Személyes adatokkal közvetlenül kapcsolatba hozható adatbázist nem találtam.

[83] Automatizált kibertámadási módszer, amely során a támadók ellopott vagy kiszivárgott felhasználónév-jelszó párosokat próbálnak ki más online szolgáltatásokon, abban a reményben, hogy a felhasználók ugyanazokat a hitelesítő adatokat több helyen is használják.

A Dread esetében lehetőség van belépni az aldomainekbe, amelyek már konkrétumokat tartalmaznak. Konkrét eljárásrendeket, valamint összeköti a keresletet a kínálattal. A kutatás miatt eddig a pontig kutatható a terület. Következtetésem szerint a személyes adatok alapvetően több ponton megtalálhatóak, mint célinformációk.

2.7.7 Közösségi média

A kutatás során 396 db közösségi média klienst vizsgáltam az alapján, hogy milyen személyes adatok találhatóak meg az illető hírfolyamában[84], vagy posztjaiban. A felsorolásba azok a kliensek kerülnek be, ahol értékelhető eredmény látható.

A vizsgálat nem terjed ki arra, hogy a felhasználó azt tévesen vagy szándékosan osztotta meg, valamint a megosztott névjegyén milyen személyes adatok szerepelnek. A keresés a szövegesen feltöltött (vagy képen egyértelműen olvasható) személyes adatokra korlátozódott, következtetéseket az adatok nem tartalmaznak.

A kutatás során egyértelműen azonosítható adattípusok:

- NKE bizonyítvány közigazgatási szakvizsgáról (név, anyja neve, vizsgarész minősítés, vizsgabizottság tagjainak adatai, vizsga időpont) -feltöltött fénykép;
- Cambridge nyelvvizsga eredmény (névvel, feltöltött oklevél képpel, oklevél számmal és azonosítóval) -feltöltött fénykép;
- Országos Egészségbiztosítási Pénztár Egyedi Méltányossági Ügyek Főosztálya nyomtatvány;
- Házassági bontóper teljes iratanyaga (név, tanúk, különleges személyes adatok);
- Talált magyar személyigazolvány (két oldalra lefotózva anonimizálás nélkül – 5db);
- Szabadalmi per iratanyaga a felperes és alperes adataival;
- Született gyermek születési és egészségügyi adatai (név, születési súly, anyja neve, okmány száma);
- sport tevékenységgel kapcsolatos saját biometrikus adatok;
- tartózkodási hely (bejelentkezés rendezvényről, turisztikai/vendéglátóipari objektumból);
- online térben vásárolt termékek számlái, vásárlási adatai (vásárló adataival);
- saját sportteljesítmény (név, biometriai adatok, tartózkodási hely, bejárt útvonal, hobbi);

[84] 2023. szeptember – 2023. december

- végelbocsátó katonai levél[85] (név, katonai alakulat neve);
- pályázati oklevél (név, cím, elért eredmény);
- karitatív tevékenységet igazoló díj oklevele (név, tevékenység megnevezése);
- EMMI szociális munkáért díj és oklevél (név, kitüntetett, adományozó, aláírásminta, adományozás dátuma, adományozás oka);
- katonai szakközépiskoláról osztályfotó (nevek, végzés dátuma, intézmény azonosítók);
- megszüntetett katonai alakulat tagjainak névsora, leszerelés dátuma.

A fenti eredményekből látható, hogy a felhasználók több esetben megosztják harmadik fél személyes adatait is. Természetesen úgy, hogy az illető ehhez nem adta hozzájárulását, de alapvetően nem is tud róla[86]. A fenti listában látható, hogy két esetben ez feltételezhetően szándékosan hajtotta végre a felhasználó annak érdekében, hogy az ellenérdekeltségű fél reputációját rombolja. A szabadalmi per esetében a peranyag számos személyes adatot tartalmazott, valamint egyértelműen beazonosítható volt a sértett és a feltételezett szabálysértést elkövető személye. A bontóper esetében olyan személyes adatok is felkerültek, amelyeket a sértett a vélt vagy valós sérelmeit elkövető személy lejáratása érdekében mutatott be. A fenti adatok kiemelten jól használhatóak adatdúsításhoz, ami további kibertámadást segíthet elő a hekkereknek.

2.7.8 Hipotézis igazolása

Az illegális és hanyag adatkezelés napjaink egyik legsúlyosabb problémája, amely folyamatosan növekvő kockázatot jelent mind az egyének, mind a szervezetek számára. Az adatlopások, adatszivárgások, illetve a személyes adatokkal való visszaélés nem csupán a Dark Web piacain folyik, hanem a Surface Weben is, ahol a kiszivárgott adatok egy része nyíltan hozzáférhetővé válik. Ez a tendencia hosszú távon komoly veszélyeket rejt magában, hiszen az adatok szivárgása exponenciálisan növekszik, és ezzel együtt a kibertérben megjelenő fenyegetések is nőnek.

A személyes adatok kiszivárgása elsősorban két fő tényezőből fakad: az adatlopásokból és a hanyag adatkezelésből. Az előbbi esetében szervezett bűnözői csoportok hekkertámadásokat hajtanak végre vállalatok, kormányzati szervezetek vagy egyéni felhasználók ellen, hogy hozzáférjenek a bizalmas adatokhoz. Az ilyen támadások gyakran kifinomult módszerekkel, például adathalász e-mailekkel, kártékony szoftverekkel vagy zsarolóvírusokkal zajlanak. A

[85] Olyan katona, aki szolgálati idejét letöltötte, és obsitot kapott.
[86] A megosztott képeken nem „taggalik” be a rajta szereplőket.

megszerzett információkat – például neveket, címeket, bankkártya adatokat és társadalombiztosítási számokat – gyakran a Dark Web piacain értékesítik, ahol ezeket további illegális tevékenységekhez használják fel. Az adatlopások mértéke folyamatosan növekszik, amit a jelentős adatszivárgási incidensek száma és azok volumene is alátámaszt.

A hanyag adatkezelés szintén kulcsfontosságú tényező. Sok szervezet nem fordít megfelelő figyelmet az adatok védelmére, gyakran elavult biztonsági rendszereket használnak, vagy nem tartják be a vonatkozó adatvédelmi előírásokat, például az Európai Unió által előírt GDPR-t. Ennek következtében a személyes adatok könnyen hozzáférhetővé válhatnak a nyilvánosság számára, akár véletlenül, akár a szándékos visszaélések révén. Az adatszivárgások egy része emberi mulasztás miatt történik, például rosszul konfigurált szerverek, nyitott adatbázisok vagy a munkavállalók figyelmetlensége miatt.

Az illegális adatlopások és a hanyagságból eredő adatszivárgások egyre nagyobb méreteket öltenek, és a kockázatok súlyosbodnak. Az ilyen esetek nemcsak pénzügyi károkat okoznak az érintetteknek, hanem jelentős érzelmi és társadalmi hatással is járnak. Az adatokkal való visszaélés növeli az identitáslopás, a pénzügyi csalás és más kibertámadások valószínűségét, amelyek hatása messze túlmutat az egyéneken. A szervezetek számára pedig az adatszivárgások reputációs károkat, bírságokat és üzleti veszteségeket eredményezhetnek.

A jövőre tekintve az adatszivárgások növekvő tendenciája várható. Az adatállományok mérete exponenciálisan növekszik, ahogy a digitális világban egyre több személyes információt gyűjtenek és tárolnak. Emellett a kibertámadások technológiája is fejlődik, és a támadók egyre kifinomultabb módszereket alkalmaznak. A mesterséges intelligencia és az automatizáció megjelenése lehetővé teszi, hogy a támadások gyorsabban és szélesebb körben valósuljanak meg, miközben a védelmi rendszerek nem tudnak lépést tartani a fenyegetésekkel. A Dark Web piacai pedig továbbra is jelentős keresletet generálnak a kiszivárgott adatok iránt, ami anyagi ösztönzést biztosít az adatlopások elkövetői számára.

A fenti adatok, esettanulmányok, valamint a Dark Web-en megtalálható adatok mennyiségi mutatója alapján világosan látható, hogy az illegális és hanyag adatkezelés révén kiszivárgó személyes adatok komoly és folyamatosan növekvő biztonsági kockázatot jelentenek. Ennek kezelése érdekében elengedhetetlen az adatvédelem szigorítása, a technológiai fejlesztések bevezetése, valamint az emberek és szervezetek tudatosságának növelése. Csak átfogó és összehangolt erőfeszítésekkel lehet lassítani, esetleg megállítani ezt a kedvezőtlen tendenciát.

Kutatásom részletes eredményeit a „Forms and risks of personal data appearing on the darkweb and surface web illegally, negligently or intentionally I.” című, illetve a „Forms and risks of personal data appearing on the darkweb and surface web illegally, negligently or intentionally című publikációmban mutattam be.

3. Személyes adatok kezelésének kockázatértékelése az egyes technológiák esetében

3.1 Áttekintés

A mai IT technológiák esetében elmondható, hogy hatalmas mennyiségű személyes adatot kezelnek az egyes felhasználók, amelyek szinte minden aspektusukat érinthetik, beleértve a hely-adatokat (geoinformációs), egészségügyi információkat, online tevékenységeiket, valamint a vásárlási szokásokat. Az okostelefonok, a viselhető eszközök, az IoT rendszerek és a közösségi média platformok mind napi szinten gyűjtenek adatokat, amelyek egyre részletesebb képet adnak a felhasználókról. A gépi tanulás és mesterséges intelligencia alkalmazása lehetővé teszi, hogy az adatok alapján előrejelzéseket és személyre szabott ajánlatokat készítsenek, ami új adatvédelmi kihívásokat hoz. Mivel a személyes adatok védelme alapvető jogi és etikai kérdés, minden olyan új technológia, amely a felhasználók adatainak gyűjtésére és feldolgozására épít, potenciális adatvédelmi kockázatokat hordoz. A GDPR és más adatvédelmi szabályozások előírják, hogy az új technológiák esetén el kell végezni egy kockázatértékelést és adatvédelmi hatásvizsgálatot (DPIA**)**, hogy megelőzzük a személyes adatok jogellenes felhasználását, illetve érintettek jogaira és szabadságaira jelentett kockázat csökkentése.

Az adatvédelmi hatásvizsgálat különösen szükséges, ha a technológia új módszereket alkalmaz az adatok kezelésére, ha nagy mennyiségű érzékeny adatot dolgoz fel, vagy ha az adatokkal kapcsolatos döntések automatizáltan történnek. Például, ha egy vállalat MI-alapú rendszert vezet be a felhasználói viselkedés elemzésére, vagy ha új IoT eszközt telepít, amely folyamatosan gyűjt adatokat, akkor a kockázatértékelés elengedhetetlen. Az új technológiák gyors fejlődése és az adatkezelési módszerek változékonysága miatt a folyamatos adatvédelmi monitorozás és a szabályozásoknak való megfelelés kiemelten fontos. Ezen intézkedések révén biztosítható, hogy az innovációk ne sértsék a felhasználók jogait, és hogy az adatkezelés megfeleljen a törvényi előírásoknak.

3.2 Hipotézis

Hipotézisem szerint a személyes adatok védelme minden új/már alkalmazott műszaki technológia esetében külön kockázatértékelést követel meg, valamint GDPR megfelelősségi vizsgálat is minden esetben szükséges, mivel nem készíthető el egy egységes adatvédelmi és kiberbiztonsági keretrendszer ebben a tekintetben.

Jelenleg nincsen olyan közös adatvédelmi minta, ami minden technológia esetében alkalmazható a GDPR tekintetében. Emellett a személyes adatok védelme minden új/már alkalmazott technológia esetében külön kockázatértékelést követel meg, valamint GDPR megfelelősségi vizsgálat is minden esetben szükséges, mivel nem készíthető el egy egységes keretrendszer.

3.3 Kutatás módszertana

Hipotézisem igazolásához a klasszikus értelemben vett dokumentum és szekunder adatzelemzést választottam. Ennek oka, hogy a dokumentumelemzés lehetőséget ad arra, hogy mélyebb megértést nyerjek az adott témáról vagy részterületről, különösen, ha a múltbeli eseményekre vagy a társadalmi és műszaki folyamatok hosszú távú vizsgálatára összpontosítunk. Jellemzően olyan részterületeket választottam a kockázatértékelés tekintetében, ahol mélyebben be lehet mutatni az adatvédelem tekintetében felmerült kockázatokat a személyes adatok tükrében.

3.4 Blokklánc technológia

A digitalizáció és az információs társadalom gyors előretörése következtében egyre több új technológia jelent meg napjainkra, ezen új technológiai megoldások esetében is felmerült a személyes adatok kezelésének kérdése, így a GDPR követelményeit értelmezni kell, valamint az új kockázatokat ismertetni célszerű a felhasználókkal. Az e-kereskedelemben és az e-gazdaságban egyre több az olyan platform, információmegosztó alkalmazás, amely személyes adatokat használ, vagy valamilyen módon kezel, például a blokkláncok is ilyenek. [75]

Az Európai Parlament (EP) már vizsgálta a blokklánctechnológia és a GDPR egymáshoz való viszonyát és összefüggéseit. [76] Ezzel kapcsolatban több kérdés is felmerült, ugyanis a GDPR követelményei és a blokklánc-technológia között vannak jelenleg feloldhatatlan kérdések.

Mint például a blokklánc alapjait képező állandó, változatlan adatblokkok, amelyek ellentmondhatnak a GDPR által előírt adattörlés vagy módosítás lehetőségének (azaz a felhasználó nem élhet például az adattörlés jogával). Emellett a blokkláncban tárolt személyes

adatok kezelésekor a GDPR által előírt adatvédelmi elveknek is meg kell felelni, például a felhasználók hozzájárulásának nyilvántartásával.

A blokklánc-technológia tekintetében bizonyos általános megállapításokat lehet tenni és következtetéseket lehet levonni, de minden esetben el kell végezni egy részletesebb elemzést, amely a konkrét technológiai megoldás jellemzői alapján vizsgálja az adatvédelmi megfelelés kérdését. Számos kutató foglalkozik azzal, hogy a blokklánc-technológiát integrálja az IoT-eszközök működésébe. Elsődleges céljuk, hogy létrehozzanak egy olyan decentralizált, blokkláncalapú adattovábbító keretrendszert, amely még a GDPR szabályainak is megfelel.[87]

„A szolgáltatók által kínált megkérdőjelezhetetlen előnyök ellenére a központosított IoT rendszerek bizonyos kihívásokkal nézhetnek szembe. Például egy titkosítatlan szerveren az adatok feltörhetők, és érzékeny információk kiszivárgását okozhatják. Ezenkívül egyes IoT-eszköz az adatkezelés során egy időben több adatkezelő is felmerül."[88]

A blokklánc megfelelősségi elemzése során a személyes adatok közül az egészségügyi adatok kiemelt hangsúlyt kaptak a vizsgálatok során. A blokkláncban tárolt egészségügyi adatokkal több tudományos cikk is foglalkozott már. Ezzel kapcsolatban számos koncepció látott napvilágot. Ilyen például a MedSBA-séma, amely titkosítás segítségével megvédi a betegek adatait. A MedSBA-sémában az attribútumalapú titkosítás, a blokklánc elosztott architektúrája, valamint a felhőtárrendszer biztosítja a felhasználók részére adataik felett a teljes kontrollt, illetve az adatbiztonságot is.[89]

A magyar jogszabályok tekintetében már kiadásra került hatósági állásfoglalás is ebben a témában. A Nemzeti Adatvédelmi és Információszabadság Hatósághoz (NAIH) intézett konzultációs beadványában a Bitcoin virtuális fizetőeszköz és az alapját képező blokklánc-technológia használatával kapcsolatban felmerülő adatvédelmi kérdésekre vonatkozóan.[90]

Minden egyes felhasználó, aki blokkokat és abban tárolt adatokat ad hozzá a rendszerhez, adatkezelőnek minősül. Később a rendszerhez adatokat hozzáadó felhasználó kizárólagos

[87] Masoud Barati & Omer Rana: Enhancing User Privacy in IoT: Integration of GDPR and Blockchain, Confernace Paper, 322-335 pp, Blockchain and Trustworthy Systems (BlockSys 2019)
[88] Muneeb UI Hassan, Mubashir Husain Rehmani, Jinjun Chen: Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions, Future Generation Computer Systems 97, 2019, 512-529
[89] POURNAGHI, Seyed Morteza – BAYAT, Majid – FARJAMI, Yaghoub: MedSBA: a novel and secure schem to share medical data based on blockchain technology and attribute-based encryption. Journal of Ambient Intelligence and Humanized Computing, (2020). https://link.springer.com/article/10.1007/s12652-020-01710-y; letöltés: 2020.02.03
[90] A Nemzeti Adatvédelmi és Információszabadság Hatóság állásfoglalása a blokklánc („blockchain") technológia adatvédelmi összefüggéseivel kapcsolatban. https://www.naih.hu/files/Adatved_allasfoglalas_naih-2017-3495-2-V.pdf; letöltés: 2020.02.03.

rendelkezési jogosultságot kap a blokkokban tárolt adatai felett, így ő határozhatja meg, hogy az adatokat melyik tranzakciókhoz fogja felhasználni. Amennyiben a tranzakciók révén a blokkban tárolt személyes adatok feletti rendelkezési jogosultság átadásra kerül egy másik felhasználónak, onnantól kezdve ez a felhasználó szerez az adatok felett kizárólagos rendelkezést, így ő fog adatkezelőnek minősülni. Ebből véleményem szerint az következik, hogy aki a blokklánc-technológiát alkalmazza – személyes és üzleti adatokkal kapcsolatban – minden esetben adatkezelőnek minősül. Valamint az előző alapvetésben az megkérdőjelezhető, hogy a blokklánc természeténél fogva nem kerülhet senki birtokába vagy fennhatósága alá.

A kriptopénz bányászatával kapcsolatban a francia Nemzeti Adatvédelmi és Szabadságjogi Bizottságnak (CNIL[91]) alapvetően hasonló az álláspontja, de az infrastruktúrát kiszolgáló személyek véleményük szerint nem tartoznak az adatkezelők közé. A CNIL iránymutatása értelmében minden olyan személy/felhasználó, aki vagy amely jogosult a blokklánc kiegészítésére, illetve a kriptovaluta-bányászok által küldött adatok hitelesítésére, adatkezelőnek minősül. Ezzel az állítással lehet vitatkozni, mivel az infrastruktúra kezelők is gyakorlatilag adatkezelők, hiszen tudják módosítani és törölni is az adatokat. Természetesen ebben az esetben nem veszem figyelembe azt, hogy ennek bármilyen jogalapja lenne, hanem maga a műszaki kivitelezés tekintetében van erre lehetőségük.

Az elfeledtetéshez (törléshez) való jog gyakorlása viszont a blokklánc sajátosságaira tekintettel teljességgel lehetetlen, mivel a blokklánc alapvetése, hogy minden előző blokk tartalmazza a teljes főkönyvet. A CNIL ezért e jog érvényesülése, illetve a blokklánc-technológia GDPR-nak való megfelelése érdekében azt javasolja, hogy az adatkezelők ebben az esetben alkalmazzanak úgynevezett „hash" technológiát, azaz a személyes adatokat alakítsák át egy olyan alfanumerikus kóddá, amely nem teszi lehetővé azok visszaállítását, visszafejtését. Véleményem szerint az átalakítás változatlanul nem jelent törlést. Arról nem beszélve, hogy maga az alapelv az, hogy az időben régebben keletkezett adatok elvileg a technológia szerint sérthetetlenek.

A GDPR a manuálisan végzett adatkezelések tekintetében tartalmaz megszorító rendelkezést. A kézi, azaz nem automatizált adatkezelések esetében a rendelet hatálya csak azokra az adatokra terjed ki, amelyek valamely nyilvántartási rendszer részei[92], vagy amelyek kezelése

[91] Commission Nationale de l'Informatique et des Libertés - Franciaország független adatvédelmi hatósága, amely a személyes adatok védelmét és a magánélet tiszteletben tartását felügyeli, összhangban a GDPR szabályaival.
[92] Az Infotv. ezt kiterjeszti [2.§ (4) bek.], ezért nemzeti szinten mindenre vonatkozik a GDPR, kivéve azt, ami háztartási adatkezelés.

nyilvántartási céllal történik. Azt, hogy mi minősül nyilvántartási rendszernek, a GDPR 4. cikk 6. pontja[93] határozza meg. A nyilvántartás fogalma tehát elég tágan értelmezhető. [77]

A GDPR akkor értelmezhető a blokklánc-technológiát alkalmazó rendszerek esetében, ha egyértelműen azonosíthatóak a rendszerelemeken belül a személyes adatokat tartalmazó adatbázisok vagy nyilvántartások. A GDPR hatályával kapcsolatos vizsgálatot minden esetben el kell végezni a rendszeren, kiemelten az adatkezelő tekintetében, mivel különbséget kell tenni az adatkezelő és az informatikai infrastruktúrát fenntartó személyek között (akik nem minősülnek adatkezelőknek egyesek szerint). A jelenlegi blokklánc-technológia nem teljes mértékben biztosítja a GDPR egyik fontosabb kritériumát, miszerint nem lehet visszamenőlegesen adatot törölni a rendszerben. A rendelkezésre álló információk alapján az adatok védelmének fő eszköze ebben az esetben a decentralizáció és ennek köszönhetően a felhasználók általi erősebb kontroll lehet az adatok fölött.

Megállapítom, hogy az internet tudatos felhasználói körében egyre jobban terjed az igény a saját személyes adatok feletti kontroll megszerzésére. A blokklánc-technológia a szolgáltatók szemszögéből erre egyes estekben megoldást nyújt. Az attribútumalapú titkosítás (ABE[94]), a felhőben tárolt nyers adatok és a blokkláncalapú szolgáltatások lehetőséget biztosítanak arra, hogy a felhasználók saját maguk kezeljék adataikat, de mégis igénybe tudják venni napjaink korszerű okosszolgáltatásaikat, azaz lehetővé teszi a rendszer azt, hogy adatok titkosítását úgy végezzük, hogy csak azok a felhasználók férhessenek hozzá, akik megfelelnek bizonyos attribútumoknak vagy előre meghatározott hozzáférési szabályoknak. Az adatok titkosítása nem egy konkrét kulccsal, hanem egy attribútumhalmazzal történik. A felhasználók egy privát kulcsot kapnak, amely szintén attribútumokhoz van kötve. Az adatok csak akkor fejthetők vissza, ha a felhasználó attribútumai megfelelnek a titkosításkor megadott feltételeknek. [78]

Megállapítható tehát, hogy a rendelet 2. cikk (1) bekezdése alapján a személyes adatokkal végzett bármilyen művelet annak tárgyi hatálya alá esik. A blokklánc-technológiát használó automatizált adatkezelések akkor eshetnek a GDPR tárgyi hatálya alá, ha ahhoz közvetlenül vagy akár közvetetten[95] kapcsolódva személyes adatok kezelése is megtörténik.

[93] nyilvántartási rendszer”: a személyes adatok bármely módon - centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint - tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

[94] Attribute-Based Encryption - KP-ABE (Key-Policy Attribute-Based Encryption és a CP-ABE (Ciphertext-Policy Attribute-Based Encryption

[95] pszeudonim módon

Az is látható, hogy nyilvánosan működő blokklánc esetén az adatkezelő azonosítása nem lehetséges, mivel bárki, aki a rendszerhez csatlakozott, saját elgondolásának megfelelően blokkokat adhat hozzá a hálózathoz, ami akár lehet személyes adat is. A nyilvános blokklánc üzemeltetése ezért adatvédelmi szempontból kockázatosabb adatkezelést eredményez. A gyakorlatban a nyilvános blokkláncokat jellemzően olyan rendszereknél használják, ahol személyes adatok kezelésére nem folyik, vagy csak pszeudonim[96] formában kerül sor.

A kutatásunk kiterjedt a blokklánc rendszerekre is. A blokklánc rendszerek viszonylatában egy forradalmian új koncepció is felmerült Simon Farshid, Andreas Reitz és Peter Roßbach kutatásában, ami szerint az új blokklánc-koncepcióban a blokkokon belüli régi adatok törölhetőek. Ennek következtében a blokklánc segítségével lehetőség nyílna olyan okosszerződést készíteni, amely műszakilag is szavatolja a törlést például a felhőszolgáltatás igénybevétele során magából a felhőből. [79]

Azaz a felhasználó, aki a szerződő fél, egy beküldött kódsor vagy parancssor segítségével a blokkokból kitörli régi adatait. A cikk alapján egy ilyen blokklánc prototípus-algoritmus segítségével feloldanák a felhőszolgáltatás és a GDPR-megfelelőség egyik fontosabb kérdését is. Véleményünk szerint az elgondolás új megvilágításba helyezi a blokklánc felhasználhatóságát, viszont szembemegy a blokklánc egyik alapelvével, mégpedig azzal, hogy a rendszerben visszamenőleg (függetlenül az adatfajtától) nem lehet törölni.

3.4.1 Kockázatértékelés

A blokklánc technológia és az okos szerződések használata számos előnnyel jár, de egyben biztonsági kockázatokat is generál, különösen a személyes adatok védelme szempontjából. A blokklánc alapvető tulajdonsága, hogy a hozzáadott adatokat nem lehet visszavonni vagy módosítani, mivel ez a rendszer egyik alaptörvénye. Ez adatvédelmi problémát jelenthet, ha személyes adatok kerülnek a blokkláncba, mivel ezek az adatok gyakorlatilag ott maradnak. A GDPR szerint az egyéneknek joguk van adataik törléséhez, mint ahogy ezt a kutatás során több szempontból is vizsgáltam, amit a blokklánc technológiával jelenleg nem lehet megvalósítani.

A blokkláncok gyakran pszeudoanonimként működnek, a felhasználók nem közvetlenül a nevükkel, hanem egy címmel jelennek meg, ez nem feltétlenül jelenti a teljes anonimitást. A tranzakciók nyomon követhetők, és ha egy cím valahogy összekapcsolható egy valós

[96] A személyes adatok védelme szempontjából a „pszeudonim” kifejezés olyan információt jelöl, amely lehetővé teszi egy személy azonosítását, de nem a valós nevén keresztül. A pszeudonim lehet például egy álnév, kód, felhasználónév vagy más olyan azonosító, amelyet a személy helyettesítőként használ, hogy a személyazonosságát elrejtse vagy megóvja.

személlyel, akkor az illető összes tranzakciója visszakövethetővé válik, ami jelentős adatvédelmi aggályokat vet fel. Emellett ez az egyik funkciója, amiért ezt a rendszert szívesen alkalmazzák. A blokklánc rendszerek gyakran anonimitást vagy pszeudanonimitást biztosítanak a felhasználóknak, viszont ez nem biztosan elegendő a személyes adatok védelmére. A lánc adataival végzett összetett elemzések, például az adattisztítás vagy strukturálás, vagy összevetés, lehetővé tehetik a felhasználók beazonosítását, főleg úgy, hogy eredetileg ezek névtelenek voltak.

Az okos szerződések automatikusan végrehajtódó kódok, amelyek a blokkláncban futnak. Ha egy okos szerződésben hibák vagy sebezhetőségek vannak, azokat kihasználva támadók hozzáférhetnek érzékeny adatokhoz, vagy jogosulatlan tranzakciókat hajthatnak végre. Ezen kívül, ha egy okos szerződés személyes adatokat tartalmaz, annak módosítása vagy törlése gyakorlatilag nem valósulhat meg. A blokklánc technológia decentralizált és átlátható természetéből adódóan nehézségekbe ütközik a személyes adatok védelmére irányuló intézkedések végrehajtása. Az adatkezelőknek gondosan kell mérlegelniük, hogy milyen adatokat rögzítenek a blokkláncon, és milyen védelmi mechanizmusokat alkalmaznak annak érdekében, hogy megfeleljenek az adatvédelmi előírásoknak. A blokklánc technológia és az okos szerződések nemzetközi természete miatt az adatvédelmi jogszabályok betartása nem megoldható. Ha egy blokklánc résztvevői több különböző országban helyezkednek el, akkor az egyes országok eltérő adatvédelmi szabályozásai felülírják egymást. [80]

A blokklánc alapú rendszerekben a hozzáférést kriptográfiai kulcsok biztosítják. Ha egy felhasználó elveszíti a privát kulcsát, akkor elveszíti a hozzáférést az adataihoz és az eszközeihez is. Ha a kulcsokat nem megfelelően kezelik, az adatok biztonsága sérülhet. A blokklánc technológia és az okos szerződések nagy lehetőségeket rejtenek magukban, de a személyes adatok kezelése szempontjából különös figyelmet igényelnek a biztonsági és adatvédelmi kérdések. A technológia fejlődésével és a szabályozások változásával ezek a kockázatok kezelhetőbbé válhatnak, de jelenleg a felhasználóknak és fejlesztőknek tudatosan kell kezelniük ezeket a kihívásokat.

További kockázatként felmerült, hogy a blokklánc rendszer egyes esetekben harmadik felek által működtetett decentralizált alkalmazásokra, vagy más néven dApp-ok segítségével működnek. Ennek következtében ezek az alkalmazások további adatkezelési kockázatokat okoznak az adattárolás és feldolgozás miatt. Főleg, hogy a harmadik felek nem feltétlenül követik egyenszilárdsággal a szabályozásokat. A dAppok száma (9. ábra) a lenti ábra szerint sem elhanyagolható.

DApp market overview for 2019

DApp platform	ethereum	EOS	STEEM	TRON	IOStoken	NEO
Active users	1.43M	0.52M	0.12M	0.97M	0.03M	0.06M
Total users	2.33M	0.57M	0.58M	1.02M	0.03M	0.1M
Active DApps	1,129	479	80	482	32	15
Total DApps	1,822	493	92	520	38	24
New DApps	690	260	34	411	38	12
Transaction volume (USD	$2.37B	$4.98B	$29.02B	$3.41B	$114.34B	$1.01B
Number of transactions	24.52B	2.81B	85.72M	290.28M	47.10M	2.27M

16. ábra dApp-ok száma

Forrás: ValueCoders

3.4.2 Megoldások

A fent említett kockázatok csökkentésére megoldást jelenthet a személyes adatok titkosított formában való letárolása, illetve olyan műszaki megoldások alkalmazása, mint a „zero-knowledge proof", amelyek lehetővé teszik az adatok védelmét a személyazonosság nyilvánosságra hozatala nélkül.

Emellett megoldás lehet az off-chain adatkezelés is, ahol a személyes adatok blokkláncon kívüli tárolása folyik, és csak a szükséges referencia adatok kerülnek bele a láncba.

Mind a láncon belüli, mind a láncon kívüli tranzakcióknak megvannak a maga előnyei és természetesen hátrányai is. A láncon belüli tranzakciók biztonságot és átláthatóságot, míg a láncon kívüli tranzakciók sebességet és alacsonyabb költségeket biztosítanak a felhasználók részére. [81]

Ideiglenes megoldás lehet az, hogy az adatvédelmi szabályozás alkalmazkodik a blokklánc műszaki sajátosságához, ezzel kezelhető lehet a decentralizált felelősségi körök kezelése is.

3.5 Elektronikus felületek

A GDPR az EU adatvédelmi rendelete, amiből tehát egyértelműen következik, hogy minden vállalkozásnak, így az e-kereskedelmi vállalkozásoknak is biztosan rendelkezésre kell állnia már most is érvényes adatvédelmi, adatkezelési belső szabályozása az EU-ban.

A honlapok használata mára a mindennapi életünk szerves részévé vált, főleg hogy jelentősen hozzájárulnak egy vállalkozás vagy szervezet sikeréhez, a felhasználók számára pedig megkönnyítik az ügyintézést, az információszerzést, a vásárlást.

A Magyar Honvédség állományában szerződéses és/vagy hivatásos szolgálatot teljesítő személyeket is érint az internetes blogszolgáltatás, webshop vagy esetleg egy mikrovállalkozás üzemeltetésével kapcsolatos megfelelősségi kérdések, ahol adatkezelés folyik, vagy önmaguk is adatkezelőkké válnak. Ez azért fontos, mert a honlapok tekintetében az adatkezelési szabályozás kialakításánál az egyik legfontosabb alapkérdés az, hogy az adatkezelési jogviszony alanyainak, valamint egyéb szereplőinek a megfelelő beazonosítása megtörténhessen, ez meghatározza az adatkezelés felelősségi körét és az adatkezeléssel kapcsolatos egyes feladatokat.

Ez abból következik, hogy a weboldalakon szinte kivétel nélkül megvalósul a GDPR 4. cikk 2. pontja szerinti adatkezelés[97].

Az üzemeltetett weblapoknak rendelkezni kell a kötelező vagy elvárható tartalmi elemekkel (3. sz. melléklet). A rendelet előírja, hogy a (személyes) adatokkal kapcsolatba kerülő üzemeltetők pontosan meghatározzák az adatok beérkezésének és feldolgozásának módját, a céljait, tárolásuk lehetőségeit és annak időbeliségét. Továbbá előírja az üzemeltetők részére, hogy ha az elektronikus felületüket igénybe vesszük, akkor ezzel kapcsolatban dokumentált módon visszakövethető legyen az adatkezelés, illetve hogy milyen tevékenységet folytatnak, történik-e személyes adat rögzítése, ami alapján egyértelműen beazonosíthatók leszünk, mint felhasználók.

Itt tisztázni kell azt, hogy az adatkezelési jogviszony egyik entitása a GDPR 4. cikk 1. pontja szerinti érintett, aki az ilyen típusú adatkezelések esetében alapvetően az a természetes személy, aki böngészi a weblapot[98]. A jogviszony másik szereplője a GDPR 4. cikk 7. pontja szerinti adatkezelő a tárhelyszolgáltató pedig az adatfeldolgozó, a pontosítás érdekében ez a személy,

[97] Kivétel abban az esetben van, amikor egy weboldal kizárólag jogi személyekre vonatkozó adatokat kezel, így nem valósul meg a GDPR hatálya alá tartozó adatkezelés.
[98] Őket megilleti a GDPR 12-22. cikkei szerinti érintetti jogok összessége.

aki a weboldallal kapcsolatos érdemi döntéseket meghozza, és ennek keretében meghatározza az itt folytatott adatkezelések célját és eszközeit.

A bevezetés előtti, valamint a bevezetést követő időszakban számos kérdés merült már fel a különböző domainek (elsősorban polgári, személyes blog vagy kkv) vonatkozásában arról, hogy a GDPR kire is vonatkozik valójában, és azt hogyan kell a gyakorlatban megvalósítani a jogszabálynak történő megfelelés érdekében. A GDPR bevezetése előtt számos tévhit vagy nem hivatalos forrásból származó információ jelent meg az interneten a megfelelőséggel kapcsolatban. A webfejlesztők a GDPR tanulmányozása során számos bizonytalansággal találták magukat szemben, és sajnos gyakorlati példák hiányában kevés rálátásuk volt arra, hogy a hatóságok miként fogják értelmezni azt, amikor a jogszabályt alkalmazzák. Ennek oka, hogy a GDPR nem tartalmaz műszaki megvalósítási irányelveket. Az elektronikus felületeken megjelentek az adatkezelési tájékoztatók, valamint részletesen lehet már olvasni több esetben arról, hogyan és milyen biztonsággal tárolják adatainkat.

Kezdetben felugró ablakokat (pop-up) alkalmaztak, és csak az adatkezelési tájékoztató elfogadása után engedett tovább az adott felület a következő hivatkozásra.

Felhasználói szemszögből nézve ez egy további kattintást követően eltűnik (általában olvasatlanul is), és folytathatjuk tovább a navigálást az interneten vagy a vásárlást a webes üzletekben. Ellenben az elmondható, hogy 2019-től 2024-ig ezek a pop-up megoldások részben fejlődtek az alábbiak szerint:

- a pop-up ablak/cella már tartalmaz egy további jelölő cellát, amit, ha megjelölünk „mint” olvasott elem akkor enged csak tovább navigálni;
- a pop-up ablakon belül hiper-link kerül elhelyezésre, ami adatkezelési tájékoztatóra mutat, illetve link mutat a GDPR online módon megtalálható dokumentumára;
- a felugró ablakon belül szövegdobozt helyeznek el, amiben beágyazott szövegként szerepel az adatkezelési tájékoztató;
- a felugró ablakon belül szövegdobozt helyeznek el, amiben beágyazott szövegként szerepel az adatkezelési tájékoztató, aminek a végén egy további harmadik szinten beágyazott elem van, ami szintén egy verifikáló cella.

Üzemeltetői oldalról nézve ugyanakkor az egyik legalapvetőbb feladat, hogy feltöltsük az adatkezelési tájékoztatóinkat a honlapunkra, és erre a tájékoztatóra minden adatbekérés előtt felhívjuk a weboldalra ellátogató felhasználó figyelmét.

Emellett természetesen főbb feladatai is vannak az üzemeltetőnek a GDPR tekintetében, a legmeghatározóbb az adatkezelés körülményeinek megfelelő kialakítása, a GDPR 30. cikke szerinti nyilvántartás vezetése. A honlap látogatóinak megfelelő tájékoztatása is természetesen a feladata[99] és érintetti jogaik gyakorlásának elősegítése[100], valamint az esetleges érintetti nyilatkozatok igazolható módon történő rögzítése. A honlap üzemeltetője köteles továbbá az elvárható szinten technikai és szervezési intézkedéseket végrehajtani annak biztosítása és bizonyítása érdekében, hogy a személyes adatok kezelése a GDPR előírásaival összhangban történjen.

A honlapot össze kell kötni az adatbekérő felülettel. Emellett fel kell tölteni plusz egy kijelölhető opciót (checkbox-ot), ahol a látogató kijelenti, hogy megismerte és elfogadja az adatkezelési tájékoztatónkat.

Fontos megemlíteni, hogy a honlapokon használt mérőkódok, konverziókövetők vagy elemzőszoftverek szintén tárolnak személyes adatokat, erről is tájékoztatni kell a weboldalt felkereső látogatókat, valamint ezen adatok felhasználásának módját is tartalmaznia kell a honlapra, webáruházra szabott adatvédelmi tájékoztató.

A webmarketing munka során elkerülhetetlen tevékenység a személyes adatok kezelése. Már a piackutatástól kezdődően a további elemzéseken át akár egy egyszerű nyereményjátékig személyes adatok futnak be adatbázisainkba. Webmarketing tevékenység során is számos kérdés merül fel a GDPR alkalmazásával kapcsolatban. Alapvetően ebben a helyzetben is a legfőbb kérdés az, hogy a felhasználó vagy vásárló tisztában van-e a rendelet által szabályozott. kritériumok megvalósulásával – vagy annak hiányával.

A weboldalak tekintetében az adatkezelés egyik megkerülhetetlen tevékenysége a sütik alkalmazásával együtt járó személyes adatok begyűjtése.

Sütik tekintetében nem szabad azt a fontos tényt elfelejteni, hogy a GDPR egyértelműen meghatározza azt, hogy az adatkezeléssel kapcsolatos tevékenységet nem hallgatólagosan kell elfogadni, hanem „kifejezett hozzájárulását[101]" kell adnia a felhasználóknak. Főleg, hogy a sütik információkat gyűjtenek a felhasználó weboldallal kapcsolatos tevékenységéről, ami természetesen személyes adatok kezelésével jár együtt, így a GDPR hatálya alá tartozó adatkezelés is megvalósul eközben.

[99] GDPR 13-14. cikkei attól függően, hogy ki a személyes adatok forrása
[100] GDPR 12. cikk (2) bekezdés
[101] kifejezett, ha különleges adatokat is enged kezelni az érintett, egyébként csak hozzájárulás

A sütik tekintetében a NAIH biztosította a helyes bemutató példát az alábbi példa szerint.

Adatvédelmi tájékoztatás

Érintett domain	Kezelt adatkör	Süti típusa	Adatkezelés jogalapja	Adatkezelés célja	Adatkezelés időtartama
naih.hu	SESSION	Munkamenet sütik	A GDPR 6. cikk (1) bekezdés e) pontja, tekintettel a GDPR 24. cikkére és 32. cikkére, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 5. §-ára, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet 3. melléklete szerint elvárt feladatokra és az Ákr. 27. § (2) bekezdésére.	A honlap megfelelő működésének biztosítása	A vonatkozó látogatói munkamenet lezárásáig tartó időszak

17. ábra NAIH süti kezelés példája Forrás: NAIH

A felhasználók további információkat kaphatnak arról, amelyek tájékoztatják őket a sütik letiltásáról. Azaz szükséges egy sütikezelő felület, ahol a felhasználók kezelhetik hozzájárulásukat és vissza is vonhatják azt. [82]

Itt hozzá kell fűzni azt, hogy a sütik esetében több csoportot is el lehet szeparálni. Az adatvédelem szempontjából a csoportokat célszerű felosztani az adatkezelés jogalapja szerint. Azaz megkülönböztetünk:

- weboldal működéséhez elengedhetetlen sütik (jogos érdek),
- funkcionális (jogos érdek),
- analitikai (hozzájárulás),
- reklám célú sütik (hozzájárulás).

Ha az elektronikus felületünkön kizárólag a Google Analytics működik[102], akkor a GDPR ide vonatkozó része nem érint minket, mivel az adatokat itt a Google kezeli. Alapvetően ebből mi csak egy kivonatot látunk a végén (statisztikai adatokat a marketingtevékenység pontosításához, finomhangolásához. Ha az elektronikus felületünkön van Google Adwords[103], Facebook vagy más oldalról származó beágyazott elem, amely a felhasználók adatait gyűjti, akkor meg kell felelnünk az előírásoknak. Ha remarketing hirdetéseket használunk[104], akkor adatvédelmi tisztviselőt kell kijelölni, aki lehet a vállalkozás/szervezet egy alkalmazottja, egy külső cég vagy egyszemélyes cégeknél az ügyvivő által felvett külsős személy. Adatvédelmi tisztviselőnek rendelkeznie kell a szükséges jártassággal. [83]

[102] Ebben az esetben ez harmadik feles süti, erről is tájékoztatni kell, valamint közös adatkezelő lesz a honlapgazda a google-lel.
[103] Hasonló mint az Analytics, azaz mindig meg kell felelnünk a GDPR előírásainak.
[104] Meghatározóan nemcsak ez befolyásolja a DPO kinevezésének kötelezettségét, hanem ha pl. gyógyászati segédeszközös webshopod van, társkeresőt üzemeltetünk.

A süti a napjainkban használt eszközalapú nyomkövető technológiához tartozik, hasonló célt szolgálnak például a helyben történt tárolási objektumok (LSO), a szoftverfejlesztő készletek (SDK), a pixel trackerek vagy pixel gif-ek, a „like" és a közösségi megosztás gombok, valamint az eszköz-ujjlenyomat technológiák is. A sütik a felhasználó (érintett) eszközén tárolt kis adatfájlok, amelyek a felhasználókat azonosítani tudják és képesek nyomon követni az internetes böngészés során. A sütiket csoportosíthatjuk céljuk (funkció, teljesítmény, analitika, közösségi média stb.), időtartamuk (lejárat a böngészési munkamenet végén, lejárat három hónap múlva stb.) és eredetük (azaz első fél vagy harmadik fél) szerint. A sütik tekintetében az „Adatvédelemről alapfokon" című – társszerzővel készített – könyvben részleteiben tárgyaljuk az ePrivacy irányelv és GDPR összefüggését a témában. Továbbá részleteiben kitérünk a magyar szabályozásra is.[105] Részletesen tárgyaljuk a műben a nyomozó hatóságok és a rendőrségről szóló törvényben meghatározott belső bűnmegelőzési és bűnfelderítési feladatokat ellátó, valamint terrorizmust elhárító szerv (nyomozó hatóságok), valamint a nemzetbiztonsági szolgálatok az Eht-ben foglaltak szerinti jogköreit a sütik tekintetében. Emellett kitértünk a „29. cikk szerinti adatvédelmi munkacsoport 2012/4. számú véleménye a sütikhez való hozzájárulás alóli mentességről", (WP194) véleményének elemzésére is. Bemutattuk a francia adatvédelmi hatóság (CNIL) sütifalra vonatkozó kritériumrendszerét. Természetesen itt figyelembe kell venni azt, hogy A CNIL kritériumrendszerét természetesen nem kötelező hazánkban figyelembe venni, ám mindenképpen segítségül hívhatjuk abban az esetben, ha olyan elektronikus felületet üzemeltetünk, amely sütiket alkalmaz. Valamint nincs olyan „egyengyakorlat", amely minden honlap és alkalmazás esetében használható lenne.

Minden weblaphoz külön adatvédelmi tájékoztatót és általános szerződési feltételeket kell készíteni, és a felhasználónak azt jóvá kell hagynia (meg kell ismertetni a felhasználóval). Fontos, hogy minden adatgyűjtés előtt a felhasználó egyértelműen tájékozódjon arról, hogy miért kérik az adatait.

Következtetésként elmondható, hogy csak olyan adatot kérjünk a vásárlótól/ügyféltől, amire gyakorlatban is szükségünk van, vagy használunk az üzemeltetés során. Működési folyamatainkat folyamatosan kísérjük figyelemmel, a működési láncot ismerjük, nézzük meg hol kerülnek az adatok harmadik fél számára átadásra. Itt se adjunk át többet, mint amennyi

[105] Az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.) 155.§

feltétlen szükséges. Ellenőrizzük a harmadik felekkel (mivel ők is adatfeldolgozók[106]) kötött megállapodásokat[107], illetve magát a szerződő partnerünket nyilatkoztassuk a megfelelőségről.

Az oldalt üzemeltetőnek biztosítania kell az adatbiztonságot, és megfelelő intézkedéseket kell hoznia az esetleges adatvédelmi incidensek elkerülése érdekében. Ha adatvédelmi incidens történik, azt jelenteni kell az illetékes adatvédelmi hatóságnak amennyiben az incidens kockázatot jelent az érintettek jogaira és szabadságaira és az érintetteknek is, ha az adatok jelentős kockázatot jelentenek.

Társszerzőmmel a 3. sz mellékletben egy példát is bemutatunk, de a témát részletesen tárgyaljuk az Adatvédelem Alapfokon című könyvünkben, valamint „A GDPR követelményeinek integrációja az elektronikus felületeken" elnevezésű cikkünkben.

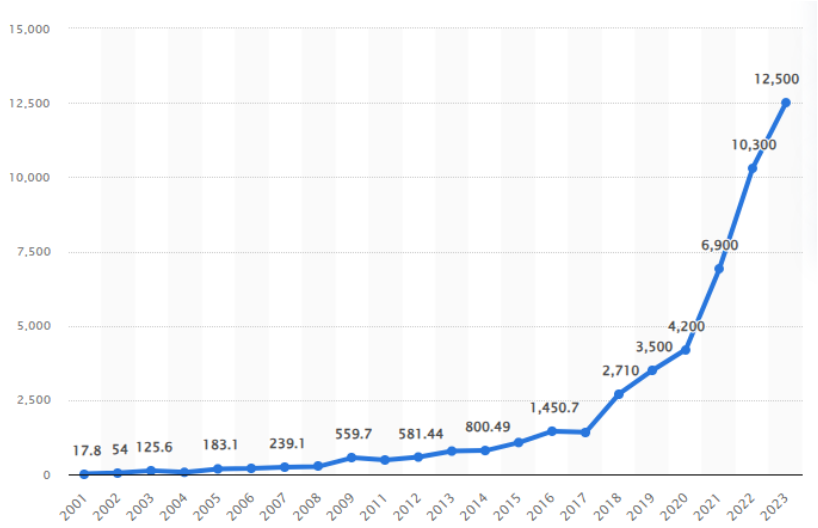
3.5.1 Kockázatértékelés

A webshopok esetében a személyes adatok kiszivárgásának legnagyobb adatvédelmi kockázatai az alábbi területeken azonosíthatók.

A fizetési folyamatok során a webshopok érzékeny adatokat kezelnek. Ha a fizetési rendszerek vagy az ezekkel kapcsolatos adatbázisok nem megfelelően védettek, komoly adatvédelmi incidensek következhetnek be (pénzügyi visszaélés).

Ezt jól tükrözi az ábra, amelyen látható a regisztrált kibertámadások által okozott anyagi kár éves összege az Amerikai Egyesült Államokban 2001 és 2023 között. 2023-ban a kiberbűnözés okozta anyagi kár éves szinten körülbelül 21 százalékkal nőtt, ami 12,5 milliárd amerikai dollár történelmi csúcsot jelent az ábra szerint.

[106] Valamint lehetnek adatfeldolgozók és közös adatkezelők is, erre számtalan bírósági ítélet van EGT-szinten.
[107] GDPR 26. ill. 28. cikkek szerint.



18. ábra 2001-2023 közötti anyagi kár millió dollárba mérve Forrás: www.statista.com

Ezek részben kiküszöbölhetőek a Payment Card Industry Security Standards Council (PCI-DSS[108]) szabványoknak alkalmazásával, biztonságos fizetési átjárók használatával, az érzékeny adatok titkosításával.

A webshopok által tárolt személyes adatok, például nevek, e-mail címek, lakcímek, vásárlási előzmények, célpontjai lehetnek adatlopásoknak vagy fiókfeltöréseknek. Gyenge jelszavak, rosszul implementált hitelesítési rendszerek vagy nem megfelelően védett adatbázisok esetén ezek az adatok kiszivároghatnak. Erős jelszóházirend bevezetése, két-faktoros hitelesítés (2FA[109]) használata, titkosítás alkalmazása az érzékeny adatokhoz, mint például a jelszavak esetében (bcrypt[110] vagy argon2[111] algoritmusok).

Statisztikai 2024. február 21-ei adatok szerint a vállalkozások 57% használt több faktoros azonosítást globálisan, a kormányzati szervezetek 19%-a használ fizikai tokent a 2FA azonosításhoz. A kiberbiztonsági incidensek 80%-a megelőzhető 2FA azonosítás alkalmazásával, viszont a nagyvállalatok 38%-a nem használja a 2FA-t. [84]

[108] A PCI DSS a fizetőkártya-iparág fizikai és információbiztonsági szabványa jelenleg, ez előírja, hogy minden olyan szolgáltatónak és banknak/kereskedőnek, amely a fizetőkártya-tranzakciók adatait tárolja, feldolgozza vagy továbbítja, meg kell felelnie a PCI DSS biztonsági szabványainak.
[109] A kétfaktoros hitelesítés (2FA) egy identitás- és hozzáférés-kezelési biztonsági módszer, amely kétféle azonosítást igényel az erőforrások és az adatok eléréséhez. A kétfaktoros hitelesítés lehetővé teszi a vállalkozások számára a legsérülékenyebb információk és hálózatok figyelését és védelmének biztosítását.
[110] A bcrypt egy jelszó-hashing algoritmus, amelyet a jelszavak biztonságos tárolására használnak. A fő célja, hogy megnehezítse a brute-force támadásokat és megvédje a jelszavakat a kiszivárgások esetén.
[111] Az Argon2 egy korszerű, erőforrás-igényes jelszó-hashing algoritmus, amely a 2015-ös Password Hashing Competition győztese is volt, széles körben elismert és használt jelszóbiztonsági eszköz.

A webshopok gyakran használnak sütiket és egyéb nyomkövető technológiákat, hogy személyre szabott élményt nyújtsanak a felhasználóknak. Ha a sütik és nyomkövetők nem megfelelően vannak kezelve, a felhasználók személyes adatai (böngészési előzmények, vásárlási szokások) illetéktelen kezekbe kerülhetnek. A sütik megfelelő kezelésére vonatkozó irányelvek betartása (hozzájárulás bekérése nem alapvető sütik használatához), adatminimalizálás és harmadik felek adatgyűjtési lehetőségeinek korlátozása. [85]

Az adatbázisokban tárolt személyes adatok (pl. vásárlók adatai és szokásai, rendelések vagy címek) könnyen kiszivároghatnak, ha az adatbázis nem megfelelően van konfigurálva vagy nem elég biztonságos. Egy SQL injekció (SQLi)[112] típusú támadás esetén az adatokhoz könnyen hozzáférhetnek illetéktelen személyek. 2024-ben az SQL injekció alapú sebezhetőségek aránya még mindig magas, a nyílt-forrású projektek 6,7%-ban, míg a zárt rendszerű projektek 10%-ban fordul elő. Bár az arány csökkent 2023-hoz képest (14%-kal nyílt forrású és 17%-kal zárt forrású projektekben), a sebezhetőségek abszolút száma várhatóan nőni fog, 2264-ről 2400 fölé. Ez azt mutatja, hogy az SQLi továbbra is komoly probléma marad, annak ellenére, hogy régóta ismert és kezelhető sebezhetőség. [86]

A személyes adatok felesleges tárolása, túl hosszú ideig történő megőrzése vagy nem megfelelő adatvédelmi protokollok alkalmazása szintén növelik az adatvédelmi kockázatokat. Ez magában foglalja az adattárolási időszakok túllépését és a harmadik felek részére történő szabálytalan adattovábbítást is.

A kockázatok csökkentésének egyik módja az adatminimalizálás és az adatok tárolási idejének szigorú betartása, a harmadik felek adatkezelésének folyamatos felügyelete és auditálása. A webshopok gyakran összetett rendszerek, amelyek különböző pluginokat, bővítményeket és harmadik féltől származó szoftvereket használnak (pl: logisztikai és fizetés). Ezekben a komponensekben biztonsági rések lehetnek, amelyeket a támadók kihasználhatnak.

Szintén hatékony védekezés a felmerült kockázatok ellen a weboldal rendszeres frissítése és a sebezhetőségek időben történő javítása, behatolás tesztelések (penetrációs tesztek) végzése, annak ellenőrzésére, hogy a rendszer mennyire védett a támadásokkal szemben.

[112] Olyan biztonsági rés, amely lehetővé teszi a támadók számára, hogy rosszindulatú SQL lekérdezéseket juttassanak el egy adatbázishoz. Ezt általában akkor használják, ha egy webalkalmazás nem megfelelően kezeli a felhasználói bemeneteket. A támadó képes módosítani vagy manipulálni a lekérdezéseket, például adatokat lopni, törölni vagy módosítani az adatbázisban. Az SQL injekció komoly adatvédelmi és biztonsági kockázatot jelent, ha nem védekeznek ellene megfelelően.

Kutatásomat részletesen „*A GDPR követelményeinek integrációja az elektronikus felületeken*” című társszerzővel készített cikkemben, illetve az *„Adatvédelemről alapfokon”* című könyvben is megtalálható (pp. 124-129).

3.6 Vasúti közlekedés

A vasúti közlekedés üzemeltetése folyamán nagy mennyiségű adat keletkezik, kezdve a közlekedés tervezésétől a lebonyolításon át egészen a közlekedtetésért fizetendő díjak beszedéséig, valamint a személyes adatok letárolásáig. A fejlődés mára már meghaladta a papíralapú adatkezelés rendszerét, a vonatok közlekedésének adatait már alapvetően digitális formában is tárolják szinte minden esetben. [87]

A korszerű közlekedésirányítási rendszereket nagysebességű adatkapcsolatot biztosító informatikai hálózatok kötik össze, ezért ezek a rendszerek fokozottan ki vannak téve a kibertérből érkező fenyegetéseknek. A vasúti fedélzeti jegykiadási rendszer GSM[113] /LTE[114]-rendszert használ a jegyértékesítés folyamán. A vasúti közlekedés területén is szükséges az informatikai védelem továbbfejlesztése és naprakészen tartása.

Az Országos Vasúti Szabályzat vasúti informatikával foglalkozó pontja nem rendelkezik a vasúti informatikai adatok védelméről. A megfelelő védelem kidolgozásához szükséges látni, hogy a vasúti közlekedés során hol és milyen adatok, információk keletkeznek kiemelten például a személyes adatok vonatkozásában. [88]

A digitális hálózatok jelenlegi életünk szerves részét képezi, és gyakorlatilag nem is tudnánk hatékonyan dolgozni vagy közlekedni ezeknek a rendszereknek a használata nélkül. Napjainkban az információs társadalmat a fejlett infokommunikációs eszközök hálózata jellemzi, ami jelentős hatással van a munkavégzés teljes menetére. Krasznay Csaba így foglalta össze röviden az informatika hatását a napjainkra kialakult helyzetre: „A 21. század embere visszavonhatatlanul kibővítette a saját életterét, a fizikai lét mellett az informatikai eszközök és ezek hálózatai által alkotott virtuális tér is meghatározó a modern társadalom működésében.” Ez az alapvetés a vasúti közlekedésre esetében sem alakul máshogy. A vasúti közlekedésben a digitalizáció elterjedésével egyre kevesebb emberi beavatkozásra van szükség, a legújabb

[113] A GSM (Global System for Mobile Communications) az Európai Távközlési Szabványok Intézete (ETSI) által kifejlesztett szabvány a mobiltelefonok által használt második generációs digitális cellás hálózatok protokolljainak leírására

[114] Az LTE (Long Term Evolution) egy negyedik generációs vezeték nélküli adatátviteli szabvány, amelyet a 3GPP Release 8 szabvány ír le.

vasúti biztosítóberendezések automatizáltak, kezelői beavatkozásra üzemszerű működés esetében nincs is szükség.

A vasúti közlekedés során az üzemeltetési adatok kezelése mellett személyes adatok kezelése is folyik. A vasúti közlekedés során a szolgáltató az utasainak és más ügyfeleinek a személyes adatait több – a működéshez szükséges – cél érdekében kezeli. Személyes adatok kezelése az alábbi pontokon folyik:

1. utasok részére menetjegyek (pénztári értékesítés során, MÁV App használata);
2. helyjegyek biztosítása (online) és azok nyilvántartása;
3. valamint kedvezményes utazásra jogosító kártyák és igazolványok elkészítése, nyilvántartása, használatának ellenőrzése;
4. emellett adatkezelést végeznek a panaszok és az észrevételek ügyintézése miatt, valamint az utazás alatti vagyonvédelem és testi épség biztosítása érdekében is;
5. ide sorolható még a velük szemben fennálló követelések érvényesítése miatti adatkezelő-tevékenység is;
6. humán erőforrás számára biztosítandó bér és juttatás;
7. partnerek (aláírási jogosultságok) személyes adatok kezelése;
8. jegykezelés során jogosultság ellenőrzés – külföldi is.

A vasúttársaságok a rendelkezésükre bocsátott személyes adatok feldolgozásához – az érintett hozzájárulásával – külső adatfeldolgozót vehetnek igénybe, amely a neki átadott adatokon csak technikai műveleteket végezhet[115].

A vasúti társaságok a külső félnél végzett adatfeldolgozás jogszerűségéért ugyanúgy felelnek, mint saját adatkezelésükért, amit az adatfeldolgozóval kötött írásos megállapodással biztosít[116]. Az üzemeltető kötelezi magát arra is, hogy adatvédelmi kötelezettségeinek teljesítésére felhívja minden olyan harmadik fél figyelmét, amelynek az adatokat továbbítja vagy átadja.

A vasúti közlekedés üzemeltetése során keletkező adatokat az előírásoknak megfelelően meghatározott ideig tárolni kell[117]. A vonatközlekedéssel kapcsolatos adatokat a MÁV Zrt. saját szerverein tárolja, amelyekhez csak belső intranethálózaton, illetve virtuális magánhálózat (VPN) kiszolgálón keresztül érhető el nyilvános hálózatból.

[115] Például számítógépes rendszerben való tárolás, megőrzés, jegykezelés digitális eszközzel.
[116] a GDPR 28. cikke szerinti tartalommal
[117] Visszakereshetőség, statisztikák, jelentések készítése.

3.6.1 Kockázatértékelés

Kockázatok tekintetében megállapítható, hogy a létfontosságú informatikai infrastruktúrák ellen leginkább kibertámadásokat hajtanak végre, amelyek mára már kritikus mennyiséget értek el. Ilyen jellegű támadásoknál kikerülik vagy üzemképtelenné teszik a tűzfalakat, és behatolnak a zárt rendszerbe, hogy onnan adatokat nyerjenek ki, vagy megváltoztassák a benne lévő adatokat. A vasúti szektort célzó kibertámadások rávilágítanak az összekapcsolt vasúti rendszerek sebezhetőségére és a kibertámadásokra való érzékenységükre, amelyek fizikai térben valós zavarokhoz vezethetnek. A vasúti üzemeltetőknek folyamatosan frissíteniük kell biztonsági protokolljaikat, rendszeres biztonsági auditokat kell végezniük, és be kell fektetniük a legmodernebb technológiákba, hogy megvédjék rendszereiket a potenciális kibertámadásoktól.

A vasút elleni kibertámadás során a szélsőséges szerveztek olyan adatokhoz akarnak hozzájutni, amelyek birtokában fizikai terrorcselekményeket lehet kivitelezni a vasúti közlekedés során az utasok és vasúti infrastruktúra ellen, vagy pedig az irányítórendszerek feletti hatalomátvétel elérésével idézhetnek elő jelentős áldozatszámmal járó szándékos baleseteket.

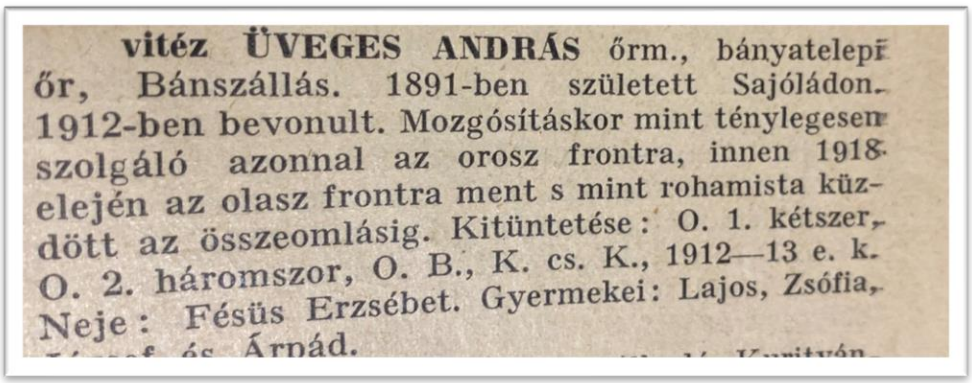
Alátámasztja ezt a Kovács László és Krasznay Csaba szerzőpáros „Digitális Mohács” című tanulmánya is, ahol a közlekedési rendszert is a kiberterrorizmus potenciális célpontjai közé sorolja. [89]

A gyorsabb és biztonságosabb kiszolgálás elősegítése érdekében a blokklánc technológia több helyen is felhasználható a vasúti közlekedésben. Az okosszerződés egy olyan leprogramozott szerződés, amely előre meghatározott feltételek teljesülése után automatikusan végrehajtásra kerül. Így a folyamat megszeghetetlen, és az időben visszamenőleg már nem módosítható. Akár a közlekedési díjak kiegyenlítése során is alkalmazható.

Például a szerződés akkor teljesül, ha az utazás megvalósul. Ez esetben a feltételrendszer változói az utazó személy eszköze és földrajzi helyzete, a felhasználói fiókja – amely kötődik egy zárt blokklánc rendszerhez – és a menetrend szerinti meglévő járat.

Ha az ismert paraméterek alapján – az összes feltétel teljesülése mellett – az utazás megvalósul, akkor az okosszerződéshez kötött fizetési szerződés (vagy folyamat) is végrehajtásra kerül. Ellenben itt is felmerül a személyes adatok kezelésének kérdése, mivel az utasadatok egy része személyes adat. Ellenben, ha ez bekerül egy blokklánc rendszerbe, akkor az utasok jogainak egy része sérülhet. Mégpedig a törléshez való jog, mivel a blokkláncban az időben visszafele nem lehet törölni. Hiszen ezzel a blokklánc alapelvét sértenénk meg.

Ugyanakkor, amikor személyes adatok kerülnek a blokkláncra, az adatvédelmi szempontok különös figyelmet igényelnek. Az ilyen típusú adatkezelés esetén elengedhetetlen, hogy a vasúti rendszerek megfeleljenek a GDPR előírásainak, különös figyelmet fordítva a személyes adatok védelmére. Az adatminimalizálás elve szerint csak a legszükségesebb adatokat szabad gyűjteni és tárolni, miközben biztosítani kell a személyes jogok, például a hozzáférés, a helyesbítés, és a törlés jogainak tiszteletben tartását. Ezen kívül a vasúti rendszerek biztonsága nemcsak a személyes adatok védelmét, hanem az egész infrastruktúra védelmét is jelenti. A rendszeres biztonsági auditok, a tűzfalak megerősítése, valamint a legmodernebb kiberbiztonsági technológiák alkalmazása nélkülözhetetlen a kibertámadások megelőzésére és az adatok védelmére. Az adatvédelmi szabályozásoknak és a kiberbiztonsági protokolloknak együtt kell működniük annak érdekében, hogy a vasúti közlekedés biztonságos, átlátható és jogszerű maradjon. A blokklánc és más modern technológiák számos előnnyel járhatnak a vasúti közlekedés számára, különös figyelmet kell fordítani azok adatvédelmi vonatkozásaira. A személyes adatok védelme és a GDPR szabályainak betartása alapvető fontosságú a jogszerű és biztonságos adatkezeléshez.


vitéz ÜVEGES ANDRÁS őrm., bányatelepi őr, Bánszállás. 1891-ben született Sajóládon. 1912-ben bevonult. Mozgósításkor mint ténylegesen szolgáló azonnal az orosz frontra, innen 1918. elején az olasz frontra ment s mint rohamista küzdött az összeomlásig. Kitüntetése: O. 1. kétszer, O. 2. háromszor, O. B., K. cs. K., 1912—13 e. k. Neje: Fésüs Erzsébet. Gyermekei: Lajos, Zsófia, és Árpád.

A társszerzőmmel készített „*A vasúti közlekedés informatikai adatvédelme”* című, valamint a „*A közlekedési rendszerek és az információs terrorizmus kapcsolata”* című publikációmba

3.7 Korszerű katonai kiképző rendszerek

A honvédelmi ágazat kiképzési szakterülete már a modern katonai és nemzetbiztonsági kiképzési rendszereket megelőzően is rögzített személyes adatokat, ha nem is a ma ismert módon és módszerekkel.

Személyes adatokat a kiképzéshez természetesen a honvédelmi szektorban is rögzítették. Nem csak a kiképzéshez hanem egyes archívumoknak és például ezred könyveknek is.

20. ábra Vitéz Üveges András őrmester

19. ábra Kivonat A Cs. és Kir. 34. Magyar Gyalogezred Története című ezredkönyvből (1734-1918)

Az 1970-es években a dandárok, ezredek és az alárendelt alegységek is kezelték a kiképzéshez szükséges személyes adatokat. Mivel az említett időszakban az informatikai támogatás alapvetően nem létezett, ezért az adatokat papírra rögzítették. A sorállományú katonák kiképzésének eredményeit, személyes adatait egyéni értékelő lapokon tartották nyilván. Ezeken a dokumentumokon a katona neve, rendfokozata, beosztása szerepelt, amelyek a szakasz- és századnaplókba kerültek lefűzésre. Ezeket az okmányokat a század- és szakaszparancsnokok tárolták. Az értékelések havonta érdemjegyekkel történtek, illetve kiképzési időszakonként ezek átlagát rögzítették. Az értékelés kiterjedt az általános katonai, illetve a szakmai kiképzésre. A hivatásos és a szerződéses továbbszolgáló katonák esetében havonta általában egy alkalommal volt összevont kiképzés, amely magában foglalta az általános katonai és a szakmai ismereteket. A részvételt ezeken a foglalkozásokon kiképzési naplóban rögzítették. A naplóban a foglalkozáson részt vevő katona neve és rendfokozata szerepelt. Az ezred, dandár teljes hivatásos állománya és a szerződéses továbbszolgáló állomány személyes adatait, személyügyi gyűjtőit az ezred, dandár parancsnokságán a személyügyi szervek kezelték. A sorállomány személyes adatait a hadkiegészítési és mozgósítási részlegek kezelték, az alegységeknél az „m-kieg” tiszthelyettes. A parancsnokok a közvetlen alárendelt állományuk adatait megismerhették. Az egység, magasabb egység parancsnoka betekinthetett a teljes személyi állomány személyes adataiba, személyügyi gyűjtőibe, hiszen nem hozhatott volna felelős döntéseket enélkül.

A légvédelmi rakétadandároknál az éles légvédelmi rakétalövészetre történő felkészülés és a gyalogsági lövészetek eredményeit jegyzőkönyvekben tartották nyilván, ahol a katona neve, rendfokozata, illetve az első esetben beosztása szerepelt. A naplókat, illetve a jegyzőkönyveket a dandár- és ezredtörzsben a hadműveleti és kiképzési alosztály, a légvédelmi rakétaosztályoknál a törzsfőnök tárolta, amelyek nyilvántartási számmal voltak ellátva, a megőrzésük idejét szabályzók rögzítették. A kiképzéssel, felkészítéssel kapcsolatban HM-szintű rendelkezések voltak az irányadóak. A kiképzési eredményeket a vizsgált időszakban elektronikusan nem rögzítették. A kiképzési terveket, naplókat a század- és szakaszparancsnokok, valamint a hadműveleti és kiképzési alosztályvezetők tárolták páncélszekrényben. A személyi állomány kiképzéséért, felkészítéséért az állományilletékes parancsnok volt a felelős. A kiképzést ezred- és dandárszinten a parancsnok általános helyettese

szervezte, irányította és ellenőrizte. A légvédelmi rakétaosztálynál ez a törzsfőnök feladata volt. Ebben az időszakban kifejezetten a személyes adatok védelmére külön személy nem volt megbízva, kijelölve. A szakasz és század kiképzési tervei nyilvánosak voltak, az alegységek elhelyezési körleteiben ki voltak függesztve. Ezeken az okmányokon a kiképzést végrehajtók neve, rendfokozata szerepelt. A tervek nyilvántartási számot kaptak, majd iratgyűjtőben helyezték el őket. Megőrzésük idejéről külön jogszabály rendelkezett. Az elöljáró szervek végezték az erre a feladatra történő felkészülést, ellenőrzést és vizsgáztatást.[118]

A korszerű katonai kiképző rendszerek minden esetben többféle személyes adatot kezelnek (2. sz. melléklet), hogy biztosítsák a hatékony és biztonságos kiképzést. Ezek az adatok különböző rendszerekben és adatbázisokban tárolódnak, és a megfelelő adatvédelmi szabályozások betartása mellett kerülnek felhasználásra, elemzésre és értékelésre.

Az adatkezelés céljai alapvetően a kiképzés tevékenység hatékonyságának növelése, a katonák fizikai-, és mentális alkalmasságának biztosítása. Azt is meg kell jegyezni, hogy emellett a kiképzéssel foglalkozó szervezetek az oktatási intézményekhez hasonlóan közfeladathoz hasonló tevékenységet látnak el, így ezeknél az intézményeknél az adatkezelés jogszabályi alapon történik. Fontos kiemelni azt is, hogy a modern kiképzőrendszerek a jövőben nem feltétlenül működnek majd a rendvédelmi szervezetek közvetlen irányítása alatt vagy azoknak a kötelékében. Így ennek tekintetében a GDPR alkalmazása egy modern polgári iparágban tevékenykedő, kiképzési szolgáltatásokat biztosító vállalkozásnál elengedhetetlen követelménnyé vált napjainkra.

A korszerű kiképző rendszerek esetében a személyes adatok kezelésének két kérdésköre merül fel, amit vizsgálni kell. Az egyik, hogy a szervezetnek meg kell felelnie ma már a GDPR és az Infotv. követelményeinek, valamint hogy biztosítani kell a személyes adatok kezelése, gyűjtése és feldolgozása során az informatikai biztonságot.

Alapvetően elmondható az, hogy az érintett egyértelmű hozzájárulása szükséges minden olyan adatkezelés esetén, amely kívül esik a kiképzési környezet jogszabályban meghatározott adatkezelési körén. Külön tájékoztatást kell adni és hozzájárulást kérni, amennyiben a vállalkozás adatfeldolgozás céljából valamely, nem jogszabályban meghatározott szervezet számára adatokat ad át.

Egy korszerű lövészeti kiképzőrendszer esetében ilyen adat lehet például az élet- és balesetbiztosítás előzetes megkötéséhez szükséges személyes adat. Emellett a digitális

[118] Saját interjú anyaga: Üveges András ezds. MH DUNA 5011 kik. és hum. ov.

társadalom és maga a korszerű kiképzéstámogató rendszerek egy része is mára tartalmazza a távoktatás egyes elemeit. Így a kiképzendő állomány az elméleti oktatási anyagokat elektronikus úton kapja meg, ezért a kiképzési adatbázisokban tárolt elektronikuslevél-címek is az adatkezelés hatálya alá esnek. A levelezést viszont nem feltétlenül a kiképzést közvetlenül végrehajtó vállalkozás végzi, hanem egy harmadik fél[119].

Természetesen ebben az esetben a harmadik felet is nyilatkoztatni kell arról, hogy az Infotv. és/vagy a GDPR szabályait milyen módon alkalmazza. A kiképzést végző vállalkozásnak meg kell győződnie arról, hogy a kiképzési adatállományt kezelő harmadik fél tevékenysége is megfelel a GDPR előírásainak, illetve jogilag kötelező érvényű megállapodással[120] kell rendelkeznie minden olyan partnerével, amely az intézmény által kezelt személyes adatokat feldolgozza. Ez alól kivétel, ha az adatok továbbítását a harmadik fél részére jogszabály írja elő.

Mindenki számára transzparenssé kell tennie az adatkezelési folyamatokat annak közlésével, hogy milyen adatok begyűjtése történik, és mi az adatkezelés jogalapja. Milyen jogai és milyen jogorvoslati lehetőségei vannak az érintettnek, valamint ki az adatbekérő. A szervezetnek rendelkeznie kell adatvédelmi tisztviselővel.

Emellett kiemelten fontos az, hogy a kiképző szervezettől továbbított adatok pontos címzettjeinek listája is vezetve legyen. Biztosítania kell, hogy az alkalmazottak munkakörüknek és felelősségi körüknek megfelelő felkészítést kapjanak a GDPR szabályrendszeréről és megfelelőségi követelményeiről. Általános adatvédelmi képzést kell kapnia a kiképzőállomány minden tagjának, emellett részletesebb felkészítést a vezető (tulajdonosi) állománynak is. [90]

Kutatásom és értekezésem elkészítésének ideje alatt egy korszerű kiképzőeszközzel kapcsolatos kutatás és fejlesztés is folyamatban van. Ennek tekintetében kutatótársam révén lehetőségem nyílt betekinteni és elemezni egy új fejlesztés adatbiztonsági kérdéseibe, valamint aktualizáltam a jelenlegi helyzettel kapcsolatos információkat.[121]

Az elhangzottak alapján a következőket lehet megállapítani. A korszerű katonai kiképző rendszereknél már a tervezés során figyelembe veszik az adatbiztonsági tényezőket.

[119] Ebben az esetben ez lehet szerződés vagy jogos érdek alapú is.
[120] GDPR 28. cikk
[121] Interjú Marlok Tamással, 2025.02.10.

Ez nemcsak szoftverfejlesztési, hanem szoftver architekturális kérdés is. A megfelelő üzemeltetési és szoftver architektúra már nagyban biztosítja a törvényi megfelelőséget és az incidensekkel szembeni ellenállóságot. Azaz ez megerősíti azt, hogy a korszerű katonai kiképző rendszerek szoftverarchitektúrájának tervezése szoros összefüggésben áll a személyes adatok védelmével mind fizikai, mind szoftveres szinten.

Ezek a rendszerek gyakran gyűjtenek és elemeznek érzékeny adatokat, például a felhasználók biometrikus és teljesítményadatait, amelyek védelme kiemelten fontos. Fizikai szinten a rendszerek biztonságos helyszíneken történő üzemeltetése, a hardveres hozzáférés kontrollálása és a titkosított adatkapcsolatok használata biztosítja az illetéktelen hozzáférések elkerülését. Szoftveres szinten a biztonságos adatkezelési elvek (pl. adatminimalizálás, titkosítás) beépítése, a hozzáférési jogosultságok szigorú szabályozása és a GDPR-nak megfelelő adatkezelési gyakorlatok kulcsfontosságúak.

A jól megtervezett architektúra tehát nemcsak a hatékonyságot, hanem az adatbiztonságot is garantálja, megvédve a felhasználók személyes információit.

Az említett digitálisan is korszerű kiképzőeszközök architektúráját már a tervezés során felkészítik az adat- és információbiztonsági incidensek kezelésére. Alapvetően egy immerzív virtuális valóság technológia alapú kiképzőeszközről van szó, amely lövész katonák, különleges egységek tagjainak a lövészeti és harcászati képzését segíti. Pontosabban katonai lövészeti, immerzív virtuális valóság technológia alapú kiképzőeszköz egy olyan szimulációs rendszert alkot, amely valósághű környezetet teremt a katonák kiképzéséhez. Ez a technológia VR-szemüvegek, mozgásérzékelők és speciális fegyverszimulátorok segítségével biztosítja a lövészeti és taktikai készségek fejlesztését, miközben minimalizálja a valós fegyverek használatából adódó kockázatokat. A rendszer interaktív és valós idejű visszajelzéseket nyújt, lehetővé téve a felhasználóknak, hogy biztonságos és költséghatékony módon gyakoroljanak különféle harci szituációkat.

Az egyik adatbiztonsági tervezési elv, hogy a kiképzési adatok, amelyek létrejönnek a rendszerben nem kapcsoljuk azonosítható felhasználókhoz. Ez esetben, az alegységek gyakoroltatása során a rögzített információ csupán a katona csoportban lévő pozíciójához van kötve.

A gyakorlási adatok a kiképzési feladat eredményein túl, a feladatban történt összes mozgást, a lövések irányát, találatokat, illetve több, a biztonsági rendszabályok betartásával kapcsolatos

kiértékelést is tartalmaz. Az így gyűjtött adatok egyetlenegy azonosítóhoz vannak csatolva, amely semmilyen formában nem tartalmaz személyes adatokat.

Az interjú szerint a tervezés során két lehetőséget kell mérlegelni:

1. komplex megoldás, amikor a nem változó személyes információkból, pl. születési név, dátum, nem, születési hely egy egyirányú hash-elési algoritmussal képzünk egyedi azonosítót a kiképzőrendszerben történő használathoz.
2. Az egyszerű megoldás esetén a kiképzőrendszerben kiosztunk egy mindentől független, de egyedi azonosítót (lehetőleg nem sorszámot, hanem például „GUID”[122]-ot), amelyet nem a kiképzőrendszeren belül kötünk össze, hanem egy másik rendszerben, mint például személyügyi nyilvántartásban, amely megfelel az információbiztonsági követelményeknek.

Mindkét esetben a cél az, hogy a kiképzőrendszer adatbiztonsági szempontból ne kezeljen aggályos adatokat. Emellett mindkét esetben kell lennie egy olyan szoftvermodulnak az architektúrában, amely szükség esetén, a megfelelő összekapcsolást úgy végzi el, hogy annak működése és adatai megfelelően védettek legyenek.

Az ilyen összekapcsolás minden olyan esetet jelent, amikor név szerinti kiértékelésre van szükség. Ez lehet alegység szintű összesítés, vagy egyéni szintű kiképzési adatok megjelenítése az elöljárók számára. A tervezés során tehát minden olyan kiértékelési adatlapot, ahol szóba jöhet a személyes adatokkal való összekapcsolás, vagy akár alegységbeli beosztás megjelenítése a kiképzési adatok fényében, megfelelő átgondolás és tervezés szükséges információbiztonsági szempontból is.

Saját álláspontom szerint a fentiek figyelembevételével megállapítható, hogy a nem változó személyes információkból egy egyirányú „hash-elési” algoritmus (SHA-256) segítségével egyedi azonosítót lehet képezni, amely részben anonim módon használható a virtuális kiképző rendszerben.

A „hash-elési” folyamat biztosítja, hogy az eredeti adatok ne legyenek visszafejthetők, valamint az azonosítók egyediek lesznek, ha megfelelő algoritmust használunk. Ezek használatával a

[122] Szoftveralkalmazások által használt álvéletlen szám – vagy olyan egyedi azonosító, amelyet arra terveztek, hogy globálisan egyedülálló legyen. A GUID általában 128-bites szám, amely hexadecimális formában jelenik meg, és annyira nagy, hogy gyakorlatilag lehetetlen, hogy két GUID egyforma legyen. A GUID-okat gyakran használják adatbázisokban, fájlrendszerekben vagy elosztott rendszerekben objektumok azonosítására. Példa az említett fogalomra: d9b2d63d-6d9b-4f6a-8f9b-47f9d6d9310b

rendszer nem tárolja az eredeti személyes adatokat, így minimalizálja az adatvédelmi kockázatokat.

Valamint ezzel a megoldással az általános elgondolás miatt, az azonosítók könnyen integrálhatók különféle rendszerekbe. Viszont kerülni kell az elavult algoritmusok (MD5, SHA-1) alkalmazását, mivel ezek sebezhetőek lehetnek ütközések[123] vagy visszafejtés szempontjából.

A korszerű és biztonságos hash algoritmus használata (SHA-256 vagy BLAKE2) viszont feloldja ezt a problémát.

Az azonosítók tényleges anonimizálása érdekében egyedi "sót" (random érték) kell hozzáadni a „hash-elés" előtt, hogy elkerüljük az egyszerű hash-táblázatok vagy "rainbow table"-ek alapján történő visszafejtést. Pontosabban, a jelszó „hash-elése" önmagában nem biztosít elég védelmet. Ha egy egyszerű, nem sózott hash-t tárolunk az adatbázisban, akkor egy támadó könnyedén visszafejtheti a jelszót, ha rendelkezésére állnak szivárványtáblák, amelyek a gyakran használt jelszavak hash-ét tartalmazzák. Ez azért lehetséges, mert az azonos jelszavak mindig ugyanazt a hash-t generálják, így ha egy adatbázisban több felhasználó is ugyanazt a jelszót használja, akkor azok hash értékei azonosak lesznek, ami segít a támadóknak a jelszó gyors kitalálását.

A sót biztonságosan tárolni kell, hogy szükség esetén ugyanazon személy azonosítója újra előállítható legyen. A hash algoritmusnak hatékonynak kell lennie a nagy mennyiségű adat feldolgozása során, különösen egy virtuális kiképző rendszerben, ahol valós idejű feldolgozás lehet szükséges. Amennyiben a sózás lehetővé teszi az azonosítók visszakeresését, akkor a megoldás "pszeudonimizáltnak" számít, ami még mindig személyes adatnak minősül GDPR szerint. Ha a só random és nem kerül tárolásra, a megoldás anonimizáltnak minősülhet.

Ha kombináljuk a felhasználó várhatóan nem változó személyes adatait[124] egyedi sóval, majd hash-eljük az eredményt az általunk választott algoritmussal, és tároljuk csak a hash-t, akkor egy működő modellt kaphatunk. Természetesen biztosítani kell azt, hogy a sókat és a „hash-elési" folyamatot csak azok az érintettek érjék el, akiknek ez szükséges. A rendszeresen auditált algoritmusok biztosítják a rendszer integritását. Ezzel a megközelítéssel egy olyan rendszert

[123] A hash ütközés vagy „hash collision" esetében két különböző bemenet ugyanazt a hash értéket (összegző értéket) eredményezi egy adott hash függvény alkalmazásával. Mivel a hash függvények véges hosszúságú kimenetet állítanak elő, de a bemenet tetszőleges hosszúságú lehet, matematikailag elkerülhetetlen, hogy létezzenek olyan különböző bemenetek, amelyek ugyanazt a hash értéket adják.
[124] salt + születési_név + dátum + nem + születési_hely

lehet létrehozni, amely hatékonyan biztosítja a személyes adatok védelmét, miközben megfelel a korszerű adatvédelmi követelményeknek.

Kockázatértékelés

A korszerű digitális katonai kiképző rendszerekben a személyes adatok kezelése jelentős kockázatokat hordoz, különösen a biztonsági és adatvédelmi szempontok tekintetében. Abban az esetben, ha az informatikai rendszer nem megfelelően védett, külső ellenérdekeltségű szervezetek vagy személyek vagy belső rosszindulatú elkövetők jogosulatlanul hozzáférhetnek a kiképzési és kiképző állomány személyes adataihoz, beleértve a katonák nevét, beosztását, kompetenciáit és más érzékeny információkat, amelyek kihasználhatóak lehetnek hírszerzés, zsarolás vagy fizikai támadások kivitelezése céljából.

A digitális kiképzési rendszerekben rögzített adatok alapján a katonai személyzet sebezhetőségeire vonatkozó információk is kiszivároghatnak. Ha egy kiképző rendszer elemzi a felhasználók gyengeségeit, ez az információ felhasználható lehet célzott támadásokhoz vagy dezinformációs kampányokhoz egy ellenérdekeltségű szervezet szemszögéből.

Információk szerezhetők be a katonai személyzet képességeiről, pszichológiai állapotáról, így következtetések vonhatóak le és automatikus profil alkotó rendszerek használhatják fel az adatokat. Ha ez az adat illetéktelen kezekbe kerül, akkor akár geopolitikai vagy stratégiai döntéseket is befolyásol, különösen, ha egy ellenérdekeltségű fél használja fel.

A személyes adatok hanyag kezelése vagy tárolása (pl. titkosítás hiánya) szintén adatvédelmi incidensekhez vezethet. Emellett, ha az adatok nem naprakészek, helytelen következtetésekre vezethetnek az elemzések során.

A GDPR és/vagy az Infotv. előírja a személyes adatok védelmét és megfelelő kezelését. Ha egy katonai kiképző rendszer üzemeltetője nem tartja be az előírásokat (pl. nem biztosítja a önkéntesség megszerzését, vagy nem teszi lehetővé az adatok törlését), akkor jogi következményekkel fog szembesülni.

A katonai kiképzési rendszerekhez kapcsolódó személyes adatok kiszivárgása nemcsak az egyéneket, hanem az egész katonai al- és magasabb egységeket, stratégiákat és műveleteket veszélyeztetheti. Az ilyen adatok segítségével egy ellenséges fél felderítheti, és aktuális képet kaphat a haderő személyi struktúrájáról és működéséről.

Mivel a digitális katonai rendszerek különösen érzékeny adatokat kezelnek, elengedhetetlen az adatvédelmi hatásvizsgálat elvégzése, amely elemzi az adatkezelés kockázatait, és segít azokat minimalizálni. A DPIA elmulasztása növeli a hibás adatkezelési gyakorlatok kockázatát.

Ezek a kockázatok mind a technológiai, mind pedig a jogi megközelítésben alapvető figyelmet igényelnek annak érdekében, hogy a katonai rendszerek ne váljanak sérülékennyé, és megfeleljenek a nemzetközi adatvédelmi előírásoknak.

3.8 Közösségi média

A közösségi média használata számos biztonsági kockázatot rejt a felhasználók számára. Ezek a kockázatok többféle formában jelentkezhetnek, és fontos tisztában lenni velük a biztonságosabb online jelenlét érdekében.

Az előzetes kutatások tekintetében számos kockázat azonosítható, de ezek közül a legrelevánsabb a honvédelmi ágazat szempontjából az, hogy a közösségi média alkalmazása egyre gyakoribb a fegyveres konfliktusok esetében is.

A fegyveres konfliktusok közben a nemzetközi és a résztvevő ország közvéleményének befolyásolására a felek gyakran alkalmazzák az információs műveleteket. A fegyveres konfliktusok kitörésekor a közösségi média (X, Telegram, Facebook stb.) alkalmazása meghatározó szerepet tölt be napjainkban. A hatékony információs műveletek kivitelezéséhez elengedhetetlen az, hogy megfelelő mennyiségű és minőségű személyes adattal rendelkezzen a műveletet végrehajtó entitás. [91]

Az információs társadalom elterjedését követően, megnőtt az információs műveletek fegyveres konfliktusokban játszott szerepe, amelyek a klasszikus értelemben vett hadszíntereken zajló katonai tevékenységekkel párhuzamosan történnek szinte minden esetben, kivétel természetesen a globális és folyamatos megfigyelési kampányok, vagy kiberbűnözői tevékenység.

A témában Dr. Krasznay Csaba is felhívta a figyelmet az információs műveletek felértékelődésére. [92] A Kiberhadviselés az orosz-ukrán konfliktus árnyékában címet viselő előadásában, a történelmi áttekintést követően többek közt ismertette az úgynevezett negyedik generációs hadviselés főbb jellemzőit, melynek már része az információs környezet hadászati célú felhasználása is.

Kutatásom során vizsgáltam azt, hogy az információs műveletek során felhasznált személyes adatok milyen formában jelentek meg és milyen kockázatot rejtettek. Az orosz-ukrán fegyveres konfliktus során az orosz vezetés felismerte azt, hogy a személyes adatok felhasználása akár

fegyverként is alkalmazható. Ennek tükrében az orosz törvényhozók jóváhagyták azt a törvényjavaslatot, amely korlátozza az orosz állampolgárok személyes adatainak külföldre továbbítását.

2022 második félévében elmondható, hogy a kinetikus katonai műveletek mellett a kiber- és információs műveletek váltak a legmeghatározóbbakká a konfliktusok során.

Egy konfliktushelyzetben alapvető cél a saját oldalon a szervezett rend, az irányíthatóság és ellenőrizhetőség fenntartása, a másik fél oldalán pedig ennek ellenkezője, a szervezetlenség és az irányíthatatlan, ellenőrizhetetlen állapot előidézése, ideiglenes kialakítása. Ezt saját oldalon pozitív, az ellenérdekeltségű félnél negatív irányú, egymással összehangolt információs művelettel lehet elérni. [93]

Az információs tér szempontjából az ukrán-orosz válság nemcsak a honvédelmi (katonai) szektort érinti, hanem a teljes össztársadalmi digitális teret az alábbiak szerint:

1. a közigazgatás;
2. a közlekedés, utazás;
3. a rendvédelem;
4. nemzetbiztonság;
5. a honvédelmi ágazat katonai információs környezete;
6. a pénzügyi, gazdasági, kereskedelmi szektor;
7. a közösségi média, online üzenetküldő platformok, bloggok, statikus és dinamikus weblapok;
8. létfontosságú információs infrastruktúra és létfontosságú infrastruktúra;
9. ITC környezet.

A személyes adatok kezelése és annak biztonsági (bizalmassági) kérdései az áldozatok hozzátartozóinak és a háborús bűnök elszenvedőinek, valamint tanúinak tekintetében is felmerült az alábbiak szerint:

1. a tanúk védelme érdekében csak minimális személyes adatot dokumentálnak a fegyveres harcok után annak érdekében, hogy a tanúk azonosítását megakadályozzák;
2. pszeudoanonimizálást alkalmaznak a tanúk védelme érdekében, továbbá a katonai műveletek (esetlegesen háborús bűncselekmények) elől elmenekült ukrán vagy orosz lakosok monitorozása során.

Az áldozatok azonosítása során dokumentálják az exhumáltak adatait, amelyek azonban már nem a GDPR értelmében vett személyes adatok, azonban az elhunyt személyekkel kapcsolatban is számtalan személyes adat szivároghat ki, például a hozzátartozók, illetve a vizsgálatokat végzők személyes adatai.

A személyes adatok megszerzése is több esetben célja volt a konfliktus során az információs műveleteknek. 2022. február 18-án a Amerikai Egyesült Államok kiberbiztonsági és infrastruktúra-védelmi ügynöksége (CISA[125]) útmutatást adott ki az orosz-ukrán konfliktusról. A „Cisa Releases New Insight To Help Critical Infrastructure Owners Prepare For And Mitigate Foreign Influence Operations" elnevezésű dokumentum már azonosítja a kockázati tényezőket az egyes cégeknél dolgozó alkalmazottak személyes adatainak kiszivárgása tekintetében. Az ajánlás külön kiemeli, hogy a munkavállalók közösségi média felhasználók (személyes adataikkal együtt) kiemelten fontosak, hiszen megszerzése után ezen adatok segítségével könnyen be lehet jutni egy adott informatikai rendszerbe. [94] [95]

A nyílt internetre kikerült személyes adatok nagy mennyisége – függetlenül az érintett nemzetiségétől – jelentős kockázattal bír az érintettek jogaira és szabadságaira. A GDPR vonatkozásában megállapítható, hogy ez a kockázat akkor merül fel, amikor a konfliktus során a két érintett fél például az Unió területén tartózkodó érintettek személyes adatait szivárogtatja ki.

A GDPR alapján jogérvényesítésre (szankciók alkalmazására) a fegyveres konfliktusban részt vevő adatkezelők esetében nincs sok lehetőség, azonban például a portugál adatvédelmi felügyeleti hatóságnak van olyan határozata, amely ukrán menekültek személyes adatainak jogszerűtlen kezelésével, illetve a gyanú szerint Oroszországba kerülésével kapcsolatos.[126]

Ha a kockázatokat csoportosítjuk, akkor meg kell különböztetni:

1. konfliktuson belüli kockázati tényezőt (orosz vagy ukrán személyes adat sérülése);
2. konfliktushoz részben köthető kockázati tényezőt (csecsen, grúz, iráni stb. külföldi zsoldos személyes adatainak kezelése);
3. valamint nemzetközi viszonylatban értékelhető tényezőket.

A felmerülés területének szempontjából:

1. a surface netre internetre kiposztolt vagy cikkben megjelent személyes adatok;
2. Dark Weben értékesített személyes adatok.

A közösségi média használata az átlag felhasználók számára különösen nagy kockázatot jelenthet a személyes adatok kiszivárgása szempontjából.

3.8.1 Kockázatértékelés

Az alábbiakban szerint a következő kockázatok azonosíthatóak:

[125] Cybersecurity and Infrastructure Security Agency - A CISA a belső biztonsági minisztérium (DHS) alá tartozik, és feladata a kormányzati és magánszektorbeli kritikus infrastruktúrák, például az energia-, közlekedési-, és pénzügyi rendszerek védelme a kiberfenyegetésekkel szemben.
[126] https://www.cnpd.pt/en/

Számos felhasználó tévesen állítja be a profiljának adatvédelmi beállításait, így személyes adatai nyilvánosan elérhetők maradnak a későbbiekben. A nyilvánosan megosztott bejegyzések, fotók és videók sokkal szélesebb körhöz juthatnak el, mint amennyire a felhasználó számít, hiszen a célcsoporton kívülre is megjelennek ezek a tartalmak.
Sok felhasználó megadja a hozzáférést a személyes adataihoz harmadik fél számára, amelyek nem mindig biztosítják megfelelő adatvédelmet, vagy egyáltalán nem rendelkezünk információval arról, miként kezeli, a személyes adatinkat. Ezek az alkalmazások gyakran megosztják az összegyűjtött adatokat más szolgáltatásokkal és partnerekkel.
Az adathalász weboldalak a közösségi média platformok hiteles megjelenését másolják, hogy megtévesszék a felhasználókat. A közösségi média platformok biztonsági rései és hibái révén hekkerek hozzáférhetnek a felhasználók személyes adataihoz. Számos esetben derült fény arra, hogy közösségi média platformok nem megfelelően kezelték a felhasználók adatait, és azokat harmadik felek számára hozzáférhetővé tették (pl. Cambridge Analytica botrány).
A nyilvánosan elérhető személyes adatok révén könnyebben válnak a felhasználók zaklatás áldozatává.
A helymeghatározás alapú szolgáltatások révén illetéktelenek könnyen meghatározhatják a felhasználó tartózkodási helyét. A közösségi médiában megosztott tartalmakat a munkáltatók is láthatják, ami befolyásolhatja a felhasználó munkahelyi megítélését és későbbi karrierjét. A személyes adatok védelme érdekében érdemes átgondoltan kezelni a közösségi médiában megosztott információkat, megfelelő adatvédelmi beállításokat alkalmazni, és óvatosnak lenni a harmadik fél számára adatot átadni kívánó alkalmazásokkal szemben.
A honvédelmi ágazatban azonosított kockázatok mellett a legnagyobb problémát jelenti, hogy a közösségi médiában megosztott személyes adataink és profil beállításunk segítségével digitális személyiségünk könnyűszerrel másolható.
Arról nem beszélve, hogy a közösségi média profilbeállításaiból kinyert információk összesége viszont érzékeny és különleges adatokat is tartalmazhat (keresési előzmények, kedvelt csoportok, nemi identitás stb.). Alapvetően itt is megállapítható az, hogy ez a kockázat csökkenthető lenne a felhasználók biztonságtudatos magatartásának erősítésével. Alapvetően ezek az adatok az elsődleges célpontjai az adathalászoknak, adatbányászoknak és marketing cégeknek. A gyakorlatban ezekre a problémákra már számos előre programozott algoritmus van, ami az online közösségi felületünk beállításait automatikusan módosítja [96]

3.9 IoT eszközök

Az IoT -eszközök alkalmazása és a digitalizációs folyamatok felgyorsulása exponenciálisan nő napjainkban. A honvédelmi ágazatban egyre több IoT-eszköz kerül alkalmazásra, egyre több esetben kell vizsgálni ezen eszközök kiberbiztonsági, információbiztonsági és nemzetbiztonsági kockázatait. Az IoT-eszközök nemcsak a honvédelmi szektorban alkalmazott rendszerek elemeiként jelenhetnek meg, hanem a hivatásos és szerződéses, tartalékos katonák, köztisztviselők és kormánytisztviselők, beszállítók munkatársainak személyes használati tárgyaként is. Így szükségszerű ezt a jelenséget is vizsgálni, mivel a napi tevékenység végzése közben számos, eddig nem használt IoT-eszköz jut be laktanyákba vagy egyéb objektumokba.

Tágabb értelemben a dolgok internete meghatároz minden olyan informatikai eszközt, amely vezeték nélkül csatlakozik az internetes hálózathoz. Szűkebb értelemben az IoT olyan összekapcsolt eszközrendszert jelent, amelyek érzékelőkkel, szoftverekkel és más technológiákkal vannak ellátva, így az adatok továbbítását és fogadását vagy akár helybeni feldolgozását is elvégzi. [97]

Az ENISA meghatározása szerint a tárgyak internete „az egymással összekapcsolt érzékelők és működtetők kiberfizikai eszközök ökoszisztémája, amely intelligens döntéshozatalt tesz lehetővé”. Az ügynökség a tárgyak internetének középpontjába az információt helyezi. [98]

Jellemzően a kommunikációs csatorna Wi-Fi hálózat, illetve 5G hálózati platformok, amelyek biztosítják a nagysebességű összeköttetést.

21. ábra Okos eszközök[127]

Az IoT-eszközök jelentős nemzetbiztonsági kockázatot okozhatnak akkor, ha nem vizsgáljuk megjelenésük és gyors terjedésük okozta kockázati tényezőket. Jelenleg nincs rendszerezve, megbecsülve, valamint osztályozva, hogy milyen csatornákon milyen kockázati tényezőt jelent az érzékeny adataink kiszivárgása ezen eszközökön keresztül. Azt is figyelembe kell venni, hogy az IoT eszközök hatékony működéséhez „elengedhetetlen az ember–gép közötti interakciók számának, valamint a felhasználóról begyűjtött adatok mennyiségének és szenzitivitásának növekedése is. Ugyanis az okoseszközök életünkbe történő optimális integrációja csak akkor valósulhat meg, ha teljes betekintést adunk mindennapi rutinunkba, szokásainkba.” [99]

A NIS2 irányelv és az új kiberbiztonsági törvény egyre nagyobb figyelmet fordítanak a kiber-fizikai rendszerekre, valamint az IoT eszközökre, amelyek a digitális infrastruktúra és a mindennapi élet szerves részévé váltak. A NIS2 irányelv kifejezetten előírja az IoT eszközök biztonságának biztosítását, és meghatározza a megfelelő védelmi intézkedéseket a hálózati és informatikai rendszerek sérülékenységeinek minimalizálása érdekében. A szabályozás célja, hogy a gyártók és szolgáltatók felelősséget vállaljanak az általuk kínált IoT termékek biztonságáért, és megelőzzék azok kihasználásából eredő kockázatokat. Ezzel együtt a szabályozási környezet fejlődése is folyamatos, mivel az IoT technológia gyorsan változik és új biztonsági fenyegetéseket hoz.

Hazai vonatkozásban 10/2024. (VIII. 8.) SZTFH rendelet az IoT-eszközök nemzeti kiberbiztonsági tanúsítási rendszeréről fogalmazza meg a kritériumokat, azaz célja az IoT eszközök biztonságának garantálása és a kiberfenyegetések ellenálló képességének növelése. A rendelet előírja, hogy a gyártóknak és forgalmazóknak az eszközeik biztonságát tanúsítaniuk

[127] https://www.sap.com/hungary/products/artificial-intelligence/what-is-iot.html

kell, és ezen tanúsítványok megszerzése alapvető követelmény lesz a piacra lépéshez. A tanúsítás során a kiberbiztonsági szempontokat, mint a sérülékenységek védelmét, a titkosítást és az adatvédelmet, szigorú szabályozás szerint ellenőrzik. Ezzel a rendelet segíti elő a biztonságosabb IoT ökoszisztéma kialakítását és az eszközök megbízhatóságának növelését.

A Findstack adatai szerint 2021-ben már 35.82 milliárd IoT-eszköz működik világszerte, 2025-re várhatóan már 38.6 milliárd ilyen eszköz lehet hálózatba kapcsolva, 2030-ra pedig ez a szám eléri majd az 30-50 milliárdot. [100] 2024-ben várhatóan körülbelül 17.08 milliárd IoT eszköz lesz összekapcsolva globálisan. [101]

A dolgok internetének alkalmazása és az általános adatvédelmi rendelet szembemehet egymással az adatvédelem és a biztonság tekintetében is. Az IoT-eszközök bevezetésekor kulcsfontosságúvá válik a GDPR-előírásoknak való teljes megfelelés biztosítása az eszközök által gyűjtött személyes adatok védelmének az érdekében. A szervezeteknek ma már alkalmazniuk kell az adattitkosítást, a felhasználói hozzájárulások meglétét, az adatok kezelésének (tárolásának) minimalizálását és az elvárható biztonságos adattárolást, annak érdekében, hogy az IoT eszközök alkalmazása a GDPR-követelményeknek megfeleljen.

Az IoT-eszközök alkalmazásának számos kiberbiztonsági/adatkezelési kockázati tényezője van.

Külön kockázati tényezőként kell figyelembe venni az értékelés során, hogy az eszközt ki és mikor, milyen biztonsági körülmények között használja. További kockázati tényezőként figyelembe kell venni a felhasználó életkorát, informatikai képzettségét, motivációját a felhasználás tekintetében. Az IoT eszközök kockázatértékelés során értékelni kell azt, hogy: – az eszköz milyen protokollokat és csatornákat használ a kommunikációhoz;

- az eszköz milyen fajta és mennyiségű szenzorokkal rendelkezik;
- az eszköz végez-e adattovábbításon kívül önmagában is adatfeldolgozást;
- az eszköz milyen személyes adatokat kezel tételesen;
- az eszköz milyen infokommunikációs szabványokat alkalmaz a kommunikációja során;
- az eszköz által használt szoftverek milyen műszaki irányelveket és EU-ajánlásokat vesz figyelembe az adattovábbítás során.

Ha részleteiben tekintjük, és fókuszba állítjuk a személyes adatokat akkor az IoT rendszerek jelentős kockázatokat rejtenek a személyes adatok védelme szempontjából. Ezek a tényezők a következők.

Az adatbiztonság vonatkozásában a gyenge jelszavak és hitelesítési módszerek kockázatot jelentenek, mivel számos IoT eszköz gyári beállításai miatt gyenge jelszavakkal rendelkezik, amelyek könnyen visszafejthetőek, valamint a titkosítás hiánya miatt az adatátvitel és -tárolás során használt gyenge vagy hiányzó titkosítás lehetővé teszi az illetéktelen felhasználók számára az adatok jogtalan megismerését. [102]

Adatgyűjtés és -tárolás szempontjából kockázatnak minősül a túlzott adatgyűjtés, mivel az IoT eszközök gyakran több adatot gyűjtenek, mint amennyi szükséges az alapvető funkcióik ellátásához. Emellett az adatmegőrzés és -tárolás szempontjából kockázat az, hogy a gyártók nem mindig biztosítanak megfelelő irányelveket az adatok tárolására és megőrzésére vonatkozóan, ami adatvesztéshez és visszaélésekhez vezethet.

Harmadik felekkel való megosztás kiemelt kockázat az IoT tekintetében, mivel az IoT eszközök által gyűjtött adatokat gyakran megosztják harmadik felekkel, reklámcégekkel vagy más szolgáltatókkal, anélkül, hogy a felhasználók tisztában lennének ezzel. Ebben az estben ismert jelenség az, amikor a felhasználó el sem olvassa a tájékoztató dokumentumokat, amit bizonyítottunk is a közvéleménykutatás során. Kérdőíves kutatásomban erre kitértem, ahol bebizonyítottam, hogy alapvetően a felhasználók túlnyomó többsége meg sem nézi ezeket a tájékoztatókat. [103]

További általános kockázati tényező a frissítések és javítások hiányossága. Számos IoT eszköz nem kap rendszeres szoftverfrissítéseket vagy biztonsági javításokat, így sebezhetővé válik.

Az egyik leggyakoribb tényező a gyártói támogatás hiánya, mivel sok IoT eszköz olcsóbb modellek, amelyeket gyorsan piacra dobnak, de a gyártók nem biztosítanak hosszú távú karbantartást és frissítéseket. Továbbá, sok esetben a gyártók nem rendelkeznek a szükséges erőforrásokkal vagy infrastruktúrával a rendszeres frissítések biztosításához.

Az elavult vagy nem támogatott IoT eszközök könnyű célpontok lehetnek a támadók számára. 2024-ben az IoT eszközök szoftverfrissítése változatlanul jelentős kiberbiztonsági kockázatot jelent. Megközelítőleg globálisan több milliárd IoT-eszköz van használatban, ezek közül egyes elemek nem kapnak rendszeres frissítéseket. Az elavult, támogatás nélküli IoT-eszközök aránya különösen magas, a becslések szerint több milliárd eszköz lehet sérülékeny a megfelelő

biztonsági frissítések hiánya miatt. [104] Egyes források azt állítják, hogy az IoT-eszközök egyharmada öt éven belül elavulttá válik, ami körülbelül 5,6 milliárd eszközt jelenthet. [105]

Az eszközökhöz történő fizikai hozzáférés lehetőséget biztosíthat a támadóknak, hogy közvetlenül beavatkozzanak az eszköz működésébe, vagy adatokat illetéktelenül megismerjenek, illetve az eszközök manipulációja során a támadók átprogramozhatják, vagy megváltoztathatják az eszközök üzemszerű működését annak érdekében, hogy adatokat szerezzenek meg.

3.9.1 Kockázatértékelés

Az IoT-ökoszisztéma általános problémáit az ENISA 2017-ben számba vette, a biztonsági szakembereknek, a gyártóknak–fejlesztőknek, és maguknak az érintetteknek szánt figyelmeztetésüket 2022-ben jelezték. [106]

Egy-egy rendszerbe integrált különböző gyártási idejű és gyártmányú eszközök műszaki tartalom alapján jelentősen különböznek, ez pedig megnehezítheti, vagy akár meg is akadályozza az elvárt szintű kommunikációt, valamint komoly biztonsági réseket okozhat.

Az IoT-eszközök és rendszerek biztonságának jelentős kockázati tényezője az is, hogy alacsony árszínvonalon tömeggyártásban is készülnek, és a költségtakarékosság miatt gyenge biztonsági megoldásokat tartalmaznak.

Ezek az eszközök rendszerbe integrálásukkal olyan komplex ökoszisztéma részévé válhatnak, amely jelentős mennyiségű adatot kezel, és amellyel szemben magas szintű bizalmassági, sértetlenségi és rendelkezésre állási követelmények vannak. [107]

Megállapítható, hogy az adatvédelemi követelményeket az IoT-rendszerek teljes életciklusában teljesíteni kell az eszközök/rendszerek tervezésétől egészen a gyártásig, működésbe állításon, használaton és szervizelésen át egészen az ökoszisztémából kivonásig és a leselejtezésig (megsemmisítésig).

Egyre gyakoribb a mesterséges intelligenciát alkalmazó eljárások beépítése is az IoT-eszközökbe. Ezek kiberbiztonsági kockázatokat jelentenek az összes eszköz tekintetében. Emellett további kockázati tényező a End-to-End titkosítás (E2E[128]), amely szintén az IoT eszközök életciklusán keresztül biztosítani kell a gyártónak. [108]

[128] E2E Encryption - Az adatokat a küldőtől a fogadóig titkosítva tartják, így azok közvetlenül a kommunikáló felek között védettek, és csak ők tudják dekódolni őket.

Az IoT-eszközök nagyon gyorsan igen széles spektrumon elterjedtek, a magánhasználattól a kereskedelmi és ipari alkalmazások mellett a létfontosságú infrastruktúrák és az intelligens infrastruktúrák terén is. Ez a probléma különösen jelen van olyan területeken, mint például a vasúti közlekedés, amely olyan nagy infrastruktúraigényű ágazat, amelyben az üzembiztonság egy pillanatra sem elhanyagolható szempont, illetve területileg szétszórt, különböző korú elemeket tartalmaz, amelyeket számtalan szereplő működtet(het), miközben a jegyárakban az új fejlesztések csak erősen korlátozott mértékben érvényesíthetőek.

A biztonsági szempontoknak fokozottan kell érvényesülniük az IoT ökoszisztémában, mivel a működtetők (kapcsolók) a fizikai világra hatnak. A fenyegetések számtalan emberéletet veszélyeztetnek (pl. ivóvízrendszer manipulálása, kőolajfinomító elleni szabotázsakció, vasúti szolgáltató ellen végrehajtott kibertámadások stb.).

A biztonsági integráció nehézkes az esetlegesen egymásnak ellentmondó szempontok és követelmények miatt, a biztonsági szakemberek számára komoly kihívást jelenthet a különböző hitelesítési megoldásokon alapuló IoT-eszközök és rendszerek integrálása, és ezen rendszerek interoperábilissá tétele.

3.9.2 IoT-ökoszisztéma kockázatai

Az IoT-környezetekben az eszköz olyan fizikai vagy virtuális tárgy, amely egyedileg azonosítható és integrálható a már meglévő kommunikációs hálózatokba, és amelynek mindenképpen képesnek kell lennie hálózaton keresztül adatcserére egy másik eszközzel vagy rendszerrel és/vagy felhőalapú szolgáltatással. Ezen eszközök nemcsak az adatcsere szempontjából fontosak a kockázatkezelés során, hanem amiatt is, hogy ma már ezek az eszközök lehetnek olyan komplex eszközök is, amelyek tárolják, és egyben feldolgozzák, vagy akár titkosít(hat)ják is az adatokat. Az IoT-ökoszisztéma fontos elemei az érzékelők is, mivel ezek szerves részét képezik annak a környezetnek, illetve azon környezet megfigyelésének, amelyben az IoT-rendszereket használjuk. [109]

3.9.3 Nemzetbiztonsági kockázatok

A GDPR adatvédelemre és adatbiztonságra vonatkozó szabályozásával foglalkozni kell akkor is, ha egy adott szervezetben jellemzően az Infotv. hatálya alá tartozó nemzetbiztonsági célú adatkezelés folyik, mivel nemzetbiztonsági kockázatot nemcsak az az adatkezelés hordozhat, amely a nemzetbiztonsági és honvédelmi adatkezelések nagy halmazába tartozik, hanem sok más, akár a GDPR hatálya alá tartozó adatkezelés is.

A GDPR adatvédelmi logikájának ismerete azért is fontos az IoT-eszközök nemzetbiztonsági kockázatkezelési célú vizsgálata során, mert ugyanazzal az eszközzel folytatott adatkezelés – az eszköz éppen aktuális felhasználásától függően – a GDPR és az Infotv. hatálya alá is tartozhat, valamint az egyértelműen a GDPR hatálya alá tartozó adatkezelésnek (illetve az adatkezelésre használt IoT-eszköznek, rendszernek) is lehet nemzetbiztonsági kockázata. Számos új IoT-eszköz rejt nemzetbiztonsági kockázatot a Virtual Voice Assisstant alkalmazásának köszönhetően, mivel az ezzel felszerelt eszközök akár távolról beindítható lehallgató funkcióval is üzemeltethetőek, miközben az adott tárgy tulajdonosa, illetve az eszköz hatókörében tartózkodó egyéb személyek (érintettek) nem biztos, hogy tudatában vannak annak, hogy lehallgatják őket.

A teljesség igénye nélkül a fokozottan kockázatos IoT-eszközök körébe sorolhatók például:

- otthoni munkavégzéshez szükséges technika (PC, laptop, tablet, telefon, okosóra, nyomtató, rajztábla stb.);
- az okos játékok (RC45 -járművek, okosbaba, okos játékkonyha, okos babaház, játékkonzolok stb.) polgári UAV -rendszerek (pld. klasszikus értelemben vett drónok);
- okos otthon eszközök („smart home”), ide számos alrendszer is tartozik, jellemzően ház automatizálási eszközökre kell gondolni. [110]

Összességében megállapítható, hogy a műszaki újítások megjelenése, illetve a már meglévő eljárásokban rejlő nemzetbiztonsági kockázatok, valamint a személyes adatok (pld. kép- és hangfelvétel) biometrikus adatokként felhasználása a hatályban lévő jogszabályok alapelveinek újra értelmezésére kényszeríti mind az Európai Unió Alapjogi Chartát[129] tiszteletben tartani kívánó adatkezelőket, mind a jog érvényesítésére törekvő felügyeleti hatóságokat és bíróságokat. A helyzetet tovább bonyolítja, hogy bizonyos személyes adatokkal kapcsolatos adatkezelések nem tartoznak a GDPR hatálya alá, így ezekben az esetekben a vonatkozó jogszabályok értelmezése a nemzeti hatóságok feladata, illetve bűnügyi adatok kezelése esetében a bűnügyi adatvédelmi irányelv hatálya alá tartozó adatkezelésekkel kapcsolatban az Európai Adatvédelmi Testület is bocsáthat ki iránymutatást és véleményt.

[129] Az Európai Unió Alapjogi Chartáját 2000-ben fogadták el, hogy biztosítsák az uniós polgárok alapvető jogait és szabadságait. A Charta célja, hogy jogi keretet adjon az uniós intézmények és tagállamok számára, amelyek kötelesek tiszteletben tartani és védelmezni az alapjogokat, beleértve a személyes adatok védelmét is. Charta hangsúlyozza a személyes adatok kezelésének átláthatóságát, a célhoz kötöttséget, és azt, hogy az adatok feldolgozása során tiszteletben kell tartani az egyén magánéletét és szabadságjogait.

Mivel az IoT eszközök száma és típusa egyre nő, valamint a rendszerek komplexitását folyamatosan változó tényezők alakítják, ezért megállapítható, hogy kockázatelemzésüknek folyamatos tevékenységgé kell válnia, épp úgy, ahogy az IoT rendszerek és alkalmazások fejlődnek, további új szempontok összetett rendszere merül fel, amit a meglévő megbízhatósági modellek és megoldások már nem tárgyalnak. Ennek következtében folyamatosan új megbízhatósági modelleket és megoldásokat kell fejleszteni. [111]

Napjainkban már a polgári térhódítás mellett az IoT honvédelmi ágazati megjelenését is meg kell vizsgálni, hiszen ebben a technológiában számos hadiipari vállalat is érintett. Ezek a vállalkozások jelentős erőforrásokat fordítanak arra, hogy az IoT-eszközökre épülő megoldások segítségével fejlesszék a gépi tanulást, illetve automatizálják a katonai döntéshozatali rendszereket. Az IoT katonai alkalmazásának lehetőségének vonatkozásában számos tudományos cikk készült, ezek alapvetően úgy értékelik, hogy az IoT-eszközök megjelenése elkerülhetetlen a haderőben. Kollár Csaba 2017-ben megjelent művében röviden összefoglalta azt, hogy „a hálózatos katona az utópisztikus távoli jövőből kézzelfogható távolságba, több területen pedig már a jelen valóságába került", 2021-ben pedig ez már nem utópia, hanem maga a valósággá vált koncepció. [112] A tanulmány alapvetően jól összefoglalja a fejlesztési irányokat, és foglalkozik az információbiztonság kérdéskörével is. Ugyanezt az elgondolást támasztja alá az is, hogy az IoT-eszközök közigazgatási alkalmazásával kapcsolatban már 2015-ben is születtek koncepciók, Haig Zsolt írásában, ahol megjelenik ez az elgondolás is, miszerint: „*A közigazgatási rendszerekben az ügyfélszolgálatok hatékonysága javítható, illetve az online ügyfélszolgálatok terén nyújthatnak plusz lehetőségeket az IoT-megoldások".* [113] A publikáció előre mutatóan meghatároz három olyan katonai területet, ahol az IoT eszközök alkalmazhatóak (logisztika, helyzetismeret, egészségügyi kiszolgálás).

Az ENISA javaslata szerint minden egyes IoT-környezet esetében kockázatértékelést kell végrehajtani, átvizsgálva a különböző eszközöket érintő fenyegetéseket, és meg kell határozni a valószínűsíthető támadási forgatókönyveket is. Az IoT-eszközök nemzetbiztonsági kockázatainak feltárása esetén a kockázat értékelése minden esetben egyedi mérlegelést igényel, azaz esetről-esetre egyedileg kell felmérni, van-e az adott eszközzel vagy rendszerrel kapcsolatban nemzetbiztonsági kockázat, és ha van, milyen intézkedésekkel lehet azt csökkenteni. Az általános értelemben vett IoT-eszközök többségének nemzetbiztonsági kockázata azonban abból adódik, hogy ki, mikor, hol és milyen céllal alkalmazza az említett eszközöket, valamint ki fér hozzá az az esetlegesen tárolt vagy feldolgozott adatokhoz, vagy esetleg a tulajdonos tudta nélkül hová kerül továbbításra az IoT által összegyűjtött adat.

Kiemelt nemzetbiztonsági kockázati tényező az olyan IoT-eszköz, amelyről a felhasználó nem rendelkezik megfelelő mennyiségű és minőségű adattal, azaz, hogy ez említett eszköz IoT. Egy okos gyermekjátéknak polgári környezetben nem értékelhető a nemzetbiztonsági kockázata. Ha ugyanez az eszköz egy katonai objektum parancsnokának gyermekéhez tartozik, akkor viszont akár kritikus is lehet ez a tényező, mivel bekerülhet az illetékes parancsnok munkakörnyezetébe.

Az okoseszközök nemzetbiztonsági kockázata függ attól, ki használja azt. Az eszköz nemzetbiztonsági kockázata nagyságrendekkel nagyobb akkor, ha szervezett bűnözésben érdekelt személyek használják kommunikációra fedést biztosító alkalmazások segítségével az adott eszközt, és máshogy kell értékelni akkor, ha egyetemisták beszélik meg rajta a következő csoportprojekt feladataikat az egyetemi oktatás során.

Ez a kockázat jelentősen csökkenthető abban az esetben, ha a hatóságok által feltörhető, a szervezett bűnözői csoport által viszont feltörhetetlennek hitt alkalmazásokon keresztül történik a bűnszervezet kommunikációja[130]. A használat helyszíne is nagyban befolyásolhatja a nemzetbiztonsági kockázat szintjét, más kockázattal bír egy internetre kötött kávéautomata egy polgári vállalkozásnál, és mással akkor, ha egy katonai objektum területén helyezkedik el.

Az okos rendszerek térhódításával az IoT-világ nemzetbiztonsági kockázata egyre nagyobb, az intelligens város, repülőtér, kikötő, vasút-, közút- és energiahálózat megjelenésével. Ezek stratégiai szerepe mind nemzeti, mind globális szinten jelentős, az összekapcsolódásuk és egymástól függésük egyre interdiszciplinárisabb problémákat okoz, az információbiztonság pedig egyben nemzetbiztonsági kérdés is lesz.

Kutatásom során cikkemben részleteiben kitértem még a IoMT- és IoBT-eszközökre is, valamint az IoT IPAR 4.0 (IIoT[131]) alkalmazásának kockázataira is. Az IIoT-rendszerek kockázatát tovább fokozza a beszállítói láncok összetettsége, az elemek kapcsolódása, és a lánc tagjainak eltérő biztonsági szintjei. Az ENISA külön dokumentumban tárgyalja az intelligens gyártást, amely során számos, korábban nem tapasztalt kockázatra hívja fel a figyelmet az IIoT rendszerekkel kapcsolatban. [114]

[130] Mint például az amerikai FBI „ANON" projektje, amikor világszerte több mint 300 bűnözői szindikátus tartóztattak le több mint 100 országban.

[131] Industrial IoT -Az IIoT eszközök és rendszerek képesek adatokat gyűjteni, feldolgozni és megosztani az ipari környezetekben, például gyártósorokon, energiatermelésben, vagy logisztikában, lehetővé téve a valós idejű monitorozást és optimalizálást. Az IIoT alkalmazások javíthatják az operatív hatékonyságot, csökkenthetik a költségeket, és segíthetnek a prediktív karbantartásban, miközben biztonságosabbá teszik az ipari működést.

Továbbá a kutatás során elemeztem az okos szolgáltatói rendszereket is. A szolgáltatások területén is megfigyelhető az IoT térhódítása. Ezen rendszerek problémái alapvetően hasonlóak az ipari rendszerek problémáihoz, azonban a kockázatok kitettségét fokozza, hogy napi szinten akár emberek millióival (felhasználókkal) is kapcsolatba kerülhetnek, rendkívül komplex adatstruktúrát generálva. Valamint tárgyaltam az otthoni IoT-rendszerek kockázatát is. Az IoT-rendszerek kockázatmenedzselése során semmiképpen sem szabad lebecsülni a privát hálózatok jelentőségét. Az otthoni IoT-ökoszisztémák nagy többsége – ellentétben a tudatosan tervezett hálózatokkal – véletlenszerűen beszerzett és egy hálózatba kapcsolt legkülönfélébb IoT eszközök strukturálatlan rendszere. Az „otthoni" eszközök képesek lehetnek távoli szolgáltatásokkal való interakciókra és adatcserére, beleértve a távoli aktiválást, a távoli tárolást vagy tartalomkezelést, az eszközadminisztrációt és az elemzést. Ezen kívül jellemző rájuk a mobilalkalmazásokkal történő interakciók és adatcserék vezérlési célokra és ezen eszközök közötti adatcserék megvalósítása. [115]

3.10 Felhő hálózatok

Kutatásom során a felhőszolgáltatások esetében megvizsgáltam, milyen követelményeket kell teljesíteniük a szereplőknek a GDPR-megfelelőség érdekében, illetve azt, hogy a GDPR milyen módon hatott a felhőszolgáltatók adatvédelmi gyakorlatára. A téma szerteágazó természete és komplexitása miatt a kutatás alapvetően a felhőtárhelyeken tárolt adatok kezelésének GDPR-megfelelőségét, valamint a felhőszolgáltatás (cloud computing) és a GDPR összefüggését vizsgálta.

A kutatás során esettanulmányokat és interjúkat, valamint elemzéseket is felhasználtam, amelyben a kezelt adatok felhőben történő tárolásának problémáit, valamint a jelenlegi felhőszolgáltatások általános problémáit tárgyaltam a GDPR vonatkozásában. Emellett jelentősebb felhőszolgáltatók adatkezelési tájékoztatóit elemezve értékeltük az ezekben a tájékoztatókban megfogalmazott garanciákat és biztosítékokat, illetve az esetlegesen felmerülő egyedi megoldásokat is. [116]

Napjainkra a felhőszolgáltatások nélkülözhetetlen részei lettek a globális digitális ökoszisztémának. A felhő alkalmassá vált már arra, hogy személyes adatainkat tárolja, továbbítsa vagy akár feldolgozza. IoT eszközeink is jellemzően ezt a szolgáltatást használják annak érdekében, hogy adatink bárhonnan hozzáférhetőek legyenek.

A GDPR jelentősége, hogy a felhőszolgáltatásokat az Európai Unió szintjén immáron egységesen szabályozza, illetve az EGT-tagállamokon kívüli harmadik országba adattovábbítást csak abban az esetben minősíti jogszerűnek, ha a harmadik országban az adatkezelő, illetve a megbízása alapján eljáró adatfeldolgozó, azaz a felhőszolgáltató az uniós védelemmel „egyenszilárdságú” védelmet biztosít.

A felhőszolgáltatásokat a tartalmuk alapján több csoportra kell felosztani. Lehet szoftver, mint szolgáltatás[132], vagy platform, mint szolgáltatás[133], infrastruktúra (kiszervezett kapacitás[134]) mint szolgáltatás, tárolás, mint szolgáltatás[135]. Emellett projekt (művelet vagy küldetés) szintjén is lehet már felhőszolgáltatásokat alkalmazni, például felhőalapú pilóta nélküli repülőrendszer (UAS) megvalósítása vonatkozásában. Ez utóbbi témában Vránics Dávid Ferenc és Palik

[132] A felhőszolgáltató a szoftvert nyújtja interneten keresztül („SaaS”).
[133] A felhőszolgáltató az alkalmazás üzemeltetéséhez szükséges környezetet biztosítja („PaaS”).
[134] A felhőszolgáltató az infrastruktúrát (virtuális gépet és más erőforrásokat) biztosítja, az operációs rendszert és az alkalmazásokat a felhasználó működteti („IaaS”).
[135] Storage as a Service (STaaS).

Mátyás készített egy összefoglaló művet, amelyben már a megvalósítás gyakorlati kérdéskörét is tárgyalják. [117]

Más rendszer alapján csoportosítva a felhőszolgáltatásokat feloszthatjuk publikus és privát felhőszolgáltatásra is.

A felhőszolgáltatások és a GDPR vonatkozásában is készült már tanulmány, amely részletesen tárgyalja a felhasználók adatainak felhőszolgáltatás alatti továbbítását. A tanulmányban nemcsak kizárólag az adatmozgatással kapcsolatos kérdéseket vizsgálták, hanem azt is, hogy a felhőszolgáltatásnak a GDPR alapján milyen kritériumoknak kell megfelelnie.

Az említett kutatás eredménye, hogy a felhőszolgáltatók változatlanul versenyképes termékeket kívánnak nyújtani ügyfeleiknek, akkor az adatok hordozhatóságához adatkezelőként és adatfeldolgozóként is teljesíteniük kell a GDPR követelményeit. Emellett valamilyen új követelmény teljesítése érdekében a szolgáltatásnak rugalmassá kell válnia. Mivel maga a tanulmány az adathordozhatóságot vizsgálja, így a cikk fókuszában a GDPR 20. cikke áll.[136]

A 95/46/EK európai parlamenti és tanácsi irányelv 29. cikke szerinti Adatvédelmi Munkacsoport 2012 júliusában elfogadott, 05/2012. sz. véleményében (WP 196) fektette le a felhőszolgáltatásokat érintő adatvédelmi elvárások főbb kritériumait. A felhőszolgáltató igénybe vevője és a felhőszolgáltatás biztosítójának kapcsolata alapvetően adatkezelő–adatfeldolgozó kapcsolat, amelyben a szolgáltatást igénybe vevő határozza meg az adatkezelés célját, és ő viseli a felelősséget is az adatkezelés tekintetében. [118]

A vélemény kiemelt fontossággal kezeli a felhőszolgáltatásokkal kapcsolatos kockázatokat, amely kockázatok többsége két kategóriába sorolhatók: egyrészt az adatok feletti ellenőrzés hiányából fakadnak, másrészt magával az adatkezelési műveletekkel kapcsolatos elégtelen információk (azaz az átláthatóság hiánya) miatt számottevőek.

Az átláthatóság hiánya azt eredményezheti, hogy az adatkezelők nincsenek tisztában azzal, hogy nem egy adatfeldolgozóval, hanem akár az adatfeldolgozók többszintű, egymásnak alárendelt láncolatával állnak szemben, és az sem mindig világos, az adatokat a világ mely pontján és milyen joghatóság alatt tárolják.

Kiemelendő, hogy a felhőszolgáltatást igénybe venni tervező szervezeteknek első lépésként átfogó és alapos kockázatelemzést kell végezniük, a szolgáltatóknak pedig minden olyan

[136] EU általános adatvédelmi rendelet: Az adathordozhatósághoz való jog. https://www.privacy-regulation.eu/hu/20.htm; letöltés: 2021.01.19.

információt rendelkezésre kell bocsátaniuk, amelyek segítségével ezt a kockázatelemzést el lehet végezni.

Az Adatvédelmi Munkacsoport szerint a szolgáltatást igénybe vevő csak úgy vehet igénybe felhőszolgáltatást, hogy annak igénybevétele előtt megfelelő kockázatelemzést végzett, amely kiterjedt az adatfeldolgozást végző szervezetek földrajzi helyére, az adatvédelmi kockázatok, valamint a szolgáltatás igénybevételéből fakadó előnyök elemzésére. A vélemény idézi a berlini Nemzetközi Távközlési Adatvédelmi Munkacsoport 2012 áprilisában elfogadott Sopoti Nyilatkozatát [119], amely kimondja, hogy a felhőszolgáltatás „nem eredményezheti az adatvédelmi normák csökkentését a hagyományos adatfeldolgozáshoz képest".

A kockázatértékeléshez az EU Kiberbiztonsági Ügynöksége (ENISA) 2009-ben megjelent kiadványa is segítséget ad a szervezetek számára. Emellett a kis- és középméretű vállalkozások (kkv) részére 2015-ben adtak ki hasonló iránymutatást segítségként a témában. [120]

A felhőszolgáltatók már a GDPR hatályba lépése előtt megkezdték a felkészülést a megfelelőségi szabályok teljesítése érdekében. Az európai felhőinfrastruktúra-szolgáltatók szakmai szövetsége, a CISPE[137] ezért kidolgozott egy magatartáskódexet, ahol szövetség minősíti, majd ellenőrzi a csatlakozó szolgáltatókat a kritériumok megvalósítását követően[138].

Az adatvédelmi hatóságok gyakran adnak ki tájékoztatókat különféle adatvédelmi témákban, az egyik ilyen a cloud computing, azaz a felhőszolgáltatás. Ezekben a kiadványokban segítséget nyújtanak a szakértelemmel nem rendelkező leendő felhőhasználóknak annak érdekében, hogy egyrészt tisztában legyenek azzal, mi is az a felhőszolgáltatás, és milyen kockázatokat kell felvállalniuk, ha ilyet kívánnak igénybe venni, másrészt a lehető legkörültekintőbben tudjanak választani a számukra elérhető szolgáltatók közül.

A brit hatóság 2012-ben olyan tájékoztató anyagot adott ki a felhőszolgáltatások témájában, amely mind a mai napig hasznos tanácsokat nyújt az érdeklődőknek a tekintetben, hogy hogyan válasszanak felhőszolgáltatót, és mit tegyenek annak érdekében, hogy csökkentsék a kockázatukat. [121]

Az ír hatóság a kiadványában a hangsúlyt a biztonságra, illetve az adatfeldolgozási megállapodásra helyezi, valamint azokra az alapelvekre, amelyek teljesítését a GDPR elvárja a felhőszolgáltatóktól, míg egy másik útmutatója a felhőszolgáltatások technikai kockázataira

[137] Az európai felhőinfrastruktúra-szolgáltatók szakmai szövetsége: Cloud Infrastructure Services Providers in Europe – CISPE
[138] A CISPE magatartási kódex verifikációját a szolgáltatók egy logóval jelezhetik.

hívja fel a figyelmet (adatvédelmi incidens, adatokhoz jogosulatlan hozzáférés, felhasználói fiókok „eltérítése”). [122]

Az Európai Bizottság 2020 februárjában tette közzé az adatokkal kapcsolatos stratégiáját. Az elgondolás szerint az európai „adatökoszisztéma” kereteit tovább kell fejleszteni és versenyképességé kell tenni, de kiemeli és hangsúlyozza az adatok védelmét is.

Részletezi a főbb problémákat és kihívásokat, ezek között pedig kiemelt szerepet kap az adatok hozzáférhetősége, a kiegyensúlyozatlanság a piacokon, az interoperabilitás hiánya, az adatok minőségével kapcsolatos problémák, valamint az EU jelenlegi technológiai függősége az amerikai és a kínai felhőszolgáltató óriásoktól.

A felhőszolgáltatók – annak ellenére, hogy feltehetően alapvetően teljesítik a GDPR adatkezelésre vonatkozó szabályait – az adatkezelési tájékoztatóikban (adatfeldolgozói kódexeikben, adatkezelési szabályzataikban) jellemzően bizalmi alapra építik a szerződő felek közötti adatkezelést, és így az adatok törlését is.

A kutatás során Magyarországon üzemelő tíz nagyobb felhőszolgáltató adatkezelési tájékoztatóját vizsgáltam.

Megállapításom szerint a vizsgált adatvédelmi tájékoztatók alapvetően tartalmazzák a GDPR ide vonatkozó pontjait (érintetti jogok felsorolása, adattovábbítás garanciái stb.), illetve tökéletesen idézik a GDPR definíciótárát is. Általános probléma, hogy a tájékoztatók keverik a GDPR, illetve az Infotv. rendelkezéseit, valamint nem követték le a GDPR bevezetése utáni hazai korrekciós jogszabály-módosításokat.

Kockázatként értékelhető az, hogy a szervezetek csak egyes esetekben azonosítják be saját szerepkörüket (mikor adatkezelők és mikor adatfeldolgozók, illetve amennyiben ez utóbbiak, akkor milyen felelősségeik vannak), valamint az általuk igénybe vett adatfeldolgozók és adatfeldolgozó alvállalkozók tekintetében sem biztosítják a megfelelő minőségű és mennyiségű információt az érintettek számára, miközben ez létfontosságú lenne a szolgáltatások igénybe vevőinek bizalma megszerzéséhez, illetve megtartásához.

Ezekben az példákban a szolgáltató hanyagul kezeli a GDPR 13. és 14. cikkeiben foglalt tájékoztatási kötelezettséget, amely szerint az érintett rendelkezésére kell bocsátani – többek között és adott esetben – a személyes adatok címzettjeit, illetve a címzettek kategóriáit, ha van ilyen.

Harmadik országba történő adattovábbítás jelentős kockázattal bír. Megemlítése leggyakrabban a domain regisztrációjával kapcsolatban merül fel. Amennyiben a regisztráció nem EGT tagállam területén történik, illetve van olyan szolgáltató is, amelyik bevállalja a nemzetközi adattovábbítást úgy, hogy garanciaként általános adatvédelmi kikötéseket, illetve adatfeldolgozói megállapodást jelöl meg, az érintettek számára ismeretlen mozaikszavakkal (SSC[139] + DPA[140]). A hanyag tájékoztatás jellemző példája, ha a szolgáltató ugyan ad meg cégneveket az adattovábbítással kapcsolatban, de Magyarországot, Romániát és Csehországot is a GDPR szempontjából harmadik országok közé sorolja.

Az adatbiztonság vonatkozásában a felhőszolgáltatók felületes és igen általános jellegű műszaki információkat közölnek a tájékoztatóikban arról, hogy az adatokat mily módon védik, valamint milyen módszerrel törlik, illetve anonimizálják szükség szerint.

Elmondható, hogy a tájékoztatás leginkább adatvédelmi szabályok és garanciák általános jellegű közlésében merül ki.

A felhőszolgáltatásokhoz köthető adatkezelési tájékoztatókban érintve megjelenik a felhasználók lehetősége arra, hogy személyes adataik vonatkozásában saját maguk járjanak el. Ilyen szolgáltatás például a webmail is, vagyis a webmail szolgáltatással a megrendelő, aki egyben az érintett is, közvetlenül menedzselheti e-mail fiókját és beállításait.

A GDPR további hatása az, hogy az egyes felhő szolgáltatók a saját belső audit mellett igénybe vesznek külső auditszolgáltatást is. Így végeztethet független auditot, amelynek az eredményét nyilvánosságra hozza, ezzel növelve a szolgáltatás kiberbiztonságát.

A GDPR-megfelelőség sok felhőszolgáltató esetében az IT rendszerekben korábban elhanyagolt fejlesztéseket kényszerített ki, amelyek során esetleges sérülékenységeket is kijavíthattak, vagy legalábbis csökkenthettek.

A GDPR tekintetében megállapítható, hogy a rendelet hatályba lépésétől a felhő szolgáltatók várhatóan több forrást fognak ráfordítani a törlést és az anonimizálást végrehajtó speciális célszoftverekre. Az interjúk és az adatkezelési nyilatkozatok elemzése és értékelése során megállapítottuk, hogy ezek a tájékoztatók még jelenleg is hiányosak vagy elnagyoltak.

[139] Szabványos Szerződéses Kötelmek - Standard Contractual Clauses: Az SSC-k az Európai Unió adatvédelmi szabályozásainak (például a GDPR) keretében használt előre meghatározott szerződéses feltételek, amelyeket adatkezelők és adatfeldolgozók alkalmaznak.

[140] Adatfeldolgozási Megállapodás – Data Processing Agreement: A DPA egy jogi megállapodás, amelyet az adatkezelő és az adatfeldolgozó között kötnek, és amely meghatározza az adatfeldolgozás feltételeit, a felelősségeket és az adatvédelemhez kapcsolódó előírásokat.

Emellett közös jellemzőik, hogy laikus felhasználók vagy ügyfelek részére nehezen olvashatók vagy értelmezhetők, bár a GDPR meghatározza, hogy a tájékoztatóknak közérthetőknek kell lenniük.

A felhőhálózatokban tárolt személyes adatok védelmével kapcsolatban számos kockázat merül fel, főleg hogy a felhőszolgáltatások használata tovább növekszik. Adatbiztonsági sérülékenységek tekintetében elmondható, hogy az adatok titkosítása az átvitel során kritikus, mivel az érzékeny adatok megfigyelésre kerülhetnek, ha nem megfelelően vannak titkosítva.

A felhő szolgáltatások alkalmazásai nem minden esetben biztonságosak, ennek tükrében illetéktelen felhasználók könnyen kihasználhatják a réseket, hogy hozzáférjenek a személyes adatokhoz. [123]

Alapvetően, ha már az adatokra nincs szükség, akkor véglegesen törölni kell azokat. viszont az adathordozó fizikai jellemzői miatt a törölt adatok továbbra is létezhetnek, és visszaállíthatóak maradnak. Ez azzal a kockázattal járhat, hogy illetéktelen személyek is visszaállíthatják ezeket a személyes adatokat. [124] [125]

Az adatvédelmi jogszabályok, mint a GDPR szigorúan szabályozza a személyes adatok kezelését és tárolását. A jogszabályok megsértése súlyos pénzbírságokat és jogi következményeket vonhat maga után.

A felhőszolgáltatásokban bekövetkező adatvesztés, függetlenül attól, hogy az műszaki meghibásodás vagy támadás következménye, jelentős adatvesztést eredményezhet. A biztonsági mentések és az adatok helyreállítása nem mindig megfelelően van megtervezve és végrehajtva, ami tovább növeli az adatvesztés kockázatát.

A felhőszolgáltatók megbízhatósága és pénzügyi stabilitása szintén kockázatot jelenthet, különösen, ha a szolgáltató megszűnik vagy szolgáltatásai leállnak. A felhőszolgáltatók által elszenvedett biztonsági incidensek, mint például a DDoS támadások vagy más támadások, befolyásolhatják a szolgáltatás rendelkezésre állását és az adatok biztonságát.

A személyes adatok védelme érdekében a felhőszolgáltatások használatakor kiemelten fontos a megfelelő biztonsági gyakorlatok alkalmazása, beleértve az adatvédelmi irányelvek betartását, a titkosítás alkalmazását, a hozzáférés szigorú ellenőrzését, valamint a rendszeres biztonsági auditok és sebezhetőségi vizsgálatok elvégzését.

3.10.1 Kockázatértékelés

Álláspontom szerint a legnagyobb kockázatot az jelenti a felhő technológiában, ha elosztott/több-szolgáltató alapú felhő alkalmazást veszünk igénybe, mivel ebben az esetben személyes adataink töredékei, részei teljesen kikerülnek az irányításunk alól. Természetesen a probléma feloldására már vannak kísérletek és megoldások, mint például az elosztott/több-szolgáltatós modellnél az Redundant Residue Number System (RRNS) megoldás használata. [126]

A kérdőíves kutatás során megállapítottam, hogy maguk a felhasználók is csak a jogszabályok maradéktalan betartásában bíznak, a gyakorlatban viszont nem rendelkeznek irányítással személyes adataik felett a felhőszolgáltatóknál. Emellett a GDPR-nak nyilván van áttételes hatása az adatszivárgások vonatkozásában, mivel az érvényesíthető büntetések mértéke jelentősen növelte az üzemeltetési kockázatokból származó potenciális költségeket.

3.11 Generatív mesterséges intelligencia

Kutatásom során vizsgáltam a terrorizmus és a személyes adatok illegális felhasználásának kapcsolatát, különös tekintettel a digitális világ nyújtotta lehetőség vonatkozásában. Az eltulajdonított személyes adatok nemcsak a terrorszervezetek álcázását, toborzását és pénzmosási tevékenységeit segítik, hanem alapul szolgálnak célzott propagandakampányokhoz is. Megvizsgáltam, és mértem, hogy a mesterséges intelligenciával készített, közösségi médiában terjedő propagandavideók és manipulált tartalmak jelentős mértékben fokozzák a radikalizáció kockázatát. A kutatás részletezi a közösségi média platformok és a modern technológiák szerepét az ilyen anyagok terjesztésében, hangsúlyozza a nemzetközi együttműködés és az adatvédelem megerősítésének fontosságát, mint a terrorizmus és a digitális fenyegetések elleni küzdelem kulcsfontosságú eszközeit.

A terrorizmus eszköztárában a közösségi média platformokon keresztül történő MI-alapú propaganda terjesztése, radikalizáció és toborzás válik egyre hangsúlyosabbá napjainkra. Emellett ezek a platformok lehetőséget biztosítanak a terrorista csoportok számára a támadások célzott koordinálására, hiszen az anonimitás és a könnyű hozzáférhetőség decentralizált, nehezen nyomon követhető működést tesz lehetővé számukra. [127]

A kutatás során megállapítottam, hogy a közösségi média algoritmusai is elősegíthetik az extrém tartalmak terjedését. Így a közösségi média egy olyan információs térként jelenik meg, ahol a terrorista és a terrorizmus elleni erőfeszítések során egyaránt személyes adatokat használnak fel a felhasználók.

Empirikus kutatásom – felmérések és interjúk révén – azt vizsgálta, hogyan értékelik a nemzetbiztonsági, rendészeti és civil szervezetek a terroristák által használt MI eszközöket. Az eredmények arra utalnak, hogy az MI és a személyes adatok integrációja drasztikusan növeli a propaganda tevékenységek hatékonyságát.

Különösen a generatív MI alkalmazása teszi lehetővé a terrorista szervezetek számára, hogy új, vonzó, ugyanakkor gyakran hamis tartalmak előállításával bővítsék szervezetük elérését vagy kapcsolati hálózatát és méretét. Ezen fejlemények fényében a terrorista képességek növekedésével szembeni fellépés – különösen a NATO számára – kiemelkedően jelentős kihívást jelent a nemzetközi biztonsági közösség számára.

Az információs terrorizmus[141] a gyors digitalizáció hatására a digitális ökoszisztéma teljes spektrumára kiterjed, ahol az összekapcsolt rendszerek és eszközök kölcsönösen függenek egymástól. Az elmúlt évtizedben a terrorista szervezetek kibővítették eszköztárukat azzal, hogy a mesterséges intelligencia (MI) előnyeit kihasználva nemcsak komplex kibertámadásokat hajtanak végre, hanem adathalász/phishing módszereket és zsarolóvírust/ransomwaret is alkalmaznak érzékeny adatok – többek között személyes információk – megszerzésére. [128] [129]

Ezen túlmenően az MI segítségével generált valósághű képek, videók és szövegek révén hatékony dezinformációs kampányokat folytatnak, amelyek pánikot kelthetnek a digitális térben és a valóságban egyaránt. A terrorista tevékenységek kiterjednek a személyes adatok nagymértékű gyűjtésére is, melyek támogatják a toborzást, a koordinált műveleteket és a dezinformációs tevékenységeket, így növelve a kiberbiztonsági kockázatokat. [130] [131]

A kutatás interjúk, kérdőívek, irodalomkutatás és releváns kortárs források integrált alkalmazásával készült, és a terrorista információs műveletek műveleti-képességére vizsgálatára irányult. Az interjúalanyok olyan szakemberek voltak, akik információs műveletek, kibervédelem, elektronikus hadviselés és kapcsolódó biztonságpolitikai területeken szereztek tapasztalatot, míg a webes kérdőívek a bűnüldözés, a terrorizmus elleni küzdelem, valamint technikai és tudományos szakterületek képviselőit érintették. Emellett egyes szervezetek jogi, adatvédelmi és MI kérdésekben szolgáltattak információkat.

A kutatás kizárólag a generatív MI-re fókuszál, kizárva más MI-technológiákat[142]. A generatív MI egyedi kockázatai – elsősorban az új, tanult adatok alapján történő, potenciálisan hiteltelen tartalomgenerálás – indokolják a fókusz kizárólagosságát.

A kutatás eredményei azt mutatják, hogy az extremista szervezetek egyre nagyobb mértékben élnek a mesterséges intelligencia által nyújtott szolgáltatásokkal. Bár jelenleg elsősorban kereskedelmi úton elérhető technológiákra támaszkodnak, az MI technológia elterjedésével és költségeinek csökkenésével várhatóan képesek lesznek saját modellek fejlesztésére és betanítására.

[141] Az információs terrorizmus olyan tevékenység, amely az egyéneket vagy csoportokat szándékosan manipulálják. Alapvetően torzítják vagy meghamisítják az információt politikai, ideológiai vagy katonai célok elérése érdekében. Az információs terrorizmus célja lehet egy társadalom vagy társadalmi réteg megfélemlítése, a közvélemény befolyásolása, az alkotmányos rend megbontása, illetve a gazdasági vagy politikai instabilitás előidézése.

[142] Például szakértői rendszerek, gépi tanulás, mélytanulás, természetes nyelvfeldolgozás stb.

Az MI alkalmazásából eredő legnagyobb fenyegetést a dezinformáció jelenti, melyet a toborzás és a radikalizáció követ, mivel ezen tevékenységek során viszonylag egyszerű propaganda- és toborzó anyagok állíthatók elő. A Facebook és a YouTube jellegű közösségi média platformok kulcsfontosságú csatornákká váltak a terrorista tevékenységek terjesztésében, bár ezek a platformok intézkedéseket is hoznak az extremisták felhasználásának korlátozására, a felhasználók számára gyakran nehézséget okoz az extrém propagandatermékek felismerése. Mivel a terrorista MI-modellek alkalmazásának jellemzői és alkalmazási területeinek részletei jelenleg nem teljesen ismertek, az MI technológiát olyan módon is használhatják, amely a rendvédelmi szervek számára nehezen észlelhetővé teszi a jogellenes tevékenységeket – noha az adatok kezelése már önmagában is törvénytelen tevékenység. Mivel az MI-modellek kereskedelmi forgalomban elérhetőek, az extremista csoportok gyakran jogszerűen férhetnek hozzájuk, még akkor is, ha céljaik illegálisak. Ezért további intézkedések szükségesek a megfelelő felügyelet és végrehajtás biztosítása, valamint a EU-n kívüli szabályozások és védelmi rendszerek egységesítése érdekében. [132]

Kutatásom szerint a mesterséges intelligencia segítheti a szélsőséges szervezeteket propagandájuk hatékonyabb és gyorsabb terjesztésében. Az automatizált rendszerek nagy mennyiségű anyagot tudnak előállítani és célzottan terjeszteni a közösségi média platformokon, így növelve ezek hatását.

Az általános személyes adatokat tartalmazó adatbázisok már tartalmazzák például a felhasználók felekezeti, vallási beállítottságát, lakóhelyét vagy korábbi lakóhelyét, származási helyét (születési helyét), a család származási helyét, valamint korábbi tanulmányait vagy speciális tanfolyamait, amelyek eredményeként a botnetek célzottan tudnak szélsőséges tartalmú propagandaanyagokat eljuttatni.

A mesterséges intelligencia segítségével viszonylag könnyen és gyorsan lehet nyíltan hozzáférhető személyes adatokat gyűjteni a nyílt internetről. A szélsőséges szervezetek azonban illegális úton is hozzájuthatnak adatokhoz, ha a sötét webről vásárolnak már meglévő adatbázisokat, vagy információt gyűjtenek olyan pszichológiai manipulációs módszerekkel, mint például az adathalászat.

A mesterséges intelligencia segítségével létrehozott hamis profilok lehetővé teszik a terroristák számára, hogy hamis digitális személyeket készítsenek, ami megkönnyíti számukra a közösségekbe való beilleszkedést, ideológiájuk terjesztését és új tagok toborzását, vagy akár információszerzést is. Ezek a profilok annyira meggyőzőek lehetnek, hogy nehéz

megkülönböztetni őket a valódi felhasználók profiljaitól. Természetesen az alkotók valós személyes adatokat használnak fel egyes hamis profilokhoz, ezzel is felgyorsítva a folyamatot. Erre jó példa egy esettanulmány. A tanulmány szerint „2019-ben mesterséges intelligencia által generált profilképet használtak egy LinkedIn-fiókban Katie Jones néven. A harmincas éveiben járó fiatal szakember, Katie profilja azt mutatta, hogy egy washingtoni székhelyű vállalatnál dolgozott, és számos amerikai kormányzati szervezettel állt munkakapcsolatban.” A fent említett eset jó példa arra, hogy bizonyos esetekben az ilyen hamis profilok segítségével információkat lehet kinyerni a kormányzati szektorban dolgozóktól, hiszen a hamis profil ezekkel munkakapcsolatban volt. [133]

Ezek a profilok még online üzenetküldő alkalmazásokhoz és közösségi média szolgáltatásokhoz is alkalmasak lehetnek abból a célból, hogy célzott interakciókat folytassanak a kormányzati szektorban dolgozó, potenciálisan érzékeny információkhoz hozzáférő személyekkel. Az álprofil és a pszichológiai manipulációs eszközök segítségével közel kerülnek ahhoz a célponthoz, akitől információt szereznek. Ennek következtében huzamosabb ideig képesek rejtve maradni és információt szerezni.

Emellett további probléma, hogy az ilyen profilokat használó személyek vagy csoportok nem azonosíthatók a hamis profil miatt, vagy legalábbis erre jelentős kapacitásokat kellene fordítani.

A szélsőséges csoportok a mesterséges intelligencia segítségével olyan tartalmat generálhatnak, amely megszólítja célközönségük érzelmeit, elfogultságait és sérelmeit, hatékonyabban terjesztve ideológiájukat.

Amellett, hogy hatékonyabb, a propaganda mesterséges intelligenciával történő terjesztése is sokkal gyorsabban működik, mint a hagyományos módszerek. Az MI által készített célzott propagandaanyagok terjesztése bérelt botnet segítségével még hatékonyabbá teszi a szélsőséges szervezet tevékenységét. A propagandaanyagok eljuttatása akkor a leghatékonyabb, ha az anyagok a megfelelő célközönséget érik el. A digitális nyersanyagok (adatok), például a személyes adatok elengedhetetlenek a hatékony működésükhöz. Ennek eredményeként a botneteknek ismerniük kell bizonyos adatokat a célpontról ahhoz, hogy a dezinformációkat még pontosabban terjeszthessék.

Ilyen, kiemelten fontos adat például a név és e-mail cím, mivel a címzettek és a célközönség nagyobb valószínűséggel válaszol azokra az üzenetekre, amelyek személyes felhívást vagy releváns információkat tartalmaznak. A név használata hitelességet biztosít a küldőnek, így egy adott propaganda több emberhez eljuthat, és növelheti az elkötelezettséget.

A botnetnek tudnia kell, hogy kit célozzon meg például érdeklődés vagy hovatartozás alapján. A korábban e-mail címek vagy egyéb adatok alapján gyűjtött információk felhasználásával a botnetek pontosabban megcélozhatják a megfelelő demográfiai csoportot, legyen szó életkorról, érdeklődési körről, földrajzi elhelyezkedésről vagy vallási hovatartozásról.

A botnet könnyedén továbbíthatja az üzeneteket a célpont kapcsolattartóinak is, vagy kihasználhatja az áldozat kapcsolati hálózatát, hogy megsokszorozza a terjesztés hatékonyságát.

Annak érdekében, hogy hipotézisemet többszörösen alátámasszam, polgári vállalkozással (adatvédelmi tanácsadó), valamint adatvédelmi egyesületekkel[143] is interjút készítettem, abból a célból, hogy felmérjem ezek az entitások miket azonosítanak kockázatoknak a szélsőséges szervezetek tekintetében.

Annak érdekében, hogy még hangsúlyosabbá tegyem a kutatási témát, és bemutassam a kockázatot, kérdőíves kutatást végeztem. A kérdőíves kutatás célja az volt, hogy pontosabb képet alkossak mesterséges intelligencia fenyegetettségéről, és felmérjem a jelenlegi fenyegetés hatókörét. A kérdések között szerepelt, hogy az egyének találkoztak-e mesterséges intelligencia által előállított tartalommal, és hogyan érzékelik az adott tartalomhoz kapcsolódó kockázatokat.

Valamint elvégeztem a téma SWOT analízisét, aminek célja az volt, hogy kontextusba tegyem az MI és a személyes adatok felhasználásának lehetőségeit. A SWOT elemzéshez az interjúk anyagait is felhasználtam a saját véleményem alátámasztása érdekében.

Annak érdekében, hogy erről pontos képet kapjak a következő kérdésekre kerestem a választ:

• Milyen célokra használhatják fel a szélsőséges szervezetek az illegálisan megszerzett személyes adatokat?

Az interjúalanyok által felvetett kockázati tényezők (gyakorlati tapasztalatuk szerint) a következők voltak összefoglalva.

• Egyre több személyes adat érhető el legálisan a nyílt interneten, és könnyen hozzájuthatnak ellenérdekeltségű szereplők.

• A személyes adatok a pszichológiai manipuláció segítségével is könnyen megszerezhetők.

[143] MILTE és ASZAKE

• A kormányoknak és a vállalkozásoknak jobban együtt kell működniük a kiberbiztonság terén. Bár az olyan szervezetek, mint az EU Kiberbiztonsági Ügynöksége, számtalan iránymutatást adtak ki a kiberbiztonsággal kapcsolatban, meg kell találniuk a módját a kibervédelmi tevékenység nyomon követésének a támadások észlelése és megelőzése érdekében.

• A nagy, multinacionális cégek különösen kiszolgáltatottak, mivel nem megfelelő kiberbiztonsági gyakorlattal rendelkező vállalkozókra, alvállalkozókra támaszkodnak. Az a tény, hogy ezek az alvállalkozók olyan országokban tevékenykedhetnek, amelyek nem rendelkeznek az EU-val egységes védelemmel, sebezhetőséget okoz magánál az anyaszervezetnél is.

• A kormányzat és a vállalatok kulcsfontosságú és vezető beosztású embereinek gondoskodniuk kell a megfelelő kibervédelmi szabályzásról otthon és a munkahelyükön egyaránt. Ellenkező esetben sebezhetővé válhatnak az internethez csatlakoztatott készülékek vagy egyéb otthoni eszközök használata miatt, amelyek személyes adatokat gyűjthetnek, amelyek segítségével érzékeny rendszerekhez hozzáférhetnek.

• Az olyan szervezetek, mint a magyar Mesterséges Intelligencia és Legal Tech Egyesület és az Adatvédelmi Szakmai Egyesület aggodalmuknak adtak hangot amiatt, hogy a terrorista és bűnszervezetek zsaroló vírusokat és egyéb kibereszközöket használhatnak forrásszerzésre.

• A nagy mennyiségű legálisan elérhető adat és mesterséges intelligencia-algoritmus alkalmazásának kombinációja lehetővé teszi a bűnözői és szélsőséges szervezetek számára, hogy profilalkotást és más hírszerzési jellegű tevékenységeket végezzenek, amelyek exponenciálisan növelik illegális képességeiket.

• A legálisan és illegálisan megszerzett egészségügyi és genetikai adatok rosszindulatú felhasználása – például biológiai fegyverek előállítására – komoly problémát jelenthet.

A megkérdezett szervezetek a következő tevékenységeket sorolták fel a szervezetük számára kiemelten kockázatos tevékenységek közé.

• pénzügyi visszaélések

• célzott dezinformáció

• tartalom hamisítás és „deepfake”

• társadalmi manipuláció, adathalászat, az egyéni és szervezeti sebezhetőségek azonosítása és a megcélzott személyek profilja

• személyazonosság-lopás, például közösségi média fiókok megszerzése vagy másolása a célzott terjesztés érdekében, a közösségi médiában olyan sebezhetőségek felkutatása, amelyek lehetővé teszik a szélsőségesek megcélzását

• prediktív profilalkotás, amely előre jelezheti a jövőbeli cselekvéseket.

A megkérdezett szervezetek úgy vélték, hogy a hálózat- és információbiztonsági irányelv, amely az EU kibervédelmi keretrendszere, előrelépést jelent a kiberbiztonság terén, de hatékony felügyeletre és végrehajtásra van szükség ahhoz, hogy eredményes legyen.

A NIS1 irányelv arra kötelezi a szervezeteket, hogy egységes védelmet nyújtsanak a teljes ellátási láncban. A végrehajtás sebességét és irányát következetlennek ítélték meg. A megvalósítást közoktatási programoknak kell kísérniük az internet és a nem EU-konform országokból rendelt dolgok internete eszközeinek felelős használatára, valamint a nem EU-konform mesterséges intelligencia rendszerek felelős használatára vonatkozóan.

3.11.1 Kockázatértékelés

A szélsőséges szerveztek a rendelkezésre álló képességekkel várhatóan képesek lesznek saját MI modelljeik fejlesztésére és betanítására, amint az MI technológia mindenütt elterjedtebbé és ennek következtében olcsóbbá válik.

A terroristák mesterséges intelligencia-használatának legnagyobb azonosított kockázata a dezinformációs műveletek, amelyet a toborzás és a radikalizálódás követ. Mindkét tevékenység esetében viszonylag egyszerű a propaganda és a toborzás MI segítségével. Az olyan népszerű közösségi médiaplatformok, mint a Facebook és a YouTube, a terrorista tevékenység kulcsfontosságú csatornái. Bár ezek a platformok intézkedéseket tesznek a szélsőséges használat visszaszorítására, a felhasználók gyakran arról számolnak be, hogy nehézségeik vannak a szélsőséges propagandaanyagok megkülönböztetésében vagy felismerésében.

Mivel a terroristák mesterséges intelligencia-modellek használatának jelei/nyomai kevéssé ismertek, a csoportok olyan módon használhatják az MI-technológiát, amelyet a bűnüldöző szervek nehezen észlelhetnek. A mesterséges intelligencia modellek kereskedelmi forgalomban kaphatók, ezért a szélsőségesek gyakran legálisan hozzáférhetnek hozzájuk, még akkor is, ha céljaik illegálisak.

Az MI esetében mindig meg kell vizsgálni az adatkezelés jogalapját, valamint a tájékoztatást és átláthatóságot[144] is. Ezek figyelembevételével a következő kockázati tényezők azonosíthatóak az adatkezelők esetében:

• megfelelő adatkezelési jogalap hiánya (a GDPR 6. cikk (1) bekezdés b) pontja szerinti szerződéses jogalapot nem találta megfelelőnek a hatóság);

• átláthatóság, tájékoztatás hiányosságai;

• átláthatósági és az érintetti jogokkal kapcsolatos követelmények sérülése (a GDPR 12. cikk, 13. cikk, 14. cikk, 15. cikk stb.);

• életkori szűrés nem volt biztosított;

• megfelelő jogalap hiánya (GDPR 6. cikk);

• különleges adatok kezelésére vonatkozó rendelkezések sérelme (GDPR 9. cikk);

• EU-n belüli képviselő kijelölésének elmaradása (GDPR 27. cikk);

• hatósággal való együttműködés hiánya (GDPR 31. cikk);

• a beépített és alapértelmezett adatvédelem elvei nem érvényesültek megfelelően,

• adatbiztonsági hiányosságok, illetve a megfelelő technikai és szervezési intézkedések elmaradása;

• érintetti joggyakorlással, beleértve az automatizált döntéshozatallal kapcsolatos jogokat (GDPR 22. cikk), kapcsolatos követelmények sérelme;

• adatvédelmi hatásvizsgálat hiánya.

Ahogy előzőleg említettem, egyes MI-algoritmusok, különösen a mély tanulási modellek „fekete dobozként” működnek, megnehezítve döntéshozatali folyamataik megértését. Ennek következtében felmerül az átláthatóság teljes hiánya, ami automatikusan bizalmatlansághoz vezethet, valamint akadályozza az elszámoltathatóságot.

További kockázat lehet a munkahelykiszorítás, mivel a mesterséges intelligencia és az automatizálási technológiák módosítják a munkaerőpiaci helyzetet, az MI különféle iparágakban helyettesítik az emberi munkaerőt, ami munkahelyek kiszorításához és gazdasági

[144] A fejlesztő is „blackbox” technológiaként értékesíti egyes esetekben.

egyenlőtlenséghez vezethet, különösen kezdetben igaz ez az alacsony képzettséget igénylő munkakörökben.

Emellett további adatvédelmi aggályok merülnek fel mivel a mesterséges intelligencia rendszerek gyakran hatalmas mennyiségű személyes adatra támaszkodnak a hatékony működésükhöz és a tanuláshoz is. Ez viszont így kockázatként merül fel a magánélet megsértésével és az érzékeny információkhoz való jogosulatlan hozzáféréssel kapcsolatban, különösen az MI-képességek folyamatos fejlődése miatt. Ilyen például az adatfüggőség kérdése. A mesterséges intelligencia rendszereknek nagy mennyiségű kiváló minőségű adatra van szükségük a hatékony működéshez. A korlátozott vagy szubjektív döntések következtében tárolt adatok szuboptimális teljesítményt és pontatlan előrejelzéseket eredményezhetnek, ami korlátozza az MI-alkalmazások megbízhatóságát és hasznosságát. A környezeti károsítást is figyelembe kell venni napjainkban.

3.12 Kiberbiztonsági stratégiák

Kutatásom során több esetben vizsgáltam, hogyan épül be a személyes adatok védelme a nemzeti kiberbiztonsági stratégiákba és nemzeti dokumentumokba. A vizsgálat kiterjedt a 2021 és 2023 között közzétett stratégiákra annak érdekében, hogy részletes elemzéssel bemutassam a személyes adatok védelme és ezen stratégiai dokumentumok közötti kapcsolatokat. [134]

Kutatásom a kibervédelmi tervezés fejlődését is nyomon követte, megjegyezve, hogy a stratégiai dokumentumok gyakran képviselik a nemzeti kiberbiztonsággal kapcsolatos koncepcionális gondolkodás legmagasabb szintjét egy vizsgált országban. Fontos kiemelni, hogy 2022-2023 között az izlandi, román, olasz és dán kormány is kiadott egy új nemzeti kiberbiztonsági stratégiát. Illetve az Amerikai Egyesült Államok Védelmi Minisztériuma is kiadta a „2023 Department of Defense Cyber Strategy”-t a vizsgált időszakban.

Az Európai Unió kiberfenyegetésekre való reagálással kapcsolatos hosszú távú elgondolásával kapcsolatosan érdekesség, hogy az EU első biztonsági stratégiája 2003-ban még nem említette közvetlenül a kiberfenyegetéseket, viszont a kérdés fokozatosan egyre nagyobb hangsúlyt kapott, ahogy a digitális ökoszisztéma egyre jobban elterjedt globálisan. Az Európai Bizottság 2010-ben meghirdetett Európa 2020 stratégiája fő célokat és ezeken belül számos elgondolást tartalmazott a kibertéri fenyegetésekkel kapcsolatban.

Az EU kiberbiztonsági fejlesztésének kulcsfontosságú mérföldkövei közé tartozik a létfontosságú infrastruktúrák védelméről szóló 2012-es állásfoglalás, a 2013-as uniós

kiberbiztonsági stratégia, valamint a GDPR és a NIS-irányelv 2016-os elfogadása. Ezután pedig egy új uniós biztonsági stratégia 2016-os publikálása és hatályba helyezése. A kiberbiztonsági stratégiához szorosan kapcsolódott a 2015-ben kiadott európai digitális egységes piaci stratégia is, amely az európai társadalom átalakítását tűzte ki célul.

Ezt követően a NIS2 irányelvet azért dolgozták ki, mert a kiberfenyegetések egyre nagyobb méreteket öltöttek, és szinte minden szektorban jelen volt, emellett a NIS irányelv nem volt képes teljes mértékben kezelni a kibertámadásokkal kapcsolatos új kihívásokat, különösen az ellátási láncok biztonságát és a digitális infrastruktúrák védelmét. A NIS eredetileg nem foglalkozott alapvetően a gyorsan változó digitális környezettel, és nem tartalmazott megfelelő automatizmusokat a tagállamok közötti szorosabb együttműködésre. Főleg, hogy ez az egyik alapköve annak, hogy a tagállamok egységesen védjék meg az EU-s állampolgárok személyes adatait. A NIS2 és a hozzá kiadott Eu-s végrehajtási ajánlások már sokkal pontosabban megfogalmazták az elérendő célokat és az azokhoz vezető utat, valamint ez az irányelv felelősöket is kijelöl és büntetési tételeket is megfogalmaz.

2020 decemberében az Európai Bizottság előterjesztette az új kiberbiztonsági stratégiát, majd az előkészítő munka és tárgyalások után az Európai Unió Tanácsa 2021 márciusban következtetésekben foglalta össze álláspontját a stratégiával kapcsolatban. Az elfogadott tanácsi megállapítások feladata az volt, hogy az általános kereteket meghatározó stratégia gyakorlati megvalósításához szükséges lépéseket meghatározza. Felhatalmazza az Európai Bizottságot, valamint a kül- és biztonságpolitikai főmegbízottat arra, hogy konkrét szakpolitikai intézkedési terveket dolgozzon ki. Az Európai Bizottság által beterjesztett új kiberbiztonsági stratégia célja az volt, hogy megőrizze a globális és nyílt internetet, biztosítékot nyújtva ugyanakkor arra, hogy a biztonság mellett az európai értékek és a mindenkit megillető alapvető jogok is védelmet élvezzenek. [135] [136]

A személyes adatok védelme mára alapvető eleme lett a kiberbiztonsági stratégiáknak. Az európai országok esetében az adatvédelem és a kiberbiztonság szorosan összefonódik. Az Európai Unió által hozott jogszabályok, mint például a GDPR, megerősítik a személyes adatok védelmének fontosságát, és a legtöbb tagállam kiberbiztonsági stratégiájában kiemelt szerepet kap ez a téma. A stratégiák fogalmát és célját, valamint a kiberbiztonsági stratégiák definícióját, készítését és kritériumait kutatásom során nem vizsgáltam, mivel ezekről a fogalmakról részletes útmutatót találunk Prof. Dr. Kovács László Kiberbiztonság és -stratégia című könyvében. [137]

A kiberbiztonsági stratégiák és a személyes adatok védelmének összefüggéseinek kutatása segített az adatvédelem hatékonyabbá tételében és a kockázatok csökkentésében. Az eredmények hozzájárulhatnak új védelmi intézkedések kidolgozásához, amelyek minimalizálják az adatlopás és visszaélés esélyét. Emellett a kutatások segíthetnek a jogszabályok és szabványok fejlesztésében, így növelve az egyének és szervezetek biztonságát. Végső soron a bizalom erősödik az online szolgáltatások iránt, ami a digitális gazdaság fenntartható fejlődését is támogatja. Ennek tükrében megvizsgáltam számos stratégiai dokumentumot.

A német Kiberbiztonsági Stratégia 2021.[145] külön fejezetet (5.2) szentel a személyes adatok védelmének. A dokumentum hangsúlyozza, hogy a személyes adatok védelme a kiberbiztonság szerves része, és kiemeli az adatvédelmi jogszabályok betartását, valamint az adatvédelmi incidensek megelőzésének fontosságát is. A személyes adatok védelmét ebben az esetben jellemzően a kiberbűnözéssel összefüggésben mutatja be a dokumentum.

A francia kormány által elfogadott Kiberbiztonsági Stratégia 2020.[146] szintén külön pontban (2. célkitűzés) foglalkozik a személyes adatok védelmével. A stratégia részeként a kormány célja, hogy megerősítse az adatvédelmi jogokat, és biztosítsa az adatvédelmi szabályozások betartását a digitális környezetben. A Francia Kiberbiztonsági Hatóság (ANSSI[147]) is frissíti, és kezeli az adatvédelmi szabályozások és a kiberbiztonsági intézkedések összehangolását.

A belga kormány Kiberbiztonsági Stratégiája szintén hangsúlyozza a személyes adatok védelmének kiemelt fontosságát napjainkban. A dokumentumban az állampolgárok jogainak védelme és az adatvédelmi szabályok betartása alapvető célként szerepel. A kormány különös figyelmet fordít a nemzeti kiberbiztonsági incidensek kezelésére, amelyek az adatvédelmi jogsértésekkel is összefügghetnek.

Hollandiában a Kiberbiztonsági Stratégiában szereplő adatvédelmi irányelvek biztosítják a személyes adatok védelmét. Az ország kormányának célja, hogy elősegítse a digitális biztonságot és az adatvédelmet, valamint támogassa a GDPR alkalmazását minden kiberbiztonsági intézkedésben.

[145] Federal Ministry of the Interior, Building and Community: Cyber Security Strategy for Germany 2021. August 2021 p 14.
[146] French National Digitalsecurity Strategy p 19.
[147] Agence nationale de la sécurité des systèmes d'information

Mivel az Egyesült Királyság már nem tagja az EU-nak, a National Cyber Security Strategy (2016-2021.) és az újabb irányelvek is kiemelten kezelik a személyes adatok védelmét. A brit stratégia integrálja a GDPR elveit, és az adatvédelem alapvető része a nemzeti kiberbiztonsági politikának.

Ezek az országok különböző szinten kezelik a személyes adatok védelmének kérdését a kiberbiztonsági stratégiáikban, de közös céljuk, hogy biztosítsák az állampolgárok adatainak védelmét a digitális térben, miközben fenntartják a nemzeti és nemzetközi jogi kereteket is. Az EU-s jogszabályok és irányelvek, mint a GDPR, alapvetően alakítják a kiberbiztonsági politikákat, és minden tagállam számára kötelező a megfelelés ezeknek a szabályozásoknak.

Az Unió tekintetében megállapítható az, európai adatvédelmi reformnak három fő pillére van: a GDPR rendelet, a bűnügyi adatvédelmi irányelv – amelyet a nemzeteknek a tagállami jogukba be kellett építeniük–, valamint a jelenleg hatályban lévő e-Privacy irányelvet majdan felváltó új rendelet.

Pontosabban az e-Privacy irányelv, hivatalos nevén a 2002/58/EK irányelv, az Európai Unió egyik adatvédelmi jogszabálya, amely az elektronikus hírközlés során megvalósuló adatkezelésre fókuszál. Legfőbb célja a digitális kommunikáció titkosságának és a felhasználók magánéletének védelme, különösen az internetes szolgáltatások, elektronikus levelezés, telefonhívások, valamint a sütik és más nyomkövető megoldások használata során.

Az irányelv meghatározza, hogy milyen módon kell a weboldalaknak engedélyt kérniük a sütik alkalmazásához, milyen feltételekkel végezhető elektronikus direkt marketing, valamint hogy miként kezelhetők a kommunikáció során keletkező metaadatok. Az e-Privacy szabályozás alapvetően szűkebb területre fokuszál, de abban mélyebb és speciálisabb védelmet biztosít, mint az általános adatvédelmi rendelet (GDPR).

A kiberstratégia megvalósításának része az ENISA szerepének a megerősítése a kiberbiztonsági jogszabályban, valamint a közeljövőben az IPAR 4.0 térhódítására reagálás keretében várható olyan, a kiberbiztonságot, illetve az adatvédelmet érintő jogszabályok elfogadása, mint a mesterséges intelligencia használatával és az összekapcsolt (IoT) rendszerekkel kapcsolatos rendeletek.

Kutatásom során a fenti példákon túl összefoglaltam, hogy az uniós országok tekintetében az ENISA és a NATO Kooperatív Kibervédelmi Kiválósági Központ (CCD COE) adatai alapján számos ország aktualizálta kiberbiztonsági stratégiáját az alábbiak szerint.

Ausztria	2013.03.20.	Austrian National Cyber Security Strategy
Belgium	2021.05.20.	Belgian National Cyber Security Strategy[19]
Bulgária	2016.07.18.	Bulgarian National Cyber Security Strategy[20]
Ciprus	2020.12.03.	Cyprian National Cyber Security Strategy
Csehország	2021.01.01.	Czech National Cyber Security Strategy[21]
Dánia	2018.05.01.	Danish Cyber and Information Security Strategy[22]
Észtország	2019.05.09	Cybersecurity Strategy 2019-2022
Finnország	2013.01.24.	Finnish National Cyber Security Strategy
Franciaország	2015.10.10.	French National Digital Security Strategy[23]
Görögország	2020.12.07.	Greek National Cyber Security Strategy V3
Hollandia	2018.04.21.	Dutch National Cyber Security Agenda
Horvátország	2015.07.10	Croatian National Cyber Security Strategy
Írország	2019.12.27.	Irish National Cyber Security Strategy
Izland	2015.04.01.	Icelandic National Cyber Security Strategy
Lengyelország	2019.10.31.	Polish National Cyber Security Strategy
Lettország	2019.01.01.	Latvian National Cybersecurity Strategy
Litvánia	2018.08.13.	Lithuanian National Cybersecurity Strategy
Luxemburg	2018.01.26.	Luxembourgish National Cyber Security Strategy
Magyarország	2018.03.21.	Hungarian National Cyber Security Strategy
Málta	2016.09.26.	Maltese National Cyber Security Strategy
Németország	2021.09.09.	German National Cyber Security Strategy
Olaszország	2017.03.01.	Italian Cybersecurity Action Plan
Portugália	2019.06.06.	Portuguese National Cyber Security Strategy
Románia	2013.05.23.	Romanian National Cyber Security Strategy
Spanyolország	2019.04.01.	Spanish National Cyber Security Strategy
Szlovákia	2021.01.07.	Cyber Security Concept of the Slovak Republic
Szlovénia	2016.02.01.	Slovenian National Cyber Security Strategy

22. ábra Európai térség Forrás: Saját kutatási adatok

Kutatásom során annak érdekében, hogy szélesebb spektrumban lássam a kiberbiztonsági stratégiák és a személyes adatok összefüggését további országok kiberbiztonsággal kapcsolatos stratégiáját is megvizsgáltam az alábbi táblázat szerint.

Dél-Amerika és a karibi térség

Antigua és Barbuda	2020.01.06.	National Cybersecurity Strategy
Argentína	2019	National Cybersecurity Strategy
Barbados		nem rendelkezik stratégiával[46]
Belize	2020	National Cybersecurity Strategy towards a secure cyberspace 2020-2023
Brazília	2020.02.06.	National Cybersecurity Strategy
Chile	2017	National Cybersecurity Policy (NCSP) 2017-2022
Dominikai Köztársaság	2018	National Cybersecurity Strategy 2018-2021[47]
Ecuador	2021.07.23.	Cybersecurity Policy
Guatemala	2018	Cybersecurity Policy[48]
Guyana		nem rendelkezik stratégiával[49]
Jamaica	2015	Jamaica's National Cyber Security Strategy[50]
Kolumbia	2016	National Digital Security Policy[51]
Mexikó	2017	National Cybersecurity Strategy
Panama	2013	National Strategy for Cybernetic Security and Critical Infrastructure Protection[52]
Paraguay	2017	National Cybersecurity Plan: Challenges, Roles and Commitments
Peru		nem rendelkezik stratégiával
Suriname		nem rendelkezik stratégiával[53]
Trinidad és Tobago	2012.12.	National Cyber Security Strategy

23. ábra Dél-Amerikai térség Forrás: Saját kutatási adatok

Albánia	2021. február	Cybersecurity Strategy 2020-2025[24]
Andorra		nem rendelkezik stratégiával
Bosznia-Hercegovina	2019. október	Guidelines for a strategic Cybersecurity Framework in Bosnia and Herzegovina
Észak-Macedónia	2018	National Cybersecurity Strategy 2018-2022[25]
Liechtenstein	2021	FMA Guidance 2021/17 – Implementation of the ICT Security Guideline és FMA Guidelines 2021/3 – ICT Security Guidelines
Monaco	2017	National Cyber Security Strategy
Montenegró	2017	Cybersecurity Strategy 2018-2021[26]
San Marino	2017	State Computer Plan 2017-2019
Svájc		National strategy for the protection of Switzerland against cyber risk (NCS) 2018-2022
Szerbia	2017	Strategy for the Development of Information Security in the Republic of Serbia for the period 2017-2020[27]
Törökország	2020.12.29.	National Cybersecurity Strategy and Action Plan (2020-2023)
Ukrajna	2021.08.26.	Cybersecurity Strategy of Ukraine
Vatikán		nem rendelkezik stratégiával

24. ábra Európai térség II. Forrás: Saját kutatási adatok

A vizsgálatok alapján megállapítható, hogy a kibervédelmi koncepciók, stratégiák, valamint a kiberbiztonsági szabályozás alapvetően és döntően az adatvédelem, a kiskorúak védelme, a bűnüldözés, a terrorizmus elleni harc, a létfontosságú infrastruktúra védelme és a hálózati biztonság területén kezdtek megjelenni a stratégiák kidolgozása során. A kiberbiztonsági stratégiák számos olyan kérdést tartalmaznak, amelyek a kiberbiztonsági stratégia eredeti céljain jóval túlmutathat. Ilyen például a kiberbiztonsági stratégiában megfogalmazott olyan újonnan megjelent kérdések, mint például a személyes adatok védelme, amelyek az adott ország biztonsági stratégiájának kiegészítése érdekében kerültek bele magába a stratégiai dokumentumba.

A stratégiai dokumentumoknak komplex és ma már gyorsan változó környezetet kell lekövetniük. Ezek a dokumentumok meghatározzák, és rögzítik az adott ország politikai céljait az éppen aktuális politikai környezethez viszonyítva. A kiberbiztonsági stratégiák alapját az esetek túlnyomó többségében az adott kormány, a politikai vezetés nemzeti biztonságról, valamint az országot érintő fenyegetésekről kialakított aktuális képe jelenti.

A kiberbiztonsági stratégiák célja az, hogy egyértelműen bemutassák a nemzeti szintű kiberbiztonság szavatolásának lehetséges módjait, illetve azokat a feladatokat, amelyek felmerültek vagy felmerülhetnek annak érdekében, hogy az ország érvényesíteni tudja saját geopolitikai érdekeit a kibertérben. Ezek a stratégiák számos területre kitérnek, ezek közül tanulmányomban a személyes adatok védelmének koncepcióját és annak megjelenését vizsgáltam, ezek alapján az alábbi megállapításokat teszem.

Globális viszonylatban a kiberbiztonsági stratégiák nem mutatnak homogén struktúrát. Túlnyomó többségük azonban tartalmazza azokat a célokat, amelyek elősegítik a kiberreziliencia növelését, erősítik a fellépést a kiberbűnözés ellen, valamint fokozzák a kiberdiplomáciai tevékenységet, és természetesen a kibervédelem megerősítését tűzik ki célul. E célokon felül a stratégiákban magától értetődően megjelenik a létfontosságú infrastruktúra védelme is. A személyes adatok védelmének megjelenése vonatkozásában a következőket azonosítottam:

a) a személyes adatok megjelennek a vizsgált stratégiákban, de nem önállóan megfogalmazott célként vagy kiemelt digitális értékként, hanem csak olyan adatként, amit meg kell védeni.

b) a személyes adatok úgynevezett adatvagyon formájában megjelennek,

mert a kiberbűnözői csoportok ezeket az adatokat a későbbiekben fel tudják használni további bűncselekmények kivitelezéséhez.

c) a személyes adatok védelme sok esetben az alapvető emberi jogokhoz és szabadságjogok védelméhez kapcsolódik[148].

d) a személyes adatok védelme ritkán jelenik meg olyan formában, amely alapján ezek védelme kiemelt fontosságú különálló nemzeti kibervédelmi feladat lenne. A kiberbiztonsági stratégiák kiemelt feladatként kezelik, hogy ezen adatok védelmének és szerepének fontosságát adatvédelmi tudatosságra „nevelés" keretében közvetítsék a lakosság minden korosztálya felé.

e) Egyes létfontosságú ágazatokban, mint például a közlekedésben, az energetikában, az egészségügyben és a pénzügyi ágazatban az alapvető tevékenységek egyre inkább kiszolgáltatott a kibertérből érkező fenyegetéseknek. A személyes adatok védelme a stratégiákban hatványozottan jelenik meg azokban az országokban, ahol az e-közigazgatás már részben vagy teljes mértékben szerves része a közigazgatási folyamatoknak. Ez látható is egyes stratégiákban (Panama), ahol az ország nagyban függ a digitális szolgáltatásoktól, ott maga a stratégia is jobban kidolgozott.

f) a kiberbiztonsági stratégiákat az érintett ország geopolitikai helyzete is meghatározza, valamint a környező országoktól való viszonya, illetve attól, hogy az adott ország mennyire kiszolgáltatott a kor digitális technológiai környezetének (pl. szolgáltatási szektor).

g) a személyes adatok védelmét jellemzően nemcsak a stratégiai dokumentumok adják, hanem az ezekre ráépülő törvények és határozatok, akciótervek összessége. Vagyis megállapítható, hogy a kiberbiztonsági stratégiákban szereplő elgondolások csak akkor valósulnak meg (érvényesülnek), ha van mögöttük olyan jogszabály, amely kényszerítő hatályú.

Annak érdekében, hogy aktuális képet kaphassak a személyes adatok védelméről és a kiberbiztonsági stratégiák összefüggéséről, egyes országok kiberbiztonsági startégiáit és a személyes adatok védelmét részletesebben vizsgáltam.

A vizsgált időszakban (2021 és 2023 között) a dán, román, izlandi és olasz kormányok is közzétették nemzeti kiberbiztonsági stratégiáikat.

[148] Az Európai Unió Alapjogi Charta, illetve az Európai Unió Bírósága gyakorlatához.

Kutatásomban azt vizsgáltam, hogy a személyes adatok védelme milyen módon jelenik meg ezekben a dokumentumokban. Az elemzés során különös figyelmet fordítottam az említett országok stratégiáira, valamint arra, hogy az Amerikai Egyesült Államok Védelmi Minisztériuma szintén kiadta a „2023 Department of Defense Cyber Strategy" című dokumentumát az adott időszakban.

A kutatásom során a következő megállapításokat tettem:

A kiberbiztonsági stratégiák általában nem szabályozó jellegűek, hanem inkább azt vázolják fel, hogy az adott kormány miként tudja hasznosítani, és megerősíteni rendelkezésre álló eszközeit és erőforrásait a gyorsan fejlődő digitális ökoszisztémában való szuverenitás megőrzése érdekében. E stratégiák kitérnek a globális együttműködések erősítésére is olyan partnerekkel, akik osztják a nemzeti értékeket, például a demokrácia, a jogállamiság és az emberi jogok területe. A stratégiák a kritikus infrastruktúrák és alapvető szolgáltatások, például az egészségügyi intézmények IT-rendszerei, az energiahálózatok, a vasúti közlekedés, az IPAR 4.0[149] és az okos megoldások kiberbiztonságát is tárgyalják, beleértve a személyes adatok védelmét. [138] [139]

3.13 Az új magyar kiberbiztonsági stratégia

2025. március 31-én a Magyar Közlönyben közzétették Magyarország kiberstratégiáját. A 2025-ös magyar kiberbiztonsági stratégia egyik meghatározó eleme a személyes adatok védelmének megerősítése a digitális térben. A stratégia központi felismerése, hogy az egyre szélesebb körű digitalizáció és a mindennapi életben használt digitális szolgáltatások rohamos terjedése az állampolgárok személyes adatait kiemelten veszélyeztetetté teszi. A dokumentum számos ponton[150] tér ki a személyes adatok biztonságának garantálására, különösen az elektronikus információs rendszerek védelme és az adatbiztonság komplex megközelítése miatt.

A stratégia kiemeli, hogy a személyes és érzékeny adatok védelme nemcsak műszaki kérdés, hanem nemzetbiztonsági és társadalmi szempontból is alapvető fontosságú. A dokumentum

[149] Az IPAR 4.0 a termelési folyamatok szervezése, amelyben a hálózatba kapcsolt okos eszközök érzékelnek, információkat szereznek, egymással kommunikálnak, és adatalapú döntéseket hoznak. Mesterséges intelligenciával vezérelt gyártási folyamatokat hoznak létre. A rendszerek nyomon követik a fizikai folyamatokat és decentralizált döntéseket hoznak adatcsere alapján.
[150] 35. pont; 9.5; közvetlenül

hangsúlyozza, hogy a kiberbiztonsági ökoszisztéma elsődleges célja az állampolgárok online jelenlét biztonságának biztosítása, amely a személyes adatok integritásának, bizalmasságának és rendelkezésre állásának megőrzésén keresztül valósul meg.

Az adatbiztonság sérülékenysége külön fejezetet is kapott, amelyben rámutatnak arra, hogy mind állami, mind nem állami szereplők egyre gyakrabban használják a kiberteret érzékeny adatok, így személyes információk megszerzésére. Ennek ellensúlyozására a stratégia külön intézkedéseket javasol, például az incidenskezelő központok (CSIRT), biztonsági műveleti központok (SOC) fejlesztését és a sérülékenységek koordinált közzétételének jogi megalapozását.

Ezen felül a dokumentum hangsúlyozza a "security-by-design" elv alkalmazását: minden új digitális fejlesztés esetén már a tervezés kezdeti szakaszában figyelembe kell venni az adatvédelem és az információbiztonság szempontjait. A kritikus infrastruktúrák – például a közigazgatás, az egészségügy – esetében ez a szemlélet különösen erős elvárásokat támaszt. Az adatvédelem nem csupán belső kockázatkezelési feladat, hanem az állampolgári bizalom fenntartásának alapja is.

A stratégia összhangban van az EU NIS2 irányelvével és a 2024. évi LXIX. törvénnyel, amelyek szintén kiemelt figyelmet szentelnek a személyes adatok védelmének. A jogi szabályozás és az operatív rendszerek fejlesztése egymást erősítően hat a magyar állampolgárok adatbiztonságára, amely így nemcsak elméleti célkitűzés, hanem egyre konkrétabb intézményi és technikai keretrendszerrel is rendelkezik. A stratégia tehát komplex módon és előrelátóan kívánja biztosítani a magyar állampolgárok digitális jogainak védelmét a 21. század kihívásai között.

Abban az esetben, ha nem a személyes adatok szemszögéből elemezzük, akkor a megállapítható, hogy négy jelentősebb elgondolás köré épül fel a stratégia. A hibrid fenyegetések köré, mivel a globális válságok és a hibrid hadviselés drámai módon növelte a kiberkockázatokat. A dezinformációs műveletek, amelynek során az egyének és a társadalom közötti összhang megzavarása egyre súlyosabb problémává válik. Továbbá az adatbiztonság és ellátási láncok sérülékenysége miatt az adatok védelme és a kritikus infrastruktúra biztonsága kulcsfontosságú tényező. Valamint a technológiai függőség ami miatt a köz- és magánszféra egyre inkább új működési modellekre kényszerül.

3.14 Kutatási eredmények

Az internetet alapvetően nem a biztonságot és biztonságos adatkezelést szem előtt tartva tervezték meg. Látható, hogy jelenleg egyre több felhasználó egyre nagyobb mennyiségű személyes adatot oszt meg ebben a közegben.

A kiberbiztonsági incidensek emelkedő száma miatt, valamint a növekvő fogyasztói igényre egyes országokban különböző kibervédelmi szabályozást vezettek be, viszont a gyors növekedése a digitális ökoszisztémának magával hozta az adatok megszerzését irányzó kibertámadásokat is.

Nem csak a támadások száma nőtt meg drasztikusan, hanem az információs technológiától való függőség miatt az adatszivárgások hatásai is egyre jelentősebbek a szektorban. Mind a kormányzati, mind a polgári szektorban nagyobb figyelmet fordítunk adatvédelemre.

A személyes adatok védelme és a GDPR megfelelő alkalmazása külön kockázatértékelést igényel minden egyes új technológia bevezetésekor, valamint már alkalmazott technológiák esetén is rendszeres felülvizsgálatokat kell végezni.

Indoklásomban több kulcsfontosságú tényezőt kell figyelembe venni, amelyek a jogi előírások, a technológiai fejlődés és az adatkezelés folyamatának komplexitása köré csoportosulnak. Mivel a technológia folyamatosan fejlődik, új és innovatív megoldások jelennek meg, amelyek új típusú adatkezelést vagy adatgyűjtést tesznek lehetővé. Ha egy új technológia vagy rendszer hasonló adatvédelmi és adatbiztonsági paraméterekkel rendelkezik mint elődjei, az új eszközök vagy platformok sajátos módon kezelik, tarolják vagy továbbítják a személyes adatokat, amik új kockázatokat vetnek fel. GDPR nem csak a technológia hasznosítását szabályozza, hanem az adatkezelés minden aspektusát, amely a személyes adatokat érinti. A GDPR alapján minden adatkezelőnek és adatfeldolgozónak meg kell felelnie az alapvető adatvédelmi elveknek, mint például az adat minimális mértékű kezelése, a célhoz kötöttség és a transzparencia.

A GDPR előírja, hogy minden új adatkezelési művelet előtt [151]el kell végezni egy adatvédelmi hatásvizsgálatot (DPIA - Data Protection Impact Assessment), különösen akkor, ha a technológia bevezetése magas kockázattal jár a személyes adatok védelme szempontjából. Ilyen technológiai változások például az új szoftverek, adatbázisok, alkalmazások, vagy a biometrikus adatok kezelésére irányuló új technológiák. Ha nem végeznek el ilyen vizsgálatot, az adatkezelők felelősségre vonhatók jogsértésért.

[151] GDPR 35. cikke

Az adatok széleskörű összegyűjtése és elemzése lehetővé teszi a személyek közvetett azonosítását, ami új típusú adatkezelési kockázatokat jelenthet. A Big Data alkalmazásakor figyelembe kell venni, hogy az összegyűjtött adatok mennyisége és az azokból történő következtetések hogyan befolyásolhatják a személyek adatvédelmét (vagy privát szféráját, vagy az információs önrendelkezési jogukat).

Az IoT eszközök, mint például a viselhető okoseszközök vagy a "smart home" rendszerek folyamatosan gyűjtik a felhasználók személyes adatait, például helyadatokat, egészségügyi információkat. Ezek az eszközök gyakran folyamatos kapcsolatban állnak a felhővel, így az adatok védelme és biztonsága folyamatosan fenyegetésnek van kitéve.

Az MI és ML rendszerek különösen érzékenyek lehetnek az adatok torzulására, az algoritmusok átláthatatlanságára, és gyakran igényelnek az adatvédelmi szempontok figyelembevételét a tréningadatok feldolgozása során.

Bár a GDPR az EGT egész területére érvényes, az adatvédelemre vonatkozó előírások és a jogi környezet egyes országokban eltérhetnek. Ez különösen akkor fontos, ha egy új technológia globálisan is alkalmazásra kerül, és a különböző piacokon különböző adatvédelmi előírásoknak kell megfelelnie. Például az Egyesült Államokban az adatvédelemről szóló törvények nem azonosak az EU jogi kereteivel, így egy új technológia globális bevezetésénél folyamatos jogi tanácsadásra és az adott régió adatvédelmi törvényeinek figyelembevételére is szükség lehet.

4. Hipotézis igazolása

A személyes adatok védelme az információs társadalomban alapvető jelentőségű kérdéssé vált, különösen az új és meglévő technológiai megoldások tekintetében. A különböző iparágak digitalizációja, az IoT eszközök elterjedése, valamint az adatalapú döntéshozatal növekedése exponenciálisan növeli az adatvédelem kockázatait. Ezért minden egyes új vagy már alkalmazott, műszaki technológia esetében szükség van külön kockázatértékelésre, és elengedhetetlen a GDPR-nak való megfelelés vizsgálata. Ennek alapja, hogy nem létezik egységes, minden technológiára alkalmazható adatvédelmi keretrendszer, amely képes lenne figyelembe venni a különböző technológiák sajátosságait.

A kockázatértékelés fontosságát az adatvédelmi rendelet (GDPR) is hangsúlyozza. Az adatkezelők és adatfeldolgozók kötelessége minden esetben felmérni, hogy egy adott technológia alkalmazása során milyen típusú személyes adatokat gyűjtenek, tárolnak, és dolgoznak fel, illetve ezek milyen veszélyeknek vannak kitéve. A külön kockázatértékelés azért

szükséges, mert minden technológia más jellegű veszélyeket rejt magában. Például egy okosotthon-rendszer, amely szenzorokkal monitorozza a háztartás működését, egészen más adatvédelmi kihívásokat vet fel, mint egy felhőalapú adattárolási szolgáltatás. Az előbbiben az eszközök közötti kommunikáció védelme kritikus, míg az utóbbiban az adattitkosítás és a hozzáférés-szabályozás jelent prioritást. Ezért minden technológia esetében egyedi megközelítésre van szükség a potenciális fenyegetések és azok hatásainak azonosításához.

A GDPR megfelelőségi vizsgálat szintén alapvető követelmény minden adatkezelési folyamat esetében. A rendelet célja az egyének személyes adatainak magas szintű védelme, ezért az adatkezelők kötelesek biztosítani, hogy technológiáik és folyamataik megfelelnek a GDPR követelményeinek. Ez különösen fontos az olyan innovatív technológiák esetében, mint a mesterséges intelligencia (MI) vagy a blockchain, amelyek működése gyakran átláthatatlan a felhasználók számára. Az MI például nagy mennyiségű adatot elemez, és dolgoz fel, ami jelentős adatvédelmi kockázatokat hordozhat, például az adatok nem megfelelő anonimizálása vagy a diszkriminatív döntéshozatal miatt. Az ilyen technológiák alkalmazása előtt a GDPR-nak való megfelelőség vizsgálata biztosítja, hogy az adatok feldolgozása jogszerű, tisztességes és átlátható legyen.

Az egységes kiberbiztonsági keretrendszer kialakításának korlátai szintén alátámasztják a külön kockázatértékelések és megfelelőségi vizsgálatok szükségességét. Az eltérő iparágak és technológiák egyedi biztonsági követelményeket támasztanak. Egy egészségügyi adatokat kezelő rendszer például rendkívül szigorú biztonsági és adatvédelmi intézkedéseket követel meg, míg egy e-kereskedelmi platformon a vásárlók fizetési adatainak védelme kerül előtérbe. Az ilyen eltérések miatt nem lehetséges egyetlen, minden technológiára alkalmazható keretrendszer kialakítása, amely figyelembe venné az összes specifikus követelményt és fenyegetést.

A külön kockázatértékelések és megfelelőségi vizsgálatok nemcsak a jogszabályi megfelelőség biztosításában játszanak kulcsszerepet, hanem a szervezetek reputációjának és az ügyfelek bizalmának fenntartásában is. Az adatvédelmi incidensek, például adatszivárgások vagy adatlopások, súlyos bírságokat és jelentős üzleti veszteségeket eredményezhetnek. Ezzel szemben az adatvédelembe való proaktív befektetés[152] és a folyamatos megfelelőség-ellenőrzés hozzájárul a fenyegetések minimalizálásához és a hosszú távú üzleti sikerhez.

[152] A beépített és alapértelmezett adatvédelem a GDPR alapján kötelező.

Összességében elmondható, hogy a személyes adatok védelme minden új vagy már alkalmazott technológia esetében megköveteli a külön kockázatértékelést és a GDPR-megfelelőség vizsgálatát. Ez nemcsak jogi és etikai kötelezettség, hanem üzleti érdek is, hiszen a digitális világ biztonsága és átláthatósága alapvetően befolyásolja a szervezetek működését és a társadalom bizalmát. Az egységes kiberbiztonsági keretrendszer hiánya miatt pedig csak az egyedi vizsgálatok és a folyamatos fejlesztések biztosíthatják az adatvédelem fenntarthatóságát.

A fenti technológiák és rendszerek vizsgálata során bebizonyítottam azt, hogy a személyes adatok védelme minden új/már alkalmazott technológia esetében külön kockázatértékelést követel meg, valamint GDPR megfelelősségi vizsgálat is minden esetben szükséges, mivel nem készíthető el egy egységes adatvédelmi és kiberbiztonsági keretrendszer ebben a tekintetben. Kutatási eredményeimet részletesen a társszerzők és az általam készített könyvben, kettő könyvfejezetben és 18 darab tanulmányban bemutattam.

5. Kitekintés

A NIS2[153] irányelv elsődlegesen az információs és hálózati rendszerek biztonságának megerősítésére fókuszál, nem konkrétan a személyes adatok védelmére összpontosít természetesen. Azonban a személyes adatok védelme közvetetten jelen van az irányelvben. A NIS2 és a GDPR alapvetően kiegészítik egymást. Amikor a NIS2 irányelv alapján egy szervezet kiberbiztonsági intézkedéseket hajt végre, azok hozzájárulnak a személyes adatok védelméhez is, mivel a kutatásomban bemutattam, hogy a kiberbiztonsági incidensek egyre többször érintik a személyes adatokat. Mivel a NIS2 előírja, hogy az érintett szervezetek hatékony kockázatkezelési intézkedéseket vezessenek be. Ez így magában foglalja a személyes adatok védelmére szolgáló biztonsági intézkedéseket, az adatvesztés megelőzését, a jogosulatlan hozzáférés elleni védelmet, és az incidenskezelést. Ha egy kiberbiztonsági incidens kihatással van személyes adatok védelmére, az érintett szervezeteknek jelentési kötelezettségük van, nemcsak a NIS2, hanem a GDPR alapján is. Így a NIS2 által előírt incidenskezelési folyamatok közvetetten támogatják a személyes adatok védelmét. A NIS2 kiterjed számos szektorra, amelyek gyakran kezelnek nagy mennyiségű érzékeny személyes adatot. Ezek biztonságának megerősítése hozzájárulhat a személyes adatok védelméhez is. Így megállapítható, bár a NIS2 irányelv nem kifejezetten az adatvédelemről szól, az információs rendszerek biztonságának erősítése révén szorosan kapcsolódik a személyes adatok védelméhez.

Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban Kiberbiztonsági tv.) és a személyes adatok védelme szoros kapcsolatban állnak egymással, mivel mindkettő célja a digitális környezet biztonságának fenntartása, és a személyes adatok védelme egy alapvető eleme a kiberbiztonságnak. Különbség az, hogy a GDPR célja az érintettek jogainak és szabadságainak védelme, míg a NIS2-nek az EIR-ekben lévő adatok (információ) védelme. A Kiberbiztonsági tv. biztosítja, hogy a digitális infrastruktúrák, rendszerek és hálózatok védve legyenek a kibertámadásoktól, amelyek során személyes adatok is veszélybe kerülhetnek. Ha a kiberbiztonság megfelelő, akkor csökkenti annak a valószínűségét, hogy adatlopás, személyes adatokkal való visszaélés vagy más adatvédelmi

[153] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2022. december 14-i (EU) 2022/2555 IRÁNYELVE az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

incidens történjen. A Kiberbiztonsági tv. és az adatvédelmi jogszabályok (például a GDPR) kiegészítik egymást, vagy a GDPR által előírt adatbiztonságot a NIS2 betartása elősegíti. A kiberbiztonság nemcsak a rendszerek védelmét jelenti, hanem azt is, hogy az adatkezelők (pl. cégek, állami szervek) megfelelő intézkedéseket hozzanak a személyes adatok védelmére a kibertámadásokkal szemben. A törvény rögzíti a kiberbiztonsági kötelezettségeket, amelyek közvetlenül érinthetik a személyes adatok kezelését. A megfelelő védelmi intézkedések megléte (például titkosítás, hozzáférés-ellenőrzés, rendszeres frissítések) elősegíti, hogy az adatkezelők és adatfeldolgozók megfeleljenek a személyes adatok védelmével kapcsolatos jogszabályoknak.

A Kiberbiztonsági tv.-ben a személyes adatok védelme több helyen is megemlítésre kerül. A legfelső szintű domain név nyilvántartás esetében a törvény szerint a központi domain név nyilvántartásban szereplő adatokat nyilvánosan hozzáférhetővé kell tenni, kivételt képeznek a személyes adatok ebben az esetben.[154]

Majd ezt követően megjelenik a kiberbiztonsági auditra vonatkozó rendelkezések részben is 21. § 5. pontjában, ahol már látható a fent említettek szerint az, hogy a törvény szinergiában van a GDPR-ral. Mivel *„az auditor az ellenőrzött szervezet kezelésében lévő, az audit lefolytatásához szükséges, az ellenőrzött szervezettől megkapott dokumentumokat – ideértve a személyes adatokat és az üzleti titoknak minősülő adatokat is – az audit során ellenőrzött követelmények teljesülésének vizsgálata céljából, az audit lefolytatásához szükséges mértékben, annak befejezéséig kezeli, azokat harmadik személy részére nem továbbíthatja.”*

Valamint a törvény szerint *„az auditor köteles szabályzatban rögzíteni azokat a munkaköröket, amelyeket betöltő személyek az audit során az üzleti titkokhoz hozzáférhetnek, annak tartalmát megismerhetik. Az auditban részt vevő személyeket az audit során tudomásukra jutott személyes adatok, valamint üzleti titok tekintetében titoktartási kötelezettség terheli, amely a foglalkoztatásra irányuló jogviszony megszűnését követő 5 évig, személyes adatok tekintetében pedig időkorlát nélkül fennmarad.”* Ez szintén egy jó példa arra, hogy a GDPR alapelveit is figyelembe vették a törvényhozók[155].

[154] 14. A legfelső szintű domain név nyilvántartás, 20. § 4. pont

[155] Itt dől el, hogy a kibervédelem, vagy pedig az érintettek információs önrendelkezési joga az erősebb. Egyébként az 7/2024. MK r. védelmi intézkedései között van egy pár olyan, amelynek következetes végrehajtása a GDPR megsértésével fog járni.

6. Publikációk

6.1 Publikációk és tézisek kapcsolata

Tézis száma (H)	Hipotézis megfogalmazása	Publikáció
H1	Jelenleg a magyar társadalom jelentős része nem rendelkezik megfelelően mély ismeretekkel az adatvédelem, valamint az újonnan felmerült kiberbiztonsági kockázatokról, amelyek a személyes adatok kiszivárgása vagy illetéktelen felhasználása tekintetében jelentkeznek, emellett nem is bíznak a szolgáltatók adatvédelmi megoldásaiban.	(K1, C5)
H2	A személyes adatok illegális és hanyag kezelése, amely során ezek az adatok jelentős számban folyamatos jelleggel kikerülnek a Surface Webre és a Dark Webre, egyre jelentősebb biztonsági kockázatot okoznak 2024-ben, és ez emelkedő tendenciát mutat majd a következő években is.	(C3, C4, C6)
H3	A személyes adatok védelme minden új/már alkalmazott technológia esetében külön kockázatértékelést követel meg, valamint GDPR megfelelősségi vizsgálat is minden esetben szükséges, mivel nem készíthető el egy egységes keretrendszer ebben a tekintetben.	(K1, KF1, KF2, C1, C2, C7-14)

6.2 Könyv

- (K1) Dr. Albert Ágota, Üveges András József: *Adatvédelemről alapfokon*, HM Zrínyi Média Közhasznú Nonprofit Kft., 2023, ISBN: 9786156128140

6.3 Magyar nyelvű könyvfejezet

- (KF1) Üveges András József: *A katonai információs rendszerek elleni műveletek – az informatikai megsemmisítés a valós szőnyegbombázástól a precíziós malware-ig*; In: Krasznay Csaba. Taktikák és stratégiák a kiberhadviselésben, Budapest: Ludovika Egyetemi Kiadó, pp 199-220 2023 ISBN: 9789635317998

6.4 Idegen nyelvű könyvfejezet

- (KF2) József András Uveges: *Terrorist Use of Artificial Intelligence-Driven Social Media* In: Antony Pfaff: *The Weaponization of Artifical Intelligence,* Centre of Excellence Defence Against Terrorism (COE-DAT), Ankara, 2025 ISBN:

6.5 Lektorált hazai idegen nyelvű folyóiratcikkek

- (C1) Üveges András József: Pprotectioon of Personal Data in the view of Allied National Cyber Security Strategies 2022-2023, National Security Review: Periodical of the military National Security Service 2023: (2) pp. 119-133.
  (C2) Üveges András József: Information and cyber operations of the russian-ukrainian conflict, and the possibilities, and risks of using the personal data, national security review : National Security Review : Periodical of the military National Security Service 2023: (1) pp. 119-179.
- (C3) Üveges András József: Forms and risks of personal data appearing on the darkweb and surface web illegally, negligently or intentionally I. HU ISSN 2063-2908 (2023)
- (C4) Üveges András József: Forms and risks of personal data appearing on the darkweb and surface web illegally, negligently or intentionally II. HU ISSN 2063-2908 (2023)

6.6 Batthyány Lajos Alapítvány doktori ösztöndíjprogram

- (C5) Dr. Dezső Tamás – Pócza István: BLA Doktori Ösztöndíjprogram Tanulmánykötet 2022/2023, 2023, Budapest. ISBN 978-615-82213-1-3 in Üveges András: Adatvédelmi incidensek a személyes adatok tükrében, adatvédelmi tájékoztatók paradigmái

- (C6) Dr. Dezső Tamás – Pócza István: BLA Doktori Ösztöndíjprogram Tanulmánykötet 2023/2024, 2024, Budapest ISSN 2939-8568 in Üveges András József: Kiberbiztonsági incidensek trendjei a személyes adatok kiszivárgásának tükrében

6.7 Lektorált magyar nyelvű folyóiratcikkek

- (C7) dr. Albert Ágota; Üveges András József: Az „IoT”-eszközök biztonsága a személyes adatok tükrében, Szakmai Szemle: A katonai nemzetbiztonsági szolgálat tudományos-szakmai folyóirata (1785-1181): 20 2 pp 138-187 (2022)
- (C8) dr. Albert Ágota; Dr. Tóth Sándor; Üveges András József, Lévai Zsolt: *A közlekedési rendszerek és az információs terrorizmus kapcsolata* Felderítő Szemle (1588-242X): 20 1 pp 18-58 (2021)
- (C9) Üveges András József: *A személyes adatok védelme a kiberbiztonsági stratégiák tükrében* Felderítő Szemle (1588-242X): 20 3 pp 145-162 (2021)
- (C10) Dr. Négyesi Imre, dr. Albert Ágota, Üveges András József: *A felhőalkalmazások adatvédelmi kérdései a GDPR tükrében,* Felderítő Szemle (1588-242X): 20 1 pp 151-179 (2021)
- (C11) Lévai Zsolt, Üveges András József: *A vasúti közlekedés informatikai adatvédelme,* Felderítő Szemle (1588-242X): 19 2 pp 103-139 (2020)
- (C12) Marlok Tamás; Üveges András József: *Korszerű nemzeti taktikai kiképzőrendszer fejlesztésének kérdései*, GDPR megfelelősége, Felderítő Szemle (1588-242X): 19 3 pp 91-126 (2020)
- (C13) Üveges András József: *Az európai unió általános adatvédelmi rendeletének (GDPR) egy értelmezése a blokkláncalapú rendszerekben*, Felderítő Szemle (1588-242X): 19 1 pp 197-207 (2020)
- (C14) Stiedl Krisztián; Üveges András József: *A GDPR követelményeinek integrációja az elektronikus felületeken*, FELDERÍTŐ SZEMLE (1588-242X): 18 pp 166-184 (2019)

7. Ajánlások és gyakorlati felhasználatóság

8. Összevont következtetések

Az értekezés eredményei bizonyítják, hogy digitális világunk egyik alapvető szükséglete az adat, mivel ezzel mára már kereskednek, tárolják, így elmondható, hogy a magánszemélyek, intézmények és kormányzati szervezetek számára is értékes megújuló és folyamatosan bővülő valuta.

Ezt a folyamatot jól jellemzi az, hogy a világban használt adatmennyiség óriási ütemben növekszik. Ez nem csak az egy főre jutó adatmennyiségre igaz, de az információk megosztásának ütemére is. Becslések szerint 2025-ben a naponta keletkező adatok mennyisége eléri a 463 milliárd gigabájtot, ami közel 200-szoros növekedést jelent a jelenlegi helyzethez képest. 2019 és 2020 között, mindössze egyetlen év alatt 10%-kal nőtt a közösségi médiát használók száma, és elérte a 3,96 milliárd főt.

Az információs társadalom fejlődésével párhuzamosan egyre több személyes adat kerül ki az internetre, amely jelentősen növeli az adatvédelmi kockázatokat, vagy incidenseket. A felhasználók többsége napi szinten használja az online szolgáltatásokat, azonban gyakran nincsenek tisztában az adatvédelem alapvető fogalmaival, jogaikkal, illetve az őket érintő kockázatokkal. Az adatkezelési tájékoztatókat, valamint a vonatkozó adatvédelmi szabályozásokat – például a GDPR rendelkezéseit – sok esetben figyelmen kívül hagyják vagy csak felületesen ismerik.

Ez a tudatossághiány súlyos következményekkel járhat, mivel a digitális ökoszisztémában a személyes adatokkal való visszaélés egyre gyakoribb, különösen a kiberbűnözői csoportok részéről, amelyek célzottan keresik és használják ki a felhasználói figyelmetlenségből vagy tájékozatlanságból eredő sebezhetőségeket.

Mindazonáltal fontos kiemelni, hogy az elmúlt években pozitív irányú elmozdulás figyelhető meg. Egyre több állami és magánszereplő integrálja a személyes adatok védelmét saját kiberbiztonsági stratégiáiba és megoldásaiba, a hatóságok is fokozott figyelmet fordítanak az adatvédelmi incidensek kivizsgálására, valamint a szankciók érvényesítésére (pénzbüntetés). Ezen tendenciák azt mutatják, hogy az adatvédelem és a kiberbiztonság egyre szorosabb kapcsolatba kerül egymással, és hosszú távon csakis a felhasználók tudatosságának növelésével, valamint a jogi és technikai szabályozás szigorú alkalmazásával lehet hatékonyan fellépni az adatvédelmi kockázatokkal szemben.

9. Függelékek

Függelék: Kutatási kérdőív I/A általános kérdés (magánélet és társadalmi megítélés)

A kérdőívben feltett kérdések:

- Hallott-e már az EU általános adatvédelmi rendeletéről (GDPR)?
- Soroljon fel 5 esetet, ahol már találkozott a rendelettel!
- Munkahelyén/beosztásában találkozott-e az adatvédelmi rendelettel?
- Magánéletében hol találkozik legtöbbször a GDPR fogalmával?
- Ön végigolvassa az ön által aláírt adatvédelmi rendeleteket?
- Ön maximálisan hány oldalas adatvédelmi rendeletet olvas el?
- Ön maximálisan hány percet szán az adatvédelmi rendeletek áttekintésére?
- Az adatvédelmi rendeletekben találkozott már olyan fogalommal, amit előtte nem ismert? Ha igen mi az?
- Véleménye szerint mik tartoznak a személyes adatok közé?
- Véleménye szerint mik tartoznak a különleges személyes adatok közé?
- Ön szerint melyik a legérzékenyebb személyes adat? (Csak egy típust nevezzen meg!)
- Az ön által ismert személyes adatok közül melyeket tartja a legfontosabbnak?
- Véleménye szerint a szolgáltatók betartják saját adatvédelmi rendeleteiket?
- Önnek mi jelentene garanciát személyes adatának védelme érdekében egy adatkezelőtől?
- Véleménye szerint ön találkozott már adatvédelmi incidenssel, vagy hanyag adatkezeléssel? Ha igen hol?
- Ön tárol személyes adatot okostelefonjában képként vagy jegyzetként?

8.1 Függelék: Kutatási kérdőív I/B általános kérdés (magánélet és társadalmi megítélés)

A kérdőívben feltett kérdések:

- Az ön munkáját az EU GDPR milyen területen befolyásolja?
- Az ön véleménye szerint a rendelet szabályai könnyen értelmezhető az adatvédelmi nyilatkozatokban/ adatkezelési tájékoztatókban? (Igen/Nem/Nem olvasom el őket)
- Ön szerint mi az adatvédelem? (maximálisan 2-3 mondatban fejtse ki/ nincs információm róla)
- Okoz-e bizonytalanságot azt eldönteni, hogy az ön munkahelyi tevékenysége milyen módon érintett a GDPR tekintetében?
- Részt vett-e korábban a GDPR rendeletről szóló oktatáson? Ha igen, akkor milyen módon?
- Milyen szankcióit ismeri a rendeletnek? (Elsősorban pénzügyi vonatkozásban)
- Hallott-e már a nyílt sajtóból adatvédelmi incidens miatt kiszabott büntetésről?
- Ön szerint mi határozza meg a bírság összegét?
- Ön szerint melyik hatóság felelősségi köre az adatvédelmi rendelet betartása és betartatása Magyarországon?
- Véleménye szerint kerültek-e már illetéktelen kézbe az ön adatai? (Igen/Nem/Nem tudom)
- Véleménye szerint a kiberbűnözők tevékenysége valós veszélyt jelent a személyes adatok vonatkozásában?
- Ön szerint a GDPR hatályba lépését követően a szolgáltatók hatékonyabban védik a tárolt személyes adatokat?

1. Rövidítések jegyzéke

ACN - anonymous communication network - Az anonim kommunikációs hálózatok működése technikai megoldásokra épül, amelyek elrejtik a kommunikáló felek IP-címét, helyzetét, illetve más azonosításra alkalmas adatát.

APT - Advanced Persistent Threat - csoportok olyan kiberbűnözői szervezetek, amelyek hosszú távú, célzott támadásokat hajtanak végre az áldozataik ellen, akik jellemzően nagyobb gazdasági szervezetek és államok

CERT-EU - Computer Emergency Response Team for the EU institutions, bodies and agencies - A CERT-EU elsődleges feladata az Európai Unió intézményeinek, szervezeteinek és ügynökségeinek informatikai rendszereit érintő kibertámadások, fenyegetések, sebezhetőségek megelőzése, észlelése, elemzése és kezelése.

DoS - Denial of Service – szolgáltatás megtagadásos támadás – Az elkövető szándékosan túlterheli egy rendszer erőforrásait annyi kéréssel, hogy az lelassuljon vagy teljesen elérhetetlenné váljon a valódi felhasználók számára.

DDoS - Distributed Denial of Servic - elosztott szolgáltatásmegtagadásos támadás - egy olyan kibertámadás, amely során nagyszámú, elosztott forrásból származó forgalommal terhelik túl egy informatikai rendszert, hogy az szolgáltatásait részben vagy teljesen elérhetetlenné tegye.

DGA - Data Governance Act – DGA, 2022/868/EU

DSA - Digital Services Act – DSA, 2022/2065/EU

ENISA - European Union Agency for Cybersecurity - Európai Unió Kiberbiztonsági Ügynöksége - Az ENISA egy uniós ügynökség, amely támogatja az Európai Unió tagállamait és intézményeit a kiberbiztonság megerősítésében.

EUROPOL - Európai Unió Rendőrségi Hivatala

EUROPOL IOCAT - Ez az EUROPOL által fejlesztett technikai eszköz vagy platform**.**

FIRE - Future Internet Research and Experimentation – Az Európai Bizottság az FP7 és Horizon 2020. keretprogramokon belül indult, és a kutatás célja a egy Kutatási és tesztelési infrastruktúra létrehozása a jövő internettechnológiái számára.

GENI - Global Environment for Network Innovations - A National Science Foundation (NSF) indította, és célja a hálózati és elosztott rendszerek új generációjának fejlesztése és tesztelése.

GUID - Globally Unique Identifier - A GUID célja, hogy különféle rendszerek és alkalmazások között is biztonsággal lehessen azonosítani objektumokat anélkül, hogy azok véletlenül összekeverednének.

ICS - Industrial Control System - ICS-nek neveznek ipari környezetben minden olyan informatikai rendszert, amelyek felügyeleti és adatgyűjtő feladatokat látnak el, ugyanígy ICS-nek tekintik az elosztott irányító rendszereket (DCS) és a PLC-ket is.

IPv6 - Internet Protocol version 6 - Az IPv6 az internetes címzési rendszer legújabb verziója, amelyet azért hoztak létre, mert a régi IPv4-es címek kimerülnek. Az IPv6 protokoll közel $3{,}4\times10^{38}$ darab címet tud kiosztani.

IT – information technologies - információs technológia

ITC - Information and Communications Technology - információ- és kommunikációtechnológia.

IoT - Internet of Things – dolgok internete[156] a "dolgok internete" magyar fordítása, olyan eszközök, rendszerek és tárgyak hálózata, amelyek képesek adatokat gyűjteni, továbbítani és fogadni az interneten keresztül.

UNDP- United Nations Development Programme - Az UNDP több mint 170 országban és területen működik, és olyan projekteket indít, amelyek a gazdasági fejlődést, a társadalmi egyenlőséget és a környezet védelmét célozzák.

2FA - Two-Factor Authentication**:** kétfaktoros hitelesítés kifejezést jelenti. Ez egy biztonsági mechanizmus, amely két különböző azonosítást alkalmaz egy felhasználó hitelesítéséhez

RDP - egy Microsoft által létrehozott szabadalmazott protokoll, amely lehetővé teszi a távoli kapcsolatok létrehozását számítógépek között. Az RDP segítségével a felhasználók megtekinthetik és interakcióba léphetnek egy távoli gép asztali felületével, mintha fizikailag jelen lennének.

Privacy-Enhancing Technologies – PETs - A PET olyan technológiák, eszközök és módszerek összessége, amelyek célja a felhasználók személyes adatainak védelme az adatgyűjtés, adatfeldolgozás és adattárolás során, minimalizálva az adatvédelmi kockázatokat.

SDN - Specially Designated Nationals and Blocked Persons List – Olyan személyeket, szervezeteket és vállalatokat tartalmaz, akikkel az amerikai állampolgárok és vállalatok nem folytathatnak üzleti

[156] ASHTON, Kevin: That 'Internet of Things' Thing In the real world, things matter more than ideas, 2009. június 22, http://www.itrco.jp/libraries/RFIDjournalThat%20Internet%20of%20Things%20Thing.pdf

tevékenységet, mivel kapcsolatban állhatnak terrorizmussal, kábítószer-kereskedelemmel, pénzmosással vagy más nemzetbiztonsági kockázatokkal.

SQL - Structured Query Language - relációsadatbázis-kezelők lekérdezési nyelve. Ezek táblagyűjteményeket tárolnak, és táblázatos, oszlopok és sorok formájában rendszerezik a strukturált adathalmazokat, mint a számolótáblák.

WiFi - Wireless Fidelity: egy vezeték nélküli technológia, amely lehetővé teszi az internethez való csatlakozást és az adatátvitelt rádióhullámok segítségével. Szabványai. 802.11b/g/n**,** 802.11ac, 802.11ax, Wi-Fi 6E.

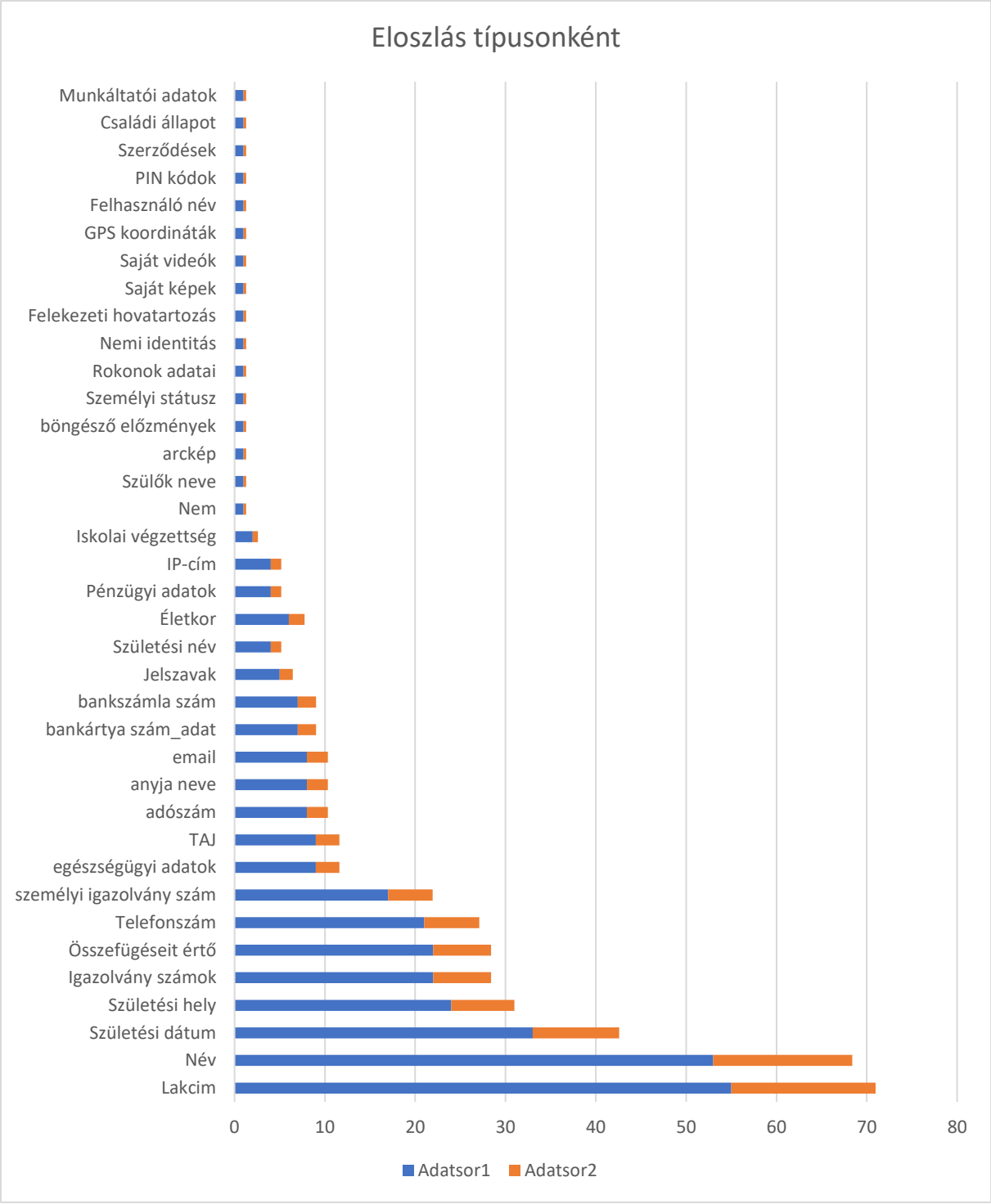
1. sz. melléklet

Adatvédelmi ismeretek mérésének célja- részletes eredmények

Az **I/A** kérdőívet **170** személy töltötte ki a 2022-23-as kutatás során. A megkérdezettek nem minden kérdésre tudták a választ, a 170 db a teljesen vagy részben kitöltött kérdőívekre összesített számát adja. A hipotézisek igazolásához csak a releváns kérdések kerültek részletes feldolgozásra az alábbiak szerint:

I/A 9. kérdése: „A Véleménye szerint mik tartoznak a személyes adatok közé?" kérdésre **149** számú személy válaszolt, azaz a megkérdezettek **87,65**%-a. Ebből 10 fő nem tudta a választ további 5 pedig nem tudott érdemi választ adni, azaz gyakorlatilag 78,82% adott felhasználható eredményt.

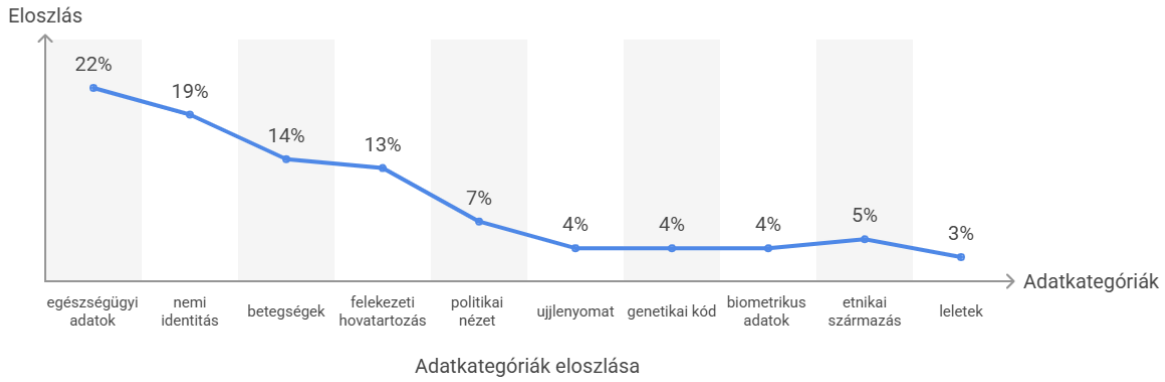
A megkérdezettek a „**lakcím", „név", „születési dátum" , „születési hely", „igazolvány számok", „telefonszám", „személyi igazolvány szám", „egészségügyi adatok", „társadalom biztosítási azonosító jel", „adóazonosító", „anyja neve", „elektronikus levél cím", bankkártya szám/bankkártyán szereplő adatok", „bakszámla szám", „jelszavak", „ születési név", „életkor", „pénzügyi adatok", „IP-cím", „iskolai végzettség", „nem", „szülők neve", „arckép", „böngésző előzmények", „személyi státusz", „rokonok adatai", „nemi identitás", „felekezeti hovatartozás", „saját képek", „saját videók", „GSP-koordináták", „felhasználó nevek", „PIN kódok", „családi állapot", munkáltató adatai"** fogalmakat azonosították, mint személyes adat. Eloszlásuk előfordulásuk szerint osztályozva és rangsorolva az alábbiak szerint alakult.



Jól látható a fenti adatokból, hogy a megkérdezettek jelentős része nem rendelkezik alapvető ismeretekkel arról, hogy mik tartoznak a személyes adatok körébe. Több esetben csoport fogalmakat említenek, vagy olyan egyéb fogalmat, ami nem tartozik a személyes adatok körébe. Alapvetően az eloszlásból látható, hogy szinte minden esetben egy példára gondoltak a megkérdezettek. Összesen a megkérdezettek **6,9%-a** fogalmazta meg azt, hogy a személyes adat minden olyan információ, amely valamely **azonosított vagy azonosítható élő**

személlyel kapcsolatos. Mindazon információk, amelyek összegyűjtése egy bizonyos személy azonosításához vezethet, ugyancsak személyes adatnak minősülnek.

„Véleménye szerint mik tartoznak a különleges személyes adatok közé?” kérdésre **119** személy válaszolt, azaz a megkérdezettek **70**%-a. A megkérdezettek a megkérdezettek **egészségügyi adatok, nemi identitás, egészségügyi állapot, felekezeti hovatartozás, politikai hovatartozás, újlenyomat, genetikai kód, biometrikus adatok, etnikai származás, egészségügyi dokumentumok** azonosították, mint különleges személyes adat.



25. ábra Adatvédelmi ismeretek mérése Forrás: saját kutatási adatok

A fenti adatokból jól látható, hogy a megkérdezettek túlnyomó többsége nem ismeri pontosan mi is tartozik a fogalomkörbe.

„*Ön szerint melyik a legérzékenyebb személyes adat*?”

A megkérdezetettek jellemzően pénzügyi szektort érintő adatokat soroltak ebbe a kategóriába, feltehetően a saját egzisztenciális állapotukat vették alapul és emiatt ezt tartották a legnagyobb kockázati tényezőnek.

„*Az ön által ismert személyes adatok közül melyeket tartja a legfontosabbnak*?” A megkérdezetettek jellemzően pénzügyi szektort érintő adatokat soroltak ebbe a kategóriába, feltehetően a saját egzisztenciális állapotukat vették alapul és emiatt ezt tartották a legnagyobb kockázati tényezőnek.

„*Véleménye szerint kerültek-e már illetéktelen kézbe az ön adatai*?” kérdésre a válaszadók 8, 82% válaszolt „igen”-nel.

„*Véleménye szerint a kiberbűnözők tevékenysége valós veszélyt jelent a személyes adatok vonatkozásában?”* kérdésre a válaszadók 100 % válaszolt „igen”-nel.

2. sz. melléklet (korszerű katonai kiképző rendszerekhez)

Személyes azonosító adatok:

Teljes név

Születési név

Születési dátum

Születés helye

Nem

Állampolgárság

Cím és elérhetőségek

Levelezési cím

Online elérhetőség

Szolgálati adatok:

Rendfokozat

Szolgálati szám

Beosztás

Beosztás azonosító

Magasabb egység és katonai alakulat

Egészségügyi adatok:

Orvosi vizsgálatok eredményei

Betegségek, sérülések és kezelések története

Fizikai alkalmasság vizsgálat

FÜV

Kiképzési adatok:

Iskolai végzettség

Egyéb végzettség

Kiképzési programok részvételi adatai

Teljesítményértékelések

Eredmények és minősítések

Képzési előzmények és tanfolyamok

Pszichológiai és mentális egészség adatok:

Pszichológiai tesztek eredményei

Mentális állapot felmérései

Stresszkezelési képességek

Biometrikus adatok:

Ujjlenyomatok - Az egyén ujjáról vett egyedi minták.

Arcfelismerési adatok - Az egyén arcvonásainak digitális képe és jellemzőinek leképezése.

Írisz szkennelés - Az egyén szivárványhártyájának egyedi mintázata.

Retinaszkennelés -Az egyén retinájának egyedi érrendszeri mintázata.

DNS minták - Az egyén genetikai anyagából nyert egyedi genetikai kód.

Kéznyomatok - Az egyén kézfelületének egyedi mintázata, beleértve a tenyér vonalait és a kéz kontúrját.

Vénaszkennelés - Az egyén kezének vagy ujjainak vénarendszerének egyedi mintázata.

Hangazonosítás - Az egyén beszédhangjának egyedi jellemzői, beleértve a hangmagasságot, hangszínt és ritmust.

Aláírásdinamika -Az egyén aláírásának egyedi jellemzői, beleértve az írás nyomását, sebességét és a mozdulatok sorrendjét.

Járásminta - Az egyén járásának egyedi mintázatai, beleértve a lépések hosszát, ritmusát és dinamikáját.

Füljellegzetességek - Az egyén fülének formája és egyedi jellemzői.

Szívritmus mintázatok -Az egyén szívverésének egyedi mintázata és ritmusa.

Képzési és teljesítményadatok:

Folyamatos teljesítmény monitorozás (pl. lőgyakorlatok eredményei, fizikai állóképességi tesztek)

Szimulációs gyakorlatok adatai

Biztonsági és hozzáférési adatok:

Belépési és kilépési időpontok

Hozzáférési jogosultságok és előzmények

3. sz. melléklet (webshop GDPR megfelelősség példa)

```
<!DOCTYPE html>
 <html lang="hu">
 <head>

<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Webshop - GDPR kompatibilis</title>
<style>
        .cookie-banner {
        position: fixed; bottom: 0;
        width: 100%;
        background-color: #333;
        color: white; text-align:
        center; padding: 15px;
        display: none; }

        .cookie-banner button {
        background-color: #4CAF50;
        color: white; border: none;
        padding: 10px;
        cursor: pointer; }

        .consent-checkbox {
        margin-top: 10px; }

                </style>
        </head>
         <body>
                <header>
                <h1>Webshop</h1>
                <nav>
                 <a href="#">Kezdőlap</a> |
                <a href="#">Termékek</a> |
                 <a href="#">Kapcsolat</a> |
                <a href="#" id="privacy-policy-link">Adatkezelési tájékoztató</a>
        </nav>
                 </header>
                <main>
                 <h2>Regisztráció</h2>
                 <form id="registration-form">
                <label for="name">Név:</label>
                <input type="text" id="name" name="name" required><br><br>
                <label for="email">Email:</label>
                <input type="email" id="email" name="email" required><br><br>

                <div class="consent-checkbox">
                <input type="checkbox" id="gdpr-consent" name="gdpr-consent"
        required>
```

```
                <label for="gdpr-consent">Elfogadom az <a href="#" id="privacy-
            link">Adatkezelési tájékoztatót</a></label>
                </div><br>
                <button type="submit">Regisztráció</button>
                 </form>
                 </main>

                <!-- Sütik kezelése (Cookie banner) -->
                <div class="cookie-banner" id="cookie-banner"> Ez a weboldal sütiket
            használ a legjobb élmény érdekében. Kérjük, fogadd el a sütiket!
                <button id="accept-cookies">Elfogadom
                </button> <button id="decline-cookies">Elutasítom</button>
                </div>

<footer>
<p>&copy; 2024 Webshop. Minden jog fenntartva.</p>
</footer>

<!-- JavaScript a GDPR és Cookie kezeléshez --> <script>
 // Sütik kezelése
document.addEventListener("DOMContentLoaded", function() {
        const cookieBanner = document.getElementById('cookie-banner');
        const consentGiven = localStorage.getItem('cookie-consent');

if (!consentGiven) {
cookieBanner.style.display = 'block'; }
document.getElementById('accept-cookies').addEventListener('click',        function()        {
localStorage.setItem('cookie-consent', 'true');
cookieBanner.style.display = 'none'; });
document.getElementById('decline-cookies').addEventListener('click',        function()        {
cookieBanner.style.display = 'none'; });
});
// Form validálása GDPR checkbox alapján
        document.getElementById('registration-form').addEventListener('submit',
function(event) { const gdprConsent = document.getElementById('gdpr-consent').checked;
        if (!gdprConsent) {
         alert("El kell fogadnod az adatkezelési tájékoztatót a regisztrációhoz!");
event.preventDefault(); } });
        // Adatkezelési tájékoztató megnyitása (példa) document.getElementById('privacy-
link').addEventListener('click', function(event) {
        event.preventDefault();
        alert("Az Adatkezelési tájékoztató ide kattintva olvasható."); });
        </script>
        </body>
        </html>
```

Hivatkozások

[1] W. Kluwer, *1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról,* Budapest: Wolters Kluwer , közlönyállapot (1992.XI.17.).

[2] P. Bernal, Internet Privacy Rights, Cambridge: Cambridge University Press, 2014 pp 6-7.

[3] EU-LEx, „https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32016R0679," EUR-LEX, EU, 2016.

[4] N. Ágnes, Több-módszertanú és vegyes módszertanú kutatások, korreferátum simon judit „kutatás-módszertani trendek a marketingben" című tanulmányához, Budapest: XLVII. ÉVF. 2016. MARKETINGTUDOMÁNYI KÜLÖNSZÁM / ISSN 0133-0179, 2016.

[5] K. László, Kiberbiztonság és Startégia, Budapest : Dialóg Campus Kiadó p. 9, 2018.

[6] D. M. M. S. m. A. m.-a. Danny Azucar, „Predicting the Big 5 personality traits from digital footprints on social," *Elsevier,* %1. számPersonality and Individual Differences 1, pp. 151-159, 2018.

[7] D. K. Károly, KIBERVESZÉLY ÉS A MAGYAR HONVÉDSÉG, Budapest: Hadmérnök, VII. Évfolyam 4. szám.

[8] EUROPOL, „EUROPOL IOCTA 2024," Publications Office of the European Union, DOI:10.2813/442713, Luxembourg, 2024.

[9] ENISA, ENISA THREAT LANDSCAPE 2024 July 2023 to June 2024 ISBN: 978-92-9204-675-0, DOI: 10.2824/0710888, ENISA, 2024 pp 62-64.

[10] Mérnökkapu, „Mi az a kiberbiztonsági incidens és hogyan kell rá reagálni?," 2023.

[11] N. K. Intézet, „Incidenskezelés," NKI, NKI, 2025.

[12] Ü. András, „Kiberbiztonsági incidensek trendjei a személyes adatok kiszivárgásának tükrében," *BLA Doktori Ösztöndíjprogram Tanulmánykötet 2023/2024,* pp. pp 112-132, 2024.

[13] D. K. K. PhD, „A HONVÉDELMI CÉLÚ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK FEJLESZTÉSÉHEZ SZÜKSÉGES TOVÁBBLÉPÉST MEGALAPOZÓ VIZSGÁLAT – EGY ZÖLD KÖNYV KIALAKÍTÁSÁNAK TÁMOGATÁSA," Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék, Budapest, 2022.

[14] I. O. DATA, „Data Science in the Military: An Overview," INSTITUTE OF DATA, USA, DECEMBER 12, 2023.

[15] K. Károly, „Az elektronikus információvédelem szabályozási kérdései a közelmúltban," *Hadmérnök,* pp. pp. 203-2013, VIII. Évfolyam 1. szám.

[16] CCDCOE, „https://ccdcoe.org/,” NATO, 14 01 2025. [Online]. Available: https://ccdcoe.org/research/data-protection-and-privacy-in-armed-conflict/. [Hozzáférés dátuma: 15 01 2025].

[17] I. -. UK, „National security and defence exemption: a guide,” ICO, Wilmslow, 2023. május 13..

[18] L. M. S. P. B. L. 2. T. E. H. D. R. L. M. E. S. Loryana L. Vie, „The U.S. Army Person-Event Data Environment: A Military–Civilian Big Data Enterprise,” *Big Data,* %1. kötetVolume 3 , %1. számNumber 2, pp. pp 67-79, 2015.

[19] B. Vincent, „DOD notifying more than 26,000 people who may be impacted by a year-old data breach,” *DefenseScoop,* p. 1, 13 február 2024 .

[20] A. Forsyth, „MoD data breach: UK armed forces' personal details accessed in hack,” *BBC on-line,* p. 1, 7 május 2024.

[21] *2012. évi I. törvény a munka törvénykönyvéről,* 2012.

[22] *2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól,* 2005.

[23] *2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről,* 2001.

[24] *2011. évi CXC. törvény a nemzeti köznevelésről,* 2011.

[25] *2011. évi CCIV. törvény a nemzeti felsőoktatásról,* 2011.

[26] *2003. évi C. törvény az elektronikus hírközlésről,* 2003.

[27] *2012. évi XLI. törvény a személyszállítási szolgáltatásokról,* 2012.

[28] P. O. a. P. Hinton, „Goodbye Mr Chips?’Modernising Defence Training for the 21st Century,” Royal United Services Institute for Defence and Security Studies, Whitehall London SW1A 2ET United Kingdom, 2023.

[29] M. R. Future, „Military IoT Market Research Report - Forecast till 2023,” Market Reserch Future, Market Reserch Future, 2019.

[30] Ü. A. J. SZÁZADOS, „A SZEMÉLYES ADATOK VÉDELME A KIBERBIZTONSÁGI STRATÉGIÁK TÜKRÉBEN,” A Katonai Nemzetbiztonsági Szolgálat tudományos-szakmai folyóirata, Budapest, 2021. XX. évfolyam 3. szám pp 145-159.

[31] J. T. Jacobsen, „Cyber offense in NATO: challenges and opportunities - https://doi.org/10.1093/ia/iiab010,” in *InternationalAffairs*, University of Cambridge, Volume 97, Issue 3, May 2021, pp 703–720.

[32] S. Reza, „Emerging Threat: InfoStealer Malware Targets Oil & Gas Industry,” LinkedIn, LinkedIn, 2024.

[33] OFAC, „Russia-related Designations,” OFAC, 2022.

[34] Securitylab, „Банк России опроверг взлом систем украинскими хакерами,” securitylab.ru, securitylab.ru, 2022.

[35] Ü. A. József, „INFORMATION AND CYBER OPERATIONS OF THE RUSSIANUKRAINIAN CONFLICT, AND THE POSSIBILITIES, AND RISKS OF USING THE PERSONAL DATA,” *NATIONAL SECURITY REVIEW,* %1. kötet Issue 1/2023, p. 119, 2023.

[36] securitylab.ru, „ Банк России опроверг взлом систем украинскими хакерами , ноября,,” securitylab.ru, https://www.securitylab.ru/news/534653.php, 2022.

[37] A. Bezverkhyi, „MicroBackdoor Malware: Belarusian APT Group UNC1151 (UAC-0051) Targets Ukrainian Government,” *SocPrime,* p. 1, 23 március 2022.

[38] M. Sableman, „https://www.thompsoncoburn.com/,” Thomson Coburn LLP, 19 december 2018. [Online]. Available: https://www.thompsoncoburn.com/insights/blogs/internet-law-twists-turns/post/2018-12-19/why-we-permit-fake-identities-even-for-russian-disinformation-campaigns. [Hozzáférés dátuma: 20 november 2024].

[39] T. Jones, „Aura,” Aura, 8 december 2023. [Online]. Available: https://www.aura.com/learn/types-of-social-engineering-attacks. [Hozzáférés dátuma: 20 11 2024].

[40] d. V. Viktor, „Jogiforum,” 22 junius 2022. [Online]. Available: https://www.jogiforum.hu/wp-content/uploads/2022/07/voros-viktor_gdpr_cimlappal.pdf. [Hozzáférés dátuma: 20 11 2024].

[41] K. M. a. S. Gunaydin, Research using qualitative, quantitative or mixed methods and choice based on the research, Prefusion - https://journals.sagepub.com/home/prf, 2014.

[42] M. Nikolett, „GDPR – Előkelő helyen a magyar büntetéskiszabás,” Magyar Nemzet, Budapest, 2023. 08. 31..

[43] d. S. Júlia, „Az információs jogok kialakulása, fejlődése és társadalmi hatása,” Pécsi Tudomány Egyetem, Budapest, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskolája, Budapest, 2011. július 1..

[44] H. H. a. C. Raab, „Ethical Dimensions of the GDPR,” *SSRN,* %1. kötet, összesen: %2Commentary on the General Data Protection Regulation, Cheltenham: Edward Elgar (2018, Forthcoming), pp. pp 12-15, 2018 july 30.

[45] J. K. A. G. Risa Arai, „Legal identity and data protection in modern societies,” EUDP, 25 október 2023. [Online]. Available: https://www.undp.org/blog/legal-identity-and-data-protection-modern-societies. [Hozzáférés dátuma: 11 november 2024].

[46] E. U. A. f. F. R. -. FRA, „Az Európai Unió Alapjogi Chartája 7. cikkA magán- és a családi élet tiszteletben tartása,” Az Európai Unió Hivatalos Lapja C 303/17 - 14.12.2007, Brüsszel, 2007.

[47] D. A. Á. L. -. Ü. A. József, Adastvédelmeről alapfokon, Budapest: Katonai Nemzetbiztonsági Szolgálat, 2023.

[48] P. Ruffio, „Dark Web Price Index 2022,” Privacy Affairs, Privacy Affairs, 2023 june 10.

[49] M. Zoltan, „Dark Web Price Index 2023," Privacy Affairs, Privacy Affairs, 2023 april 23.

[50] J. H., „Dark web statistics & trends for 2024," PreyProject, PreyProject, 2024.

[51] M. Hodson, „Dark Web Price Index 2025," PrivacySharks, 2022.

[52] *CERT-EU PROTECTION OF PERSONAL DATA Record reference: DPR-EC-07167.2,* 2022-2024.

[53] E. U. A. F. CYBERSECURITY, „ENGINEERING PERSONAL DATA PROTECTION IN EU DATA SPACES," ENISA, Brussels ISBN 978-92-9204-650-7, DOI 10.2824/210862, 2024 january.

[54] HackRead, „https://hackread.com/," HackRead, [Online]. Available: https://hackread.com/data-breach-national-public-data-records-ssns-dumped/. [Hozzáférés dátuma: 21 11 2024].

[55] N. P. Data, „Security Incident," National Public Data, National Public Data, 2024.

[56] TechCrunch, „TechCrunch," TechCrunch, 22 Julius 2024. [Online]. Available: https://techcrunch.com/2024/07/12/att-phone-records-stolen-data-breach/. [Hozzáférés dátuma: 21 november 2024].

[57] PrivacyRights, „PrivacyRights.com," PrivacyRights.com, 11 12 2024. [Online]. Available: https://privacyrights.org/data-breaches. [Hozzáférés dátuma: 11 12 2024].

[58] K. Finklea, „Dark Web," Congressional Research Service, 2017.

[59] E. PANNAH, „Cybersecurity in Electronic Commerce: Effect of Safeguarding Personal Data on Identity Theft," University of Maryland University College, November 2010.

[60] V.-M. Vargas, „ The new economic good: Your own personal data. An integrative analysis of the Dark Web DOI:https://doi.org/10.2478/picbe-2019-0107," 29 Nov 2019.

[61] A. G. János Besenyő, „THE EFFECT OF THE DARK WEB ON THE SECURITY," *JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES,* %1. kötet2021 Volume 11, 2021.

[62] B. Jamie, „Infiltrating the DarkNet, where criminals, trolls and extremist reign," NPR, 2015.

[63] M. B. R. M. a. M. R. Ciancaglini Vincenzo, „Below the surface: Exploring the DeepWeb," TrendMicro, TrendMicro, 2015.

[64] J. Eric, „The Dark Web Dilemma: Tor, Anonymity and on-line policing," Global Commission on Internet Governance Paper series No. 21., 2017.

[65] E. I. Dounia, N. ELKAMOUN és R. HILAL, „Study of the impact of the transition from IPv4 to IPv6 based on the tunneling mechanism in mobile networks," *ScienceDirect,* %1. kötetProcedia Computer Science 191 (2021) 207–214, pp. pp 208-213, 2021.

[66] I. A. Sugiu Takaaki, „Dark Web Content Analysis and Visualization," *IWSPA,* %1. kötet, összesen: %2Session: Security Analytics, Dark Web, p. 1, 2019.

[67] S. Retzkin, Learn what goes on in the Dark Web, and how to work with it, Birmingham - Mumbai: Packt, 2018.

[68] J. Mitchell, „SkyNews," SkyNews, 27 március 2024. [Online]. Available: https://news.sky.com/author/jenness-mitchell-881. [Hozzáférés dátuma: 12 12 2024].

[69] T. Team, „Top 10 Dark Web Forums," ThreatMon, ThreatMon, 2024 juni 21.

[70] Flare, „5 Key Dark Web Forums to Monitor in 2023," Flare https://flare.io/learn/resources/blog/dark-web-forums/, Flare, 2023 april 6.

[71] C. Team, „Chainalysis -," 16 04 2024. [Online]. Available: https://www.chainalysis.com/blog/crypto-drainers/. [Hozzáférés dátuma: 20 01 2025].

[72] Microsoft, „Microsoft Learn," 08 05 2024. [Online]. Available: https://learn.microsoft.com/hu-hu/azure/virtual-desktop/rdp-bandwidth. [Hozzáférés dátuma: 21 01 2025].

[73] ONION.LIVE, „TORUM," ONION.LIVE, 2025.

[74] U. D. o. P. A. -. O. o. P. Affairs, „United States Leads Seizure of One of the World's Largest Hacker Forums and Arrests Administrator," 22 04 2022.

[75] E. P. R. S. S. F. U. (STOA), „Blockchain and the General Data Protection RegulationCan distributed ledgers be squared with European data protection law?," 2019.

[76] B. a. t. G. D. P. R. European Parliemaent, „Can distributed ledgers be squared with European data protection , EPRS," European Parliamentary Research.

[77] *https://net.jogtar.hu/jogszabaly?docid=a1600679.eup,* 2025.

[78] M. Petzolt, „A quick dive into identity- and attribute-based encryption," Nord Security, 2023.

[79] S. R. A. R. P. FARSHID, „Design of a forgetting blockchain – A possible way to accomplish GDPR compatibility," 2019.

[80] M. A. A. G. C. Gautami Tripathi, „A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges," ISSN 2772-6622, 2023.

[81] S. H. K., „On-Chain vs. Off-Chain Crypto Transactions: A Comprehensive Guide," MudrexLearn.

[82] NAIH, „Nemzeti Adatvédelmi és Információszabadság Hatóság," [Online]. Available: https://www.naih.hu/suti-tajekoztato. [Hozzáférés dátuma: 24 01 2025].

[83] Google, „ads.google.com," [Online]. Available: https://ads.google.com/intl/en_uk/home/resources/gdpr/. [Hozzáférés dátuma: 24 01 2025].

[84] PERSONA, „Two-factor authentication (2FA) statistics," 2024.

[85] S. S. H. Z. H. L. C. L. D. Z. Zongda Wu, „An effective approach for the protection of user commodity viewing privacy in e-commerce website," ISSN 0950-7051,, 2021.

[86] M. Jackson, „The State of SQL Injection," Aikido, Aikido, 2024.

[87] A. M. K. R. K. R. THADURI Adithya, „Cybersecurity for eMaintenance in railway infrastructure: risks and consequences," *International Journal of System Assurance Engineering and Management, ,* %1. kötetVolume 10, %1. számIssue 2, p. pp. 149–159, 2019.

[88] Ü. A. J. s. Lévai Zsolt, „A vasúti közlekedés informatikai védelme," *Felderítő Szemle,* %1. kötetXIX. évfolyam, %1. szám2. szám, pp. pp 103-140, 2020.

[89] K. C. Kovács László, „Digitális Mohács," in *Egy kibertámadási forgatókönyv Magyarország*, Budapest, Nemzet és Biztonság, 2010. február, p. p. 48.

[90] Ü. A. J. Marlok Tamás, „Korszerű nemzeti taktikai kiképzőrendszer fejlesztésének kérdései, gdpr megfelelősége," *FELDERÍTŐ SZEMLE 1588-242X,* %1. kötet19, pp. pp 91-126, 2020.

[91] A. J. ÜVEGES, „INFORMATION AND CYBER OPERATIONS OF THE RUSSIANUKRAINIAN CONFLICT, AND THE POSSIBILITIES, AND RISKS OF USING THE PERSONAL DATA," *MILITARY NATIONAL SECURITY SERVICE - NATIONAL SECURITY REVIEW,* %1. kötetIssue 1/2023, p. p 119, 2023.

[92] D. K. Csaba, Rendező, *Kiberhadviselés az orosz–ukrán háború árnyékában.* [Film]. Magyarország: NKE, 2022.02.28.

[93] P. d. H. ZSOLT, Információs műveletek a kibertérben p 160, Budapest: Dialóg Campus Kiadó, 2018.

[94] CISA, *CISA Alert (AA22-047A) Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology,* 2023.

[95] C. Insight, *Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure,* CISA Insight, 2022.

[96] G. G. Agrima Srivastava, „Measuring Privacy Leaks in Online Social Networks," *IEEE XPLORE,* p. 2095, 2013.

[97] ,. O. B. S. B. Pradyumna Gokhale, „Introduction to IOT," IARJSET, International Advanced Research Journal in Science, Engineering and Technology, 2018.

[98] ENISA, „Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures," ENISA, 2017 p 12.

[99] C. LÁSZLÓ, „AZ OKOSKÖRNYEZET ÉS A BENNE REJLŐ BIZTONSÁGI," *Szakmai Szemle,* %1. kötet XX. évfolyam 3. szám, p. p 131 , 2022.

[100] J. Steward, „The Ultimate List of Internet of Things Statistics for 2021," Findstack, 2021.

[101] F. Duarte, „Number of IoT Devices (2024)," Exploding Topics, 2024. február 19..

[102] S. Poremba, „Will Weak Passwords Doom the Internet of Things (IoT)," Security Intelligence , 2020.

[103] Venminder, „Managing Internet of Things (IoT) Devices With Third-Party Risk Management," Venminder, 2023.

[104] A. Tóth, „Az Internet of Things rendszerek biztonsági kihívásai.," p. 101, 2023.

[105] M. Szabó, „welivesecurity," welivesecurity, 27 Augusztus 2024. [Online]. Available: https://www.welivesecurity.com/en/internet-of-things/old-devices-new-dangers-the-risks-of-unsupported-iot-tech/. [Hozzáférés dátuma: 02 12 2024].

[106] ENISA, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures,* ENISA, 2017 November.

[107] F. L. F. L. M. L. G. H. B.-H. Jonathan Tournier, „A survey of IoT protocols and their security issues through the lens of a generic IoT stack," ScienceDirect, Elsevier, 2021. december 16..

[108] Y. H. Hwang, „IoT Security & Privacy: Threats and Challenges," Software R&D Center, Samsung Electronics Co., LTD,, Singapore, 2015. április 14..

[109] P. M. C. ·. M. S. Kakkasageri, „Security and Privacy in IoT: A Survey," Springer Science+Business Media,, 2020.

[110] Ü. A. J. DR. ALBERT ÁGOTA, „AZ „IoT"-ESZKÖZÖK BIZTONSÁGA A SZEMÉLYES ADATOK TÜKRÉBEN," *Katonai Nemzetbiztonsági Szolgálat SZAKMAI SZEMLE,* %1. kötetm 2. szám , %1. szám1, pp. pp 148-149, XX. évfolyam.

[111] L. Xing, „Reliability in Internet of Things: Current Status and Future Perspectives," IEEE Xplore, IEEE Internet of Things Journal (Volume: 7, Issue: 8,, 2020 május 7.

[112] K. Csaba, „Az IoT katonai felhasználási lehetőségei és a fejlesztés irányai," *Hadmérnök,* %1. kötet4, pp. pp. 146-158., 2017.

[113] H. Zsolt, Információs műveletek a kibertérben, Budapest p. 98.: Dialóg Campus Kiadó,, 20018.

[114] ENISA, „Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures," ENISA, 2017.

[115] ENISA, „Security and Resilience of Smart Home Environments Good Practices and Recommendations," ENISA, 2015.

[116] D. N. I. e. –. D. A. Á. –. A. J. százados, „A felhőalkalmazások adatvédelmi kérdései a GDPR tükrében," *Felderítő Szemle,* %1. kötetXX. évfolyam, %1. szám1.szám, pp. pp. 151-180, 2021.

[117] P. M. VRÁNICS Dávid Ferenc, „Mission as a Service – Egy felhőalapú UAS megvalósítása," *Repüléstudományi Közlemények,* %1. kötet31. évfolyam, %1. szám3. szám, p. pp. 153–167., 2019.

[118] F. Gáspár, „A felhőszolgáltatások adatvédelmi kérdései – Az uniós adatvédelmi rendelet".

[119] 5. m. International Working Group on Data Protection in Telecommunications, „Working Paper on Cloud Computing – Privacy and data protection issues – „Sopot Memorandum"."

International Working Group on Data Protection in Telecommunications,, Sopot, Lengyelország, 2012.

[120] ENISA, „Cloud Security Guide for SMEs," ENISA, 2015.

[121] I. C. Office, „Data Protection Act Guidance on the use of cloud computing," ICO, 1998.

[122] D. P. Commission, „Guidance for Organisations Engaging Cloud Service Providers," Data Protection Commission, 2019.

[123] H. J. J. Takabi, „Security and Privacy Challenges in Cloud Computing Environments," IEEE Security and Privacy 8(6), pp 24–31, 2010.

[124] S. R. J. Rahul, „Security & Privacy Issues In Cloud Computing," International Journal of Engineering Research & Technology (IJERT) 2(3), 2013 március.

[125] L. V. M. V. L. Ayala, „Emerging Threats, Risk and Attacks in Distributed Systems: Cloud Computing," Innovations and Advances in Computer, Information, Systems Sciences, and Engineering. LNEE vol. 152, pp. pp 37–52, Springer, Heidelberg, 2013.

[126] A. C. F. T. a. A. P. Massimo Villari, „Data Reliability in Multi-provider Cloud Storage Service with RRNS," Springer, Berlin, Heidelberg, DICIEMA, University of Messina, 2013.

[127] J. G. a. B. Rumpe, „Models for Digitalization," *Software and Systems Modeling,* %1. kötet14, p. pp. 1319–1320, 2015.

[128] P. Paganini, „Spearphishing: A New Weapon in Cyber Terrorism,," Infosec (website), 2016. május 6..

[129] S. Sim, „Emerging Terrorist Threats: Everything, Everywhere, All at Once?in Emerging Technologies and Terrorism: An American Perspective, ed. Susan Sim et al," *Centre of Excellence Defence against Terrorism and US Army War College Strategic Studies Institute,* p. p. 17, 2024.

[130] C. Nelu, „Exploitation of Generative AI by Terrorist Groups,," International Centre for Counter-Terrorism (website), 2024. június 10..

[131] S. J. B. e. al, „Is AI-Generated Extremism Credible? Experimental Evidence from an Expert Survey," *Terrorism and Political Violence,* pp. pp. 1-17, 2024.

[132] H. Zsolt, Információs műveletek a kibertérben, Budapest: Dialóg Campus,, 2018, p. pp. 149–297.

[133] U. O. o. C.-T. a. U. I. C. a. J. R. Institute, „N Office of Counter-Terrorism and UN Interregional Crime and Justice Research Institute, Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes," UN Office of Counter-Terrorism and UN Interregional Crime and Justice Research Institute, UN, 2021.

[134] A. J. Uveges, „PROTECTION OF PERSONAL DATA IN THE VIEW OF ALLIED NATIONAL CYBER SECURTY STRATEGIES 2022-2023," *National Security Rewiev HU ISSN 2063-2908,* %1. kötet2, pp. pp. 119-134, 2023.

[135] E. Bizottság, „A Bizottság Közleménye: EURÓPA 2020 – Az intelligens, fenntartható és inkluzív növekedés,” Európai Bizottság, Brüsszel, 2010.

[136] E. Unió, „Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér. Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának,,” Európai Tanács, Brüsszel,, 2013.

[137] K. László, Kiberbiztonság és -stratégia, Budapest: Dialóg Campus Kiadó, 2018.

[138] A. J. ÜVEGES, „PROTECTION OF PERSONAL DATA IN THE VIEW OF ALLIED NATIONAL CYBER SECURTY STRATEGIES 2022-2023,” *National Security Rewiev,* %1. kötet2, pp. pp. 119-134, 2023.

[139] P. D. H.-G. K. Dr. Heiner Lasi, „Industry 4.0,” *Information Systems BISE – CATCHWORD,* p. 239–242, 2014.

[140] Kaspersky, „Dark web market trends: last year in review and projections for 2024,” Kaspersky Lab, January 17, 2024.