TDK-dolgozat

2023.

Fekete Heléna Lilla
Külkereskedelmi Kar

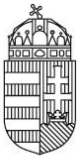
A BIZTONSÁG FÉL EGÉSZSÉG: A MAGYAR LAKOSSÁG BIZTONSÁGTUDATOSSÁGA AZ EGÉSZSÉGÜGYI ADATOKRA VONATKOZÓAN ÉS KIBERVÉDELEM AZ E-EGÉSZSÉGÜGYBEN

HALF OF HEALTH: SECURITY AWARENESS OF THE HUNGARIAN POPULATION REGARDING HEALTHCARE DATA AND CYBERSECURITY IN E-HEALTH

Dr. Nagy Milada

Kézirat lezárása: 2023. november 7.

„A KULTURÁLIS ÉS INNOVÁCIÓS MINISZTÉRIUM ÚNKP-23-1-4 KÓDSZÁMÚ ÚJ NEMZETI KIVÁLÓSÁG PROGRAMJÁNAK A NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS ALAPBÓL FINANSZÍROZOTT SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.”



KULTURÁLIS ÉS INNOVÁCIÓS MINISZTÉRIUM

TARTALOMJEGYZÉK:

TÁBLÁZATOK JEGYZÉKE:

ÁBRAJEGYZÉK:

BEVEZETÉS

Az egészségügy a jól működő társadalom egyik alappillére. Az egyik legfontosabb gazdasági ágazatként elengedhetetlen folyamatos fejlesztése, mely kiemelt feladat minden állam számára. Egy országot egészséges társadalommal lehet jól építeni. Erre ráépül a digitalizáció előretörése, mely robbanásszerű fejlődést jelent számos területen – köztük az egészségügyben is. A digitális innovációk rengeteg lehetőséget rejtenek magukban. Az online egészségügyi rendszerek megléte és használata egyre jelentősebb szerepet kap a mindennapokban, mind felhasználói, mind (egészségügyi) intézményi oldalról is.

A digitalizáció a pozitív tényezők mellett kockázatokat is hordoz magában. A kiberbiztonság kiemelten fontos az egészségügyi rendszerekre vonatkoztatva. Magánszemélyi oldalról, egészségügyi adataink személyes adatoknak minősülnek, így védelmük prioritást és magasfokú odafigyelést érdemel.

A biztonságérzet megteremtése számomra állandó cél az élet minden területén – így az online felületeken is. Az internet gyerekkorom óta jelen van az életemben. Ez lehet pozitív, míg más szemszögből nézve negatív, azonban a tudatos internethasználatot mindenféleképpen már fiatalon megtanultam. Személyes adataim védelmét sosem vettem félvállról, az internet használata során sem, azonban ez nem csak rajtam múlt. Az adatvédelem kéttényezős: függ a felhasználótól (adattulajdonos) és az adatkezelőtől is. Ezt a kettősséget kifejezetten érdekesnek és izgalmasnak találtam, és kutatási témának választottam.

Kutatásom során a hazai e-egészségügy feltérképezése mellett Magyarország lakosságának egészségügyi adataikra vonatkozó biztonságtudatosságát is igyekeztem felmérni. Az európai uniós és magyarországi szabályozások és az Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) vizsgálata jól szemlélteti az esetleges hiányosságokat, ágazati kihívásokat. A lakosság kiberbiztonsági cselekvéseit elemezve felismerhető az átlagos biztonságtudatosság mértéke és annak hiányosságai is.

A kutatásom során a következő kutatási kérdésekre kerestem a választ:

1. Milyen szinten valósul meg a kibervédelem a hazai e-egészségügyi rendszerekben, és ezek milyen további lehetőségeket rejtenek magukban?
2. Hol húzza meg a lakosság a magánszféra határát a személyes adatokra vonatkozóan?
3. Mennyire van tisztában a lakosság az egészségügyi adataik érzékenységével?

Az első kutatási kérdésemet szekunder, míg a második és harmadik kérdésemet primer kutatásom segítségével válaszoltam meg. Utóbbi kettőre az alábbi hipotéziseket állítottam:

H2.1: Az idősebb generációkba tartozó személyek kevesebb információt osztanak meg magukról.

H2.2: A magasabb iskolai végzettséggel rendelkezők több adatot tartanak személyesnek.

H3.1: Azok a személyek, akik gyakrabban látogatnak egészségügyi intézményeket, nagyobb valószínűséggel osztanak meg másokkal részletes információkat egészségi állapotukról.

H3.2: A magukat biztonságtudatosabbnak valló személyekre kevésbé jellemző, hogy saját egészségügyi állapotukat vagy egészségügyi dokumentumaikat, leleteiket megosszák másokkal az interneten keresztül.

Jelen dolgozat az Innovációs és Technológiai Minisztérium ÚNKP-23-1-I kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

MÓDSZERTAN

Kutatásom során szekunder és primer kutatási módszereket is alkalmaztam. A témához kapcsolódó magyar és idegennyelvű szakirodalom kritikai olvasata szerves részét képezte a kutatásomnak. A szakirodalom mellett a releváns törvények és rendeletek elemzése, értelmezése is szükséges volt a téma megfelelő feldolgozásához. A témakör több oldalról történő megvilágításához statisztikai adatok elemeztem, ezek többnyire a KSH és az Eurostat oldaláról származnak. Primer kutatásom egy kérdőíves felmérésből állt. A Google Form alapú kérdőív online volt elérhető és kitölthető. A felmérés kvantitatívnak minősül, a kitöltés anonim és önkéntes volt. Az összegyűjtött adatokat összesítettem, majd a Microsoft Excel és az IBM SPSS programok segítségével elemeztem őket különböző statisztikai módszerekkel.

1. AZ ADATVÉDELEM KIALAKULÁSA

1.1. Kezdeti lépések

A magánszféra védelme jelentősen átalakult az elmúlt két-három évtized során, köszönhetően a digitalizáció fejlődésének. Az új, hatékony információs technológiák különösen sérülékennyé tették, valamint szűkítették a magánszféra terét (Sziklay - Bendik, 2019). Míg a fogalom eredeti formájában a fizikai egyedüllét biztosítását foglalta magába, mára jelentésbeli tartalma kibővült. Az online térben saját, személyes adatainkon keresztül létezünk, mely fizikai testünk digitális lenyomataként is értelmezhető. Személyes minden olyan adat, amely bármely meghatározott, azonosított vagy azonosítható természetes személlyel kapcsolatba hozható (NAIH, é. n.). Ebből kifolyólag személyes adataink védelme egyenértékűvé vált a fizikai védelmünkkel.

Az adatvédelem (*data protection*) az 1970-es évektől terjedt el fogalmi használatban. Az első erre vonatkozó törvények meghatározása után szükségszerűvé vált a szabályok összehangolása, hogy a globalizáció részét képző nemzetközi adatáramlás ne ütközzön akadályokba. Ennek eredményeként 1980-ban megfogalmazták a Gazdasági Együttműködés és Fejlesztési Szervezet (OECD, Organisation for Economic Co-operation and Development) adatvédelmi irányelveit (OECD irányelvek a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról) (Jóri, 2009).

Az adatvédelmi jog csupán pár évtizedes múltra tekint vissza, ugyanakkor annál több változás történt benne a folyamatos fejlődés által. A szabályozás több generációra osztható fel, de a szakirodalom nem jutott eddig egységes döntésre ezek határairól. Csoportosíthatóak a jogforrások a számítógépes rendszerek, hálózatok fejlődése vagy a szabályozások területi hatásköre alapján is. Ugyanakkor a generációs felosztásnál valójában fontosabb a szabályozások jellemzőit és fejlődési tendenciáit megfigyelni (Szőke, 2013).

1.2. A nemzetközi szervezetek, mint az adatvédelem megalapozói

A Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) régóta központi szereplőként van jelen a személyes adatok védelmére vonatkozó politikák kidolgozásában. Az 1980-ban kiadott OECD Adatvédelmi Irányelvek (OECD Privacy Guidelines) volt az első, nemzetközileg elfogadott, egységes szabályozás erre a szakterületre vonatkozóan. Ezek az irányelvek a magánélet védelmére és a személyes adatok határokon átívelő áramlására vonatkoznak. 2013-ban megújították a korábbi rendelkezéseket, javítva az esetleges hiányosságokat (OECD, é. n.).

Az adatvédelmi szabályozások kezdetben eltérően alakultak ki Nyugat- és Kelet-Közép-Európában. Az adatfeldolgozás és -tárolás végtelen tárházát a nyugati demokratikus országokban az 1970-es évektől kezdték el felfedezni. Az addigi technológia központú gondolkodás a nyolcvanas évektől kezdett el megváltozni, az adatalany fogalmi megjelenésével. (Sziklay - Bendik, 2019). Az adatalany „*bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül, vagy közvetve – azonosítható természetes személy*" (NAIH, é.n.). A kelet-közép-európai országokban a rendszerváltás idején került előtérbe az adatvédelem kérdése, mint annyi más állampolgári és emberi jogi elem (Sziklay - Bendik, 2019).

Az 1990-es évek végére kialakult az adatvédelem európai egységes jogi szabályozása. Világszinten nézve az Európai Unió rendelkezik a legerősebb jogi védelemmel ezen a területen. Ennek egyik fő oka, hogy az Unión belüli gazdasági együttműködést ne nehezítsék meg az eltérő tagállami szabályozások, azaz nem a polgárok személyes védelme szolgált elsődleges motivációként (Révész, 2013). Az uniós adatvédelmi irányelvek erőteljes hatást gyakoroltak más országokra: befolyásolta többek között Új-Zéland és Hongkong jogalkotását, valamint mintaként szolgált Dél-Amerikában is (Jóri, 2009).

Az Unió rendeletei azonban nem a digitális térre fókuszáltak, így a 2000-es évektől kezdődő technológiai és társadalmi változások újabb kihívások elé állította az európai uniós szabályozást (Szőke, 2013). A 2002-es szabályozási csomag szolgált a felhasználók adatainak védelmére vonatkozó szabályozás fejlesztésére. Az eddig meglévő szabályok mellé bekerülő Adatvédelmi Irányelv rendelkezései – eltérően a korábbiaktól – már a jogi személyekre is kiterjednek. Az Adatvédelmi Irányelv a nyilvánosan elérhető elektronikus hírközlési szolgáltatók által végzett adatkezelést szabályozza, rendelkezik többek között az előfizetőkre és felhasználókra vonatkozó forgalmi adatok titkosságáról, a szolgáltatók adatvédelmi kötelességeiről, valamint a hívószám-azonosítás feltételeiről (Kende, 2015).

A személyes adatok védelme alapvető joggá vált az uniós jogban 2007-ben, a Lisszaboni Szerződés aláírásával (Európai Tanács, é. n.a). Az Európai Unió Alapjogi Chartája ezt a következőképp írja le:

„*(1) Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.*

(2) Az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni.

*(3) E szabályok tiszteletben tartását független hatóságnak kell ellenőriznie" (*CFREU, 2009, 8. cikk).

2016-ban fogadták el az EU Általános Adatvédelmi Rendeletét (GDPR – General Data Protection Regulation), amely hatalmas előrelépésként szolgált az addigi szabályozásokhoz képest. Az Unió tagállamainak két éve volt implementálni az új rendeletet saját országaikban (EDPS, é. n.). Ez a rendelet az alapvető jogok megszilárdítása mellett a kereskedelemre is pozitív hatással van. Egyetlen, átfogó jogszabályként megszüntette a tagállamok közötti széttagoltságot és csökkentette a különböző szabályozásból fakadó adminisztratív terhek mértékét (Európai Bizottság, 2022). A GDPR egyértelműen meghatározza a személyes és a különleges adatok körét, a kezelésükre vonatkozó elveket. Rendelkezik arról, hogy az érintett adatait csak írásbeli hozzájárulás után lehet kezelni, amely hozzájárulást az érintett bármikor vissza is vonhat. A törvény 8. cikkében külön foglalkozik a gyermekek hozzájárulásával, és kijelenti, hogy 16. életévét be nem töltött gyermek esetén a gyermek feletti szülői felügyeletet gyakorló hozzájárulása és engedélyezése szükséges. A GDPR továbbá összefoglalja az érintett jogait, valamint az adatkezelő és adatfeldolgozó feladatait és kötelezettségeit. Létrehozta az Európai Adatvédelmi Testületet, mint jogi személyiséggel rendelkező uniós szervet. A Testület biztosítja az Általános Adatvédelmi Rendelet egységes alkalmazását, így bármikor ellenőrizheti és vizsgálhatja a rendelet megfelelő használatát. A GDPR bármilyen, a rendeletet megszegő cselekedetet szigorúan büntet (GDPR, 2016).

1.3. Magyarország

A szovjet megszállás alatti Magyarországra később értek el az az újkeletű szabályozások, így az adatvédelem kérdésköre is. Az 1980-as évekig semmilyen jogszabály nem létezett az állami szervek állampolgárokra vonatkozó adatkezelésére. Szervezett és nyilvános adatgyűjtés az állami népesség nyilvántartásra volt csak jellemző (Sziklay - Bendik, 2019).

Az első nagy áttörést az *1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról* (rövidítve: Avtv.) jelentette. A törvény egyértelműen definiálta a *személyes adat, különleges adat, közérdekű adat* és további fogalmakat, valamint kitért az adatkezelésre és -továbbításra. Összefoglalta az érintettek jogait és ezek érvényesítési módjait. A törvény egyik legfontosabb rendelkezéseként elrendelte egy adatvédelmi biztos (ombudsman) kinevezését. Az adatvédelmi biztos:

„a) ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabály megtartását;

b) kivizsgálja a hozzá érkezett bejelentéseket;

c) gondoskodik az adatvédelmi nyilvántartás vezetéséről" (Avtv. 1992, 24.§,).

Az adatvédelmi ombudsman jogintézménye 2012. január elsején szűnt meg az új Alaptörvény hatálybalépésével.

A magyar szabályozások fokozatosan egyesültek az uniós rendelkezésekkel. Az 1998. évi VI. törvény a magyar jog részévé tette az Európa Tanács 108. adatvédelmi egyezményét (Sziklay - Bendik, 2019). *Az egyének védelméről a személyes adatok gépi feldolgozása során* című egyezmény célja, hogy nemzetiségtől és lakóhelytől függetlenül minden egyes fél területén biztosítva legyenek az egyének jogai és alapvető szabadságjogai, középpontba helyezve a magánélethez való jog tiszteletbe tartását a személyed adatok gépi feldolgozása során (1998. évi VI. tv.).

Az Egyezmény alkalmazása a köz- és a magánszektorra is kiterjed. Szabályozza a személyes és a különleges adatok feldolgozási és tárolási lehetőségeit. Az automatizált adatállományok fokozott ellenőrzését rendelte el, valamint az adatalanyoknak további jogokat biztosított az eddigieken felül. Kitér az országhatárokat átlépő adatáramlásra is, ezzel könnyítve a külföldi lakhelyű adatalanyok életét, illetve javítva az országok közötti együttműködés szintjét. Létrehozta továbbá a Tanácsadó Bizottságot, amely felügyeli az Egyezmény működését a gyakorlatban (1998. évi VI. tv.).

Az adatvédelem újraszabályozása a 2011. évi CXII. törvényben valósult meg, mely az információs önrendelkezési jogról és az információszabadságról szól (rövidítve: Info tv..). Az új törvény elismerte az addigi magyarországi szabályozás sikerességét, azonban időszerűnek gondolták megújítását (Lakatos-Nagy, 2012). A törvény minden személyes és közérdekű adatra kiterjed, de csak természetes személyekre érvényes. Az Info tv. bizonyos fejezeteiben érezhetően a korábbi Avtv. rendelkezéseiből inspirálódott, azonban annál egy jóval részletesebb, az új digitális korszak kihívásaival szembenéző törvény lett. Olyan szegmensek is meghatározásra, szabályozásra kerültek, amelyek korábban még nem szerepeltek. Ilyen *A személyes adatokkal összefüggő jogok érvényesítése az érintett halálát követően* című 9. cikk is (Iötv., 2011).

1.4. A Nemzeti Adatvédelmi és Információszabadság Hatóság

A 2012-es Alaptörvény eltörölte az ombudsmani rendszert, így az adatvédelmi biztos szerepe is megszűnt. A régi rendszer megszűnése és a független adatvédelmi hatóság létrehozása számos vitát váltott ki, mivel ez teljességében újraalkotta az adatvédelemmel foglalkozó személy és szerv jogállását (Lakatos-Nagy, 2012).

Az Info tv. 5. fejezete rendelkezik a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) létrehozásáról. A Hatóság autonóm államigazgatási szervként létezik, fontosságát a 38. paragrafus (2) bekezdése írja le:

„(2) *A Hatóság feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése, továbbá a személyes adatok Európai Unión belüli szabad áramlásának elősegítése*" (Info tv. 2011, 38.§ (2) bekezdés,).

A Hatóságot vezető elnököt a köztársasági elnök nevezi ki, összesen kilenc évre. 2012-től Péterfalvi Attila tölti be az elnöki szerepkört, 2020-ban újra őt nevezték ki a Hatóság élére (NAIH, 2020).

A Hatóság éves beszámolója szerint, első évében közel 3000 ügyben indult meg vizsgálati eljárás, ezeknek jelentős része adatvédelemre, kisebb része információszabadságra irányult. Tíz évvel később, 2022-ben már közel 10 ezer ügy volt a folyamatban (NAIH, 2013; NAIH, 2023). A növekedésben szerepet játszó tényező lehet a bevezetett GDPR szabályozás, a digitalizáció folyamatos fejlődése és a Hatóság egyre fokozatosabb elismertsége, valamint a lakosság bizalma a Hatóság iránt.

2. KOLOSTOROKTÓL A DIGITALZÁCIÓIG

2.1. Az egészségügy rendszerek megszületése

Az egészségügy az egyik legfontosabb ágazat egy állam működésében, a kritikus infrastruktúrák közé sorolják. Az Európai Unió 2008/114/EK irányelv szerint, amely az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről rendelkezik, a kritikus infrastruktúra nem más, mint„ *azon eszközök vagy rendszerek, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, valamint az emberek gazdasági és szociális jólétéhez*" (2008/114/EK). Az uniós szabályozáson felül, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. CLXVI. törvény rendelkezik és van jelenleg hatályban. Az egészségügyi ágazaton belül több létfontosságú rendszerelem is van, amelyek olyan eszközök, szolgáltatások, létesítmények, amelyeknek kiesése a feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna nemzeti vagy akár uniós szinten is.

Az egészségügynek, mint kritikus infrastruktúrának létfontosságú rendszerelemei:

- aktív fekvőbeteg-ellátás, és a működtetéséhez szükséges szolgáltatások,
- mentésirányítás,
- egészségügyi tartalékok és vérkészletek,
- magas biztonsági szintű biológiai laboratóriumok és
- gyógyszer-nagykereskedelem (2012. évi CLXVI. tv.).

Az elmúlt évezredek során az orvoslás folyamatosan fejlődött, egy többnyire egységes rendszerré alakult a fejlett országokban. Ennek a rendszernek a sikeres működése elengedhetetlen a társadalom jólétéhez.

A magyar egészségügy közelmúltbeli történelmébe való betekintés elengedhetetlen a digitális egészségügy kialakulásához. Az 1800-as évek végére addig sose látott mértékű kórházfejlesztés indult meg. Megalakult az Általános Munkásbetegsegélyező és Rokkant Pénztár. A századfordulót követően kialakult a Védőnői Szolgálat, mely egyedülállónak számított a korban (Buda, 2018). A kórházak és szakszervezetek fejlődését az I. világháború döntötte romba. A háborút követő Magyarország minden tekintetben, így az egészségügy szempontjából is új, nehezebb helyzetbe került (Mózsa-Szűcs, é.n.). Az 1927. évi XXI. törvény. létrehozta az Országos Társadalombiztosító Intézetet (OTI), amely a társadalombiztosítást volt köteles finanszírozni. A törvény azonban kizárta a biztosítási rendszerből az akkori legszélesebb társadalmi csoportot (a mezőgazdasági munkásokat) és más egyéb foglalkozású rétegeket is. Az Osztrák-Magyar Monarchia felbomlásának következtében Magyarországon elmaradt a szociálpolitika átfogó társadalmi reformja. Ennek eredményeként a lakosság egészségügyi állapota nagyban függött a társadalmi hovatartozástól: a szegényebb rétegek korlátozott lehetőségekkel rendelkeztek a városi középosztályhoz képest (Forgács, 2004).

A két világháború között kiterjesztették a társadalombiztosításra jogosultak körét, azonban a II. világháborút követően, egy 1947-es rendelet szigorítása újra kizárta a parasztság jelentős tömegét a biztosítási rendszerből. 1948-tól az OTI-n kívüli biztosítótársaságokat államosították, vagyonuk az OTI kezelésébe került, ezzel megszűntek a betegbiztosítási ellátás szintkülönbségei (Kollega, é.n.). Az elkövetkezendő évtizedekben folyamatosan bővítették az egészségügyi ellátásra jogosultak körét, ami az 1972. évi II. törvény alapján állampolgári joggá is vált (Forgács, 2004).

A betegbiztosítási ellátás javulása ellenére érezhetően romlott a magyar népegészségügy működése és a lakosság egészségügyi állapota. A problémák megoldásához szükség volt egy

egészségügyi reformra. Az 1980-as évek végén két fontos reformműhely is megalakult, az MTA Közgazdaságtudományi Intézetében és a Szociális és Egészségügyi Minisztérium (SZEM) szervezésében. Mindkét műhely átfogó, modellváltó reformokban gondolkodott, kiemelt helyet foglalt el az egészségügy és a gazdaság összehangolása (Orosz, 2018).

A társadalombiztosítás mellett a kórházrendszer is folyamatos épült és alakult át a XX. század folyamán. A két világháború közötti időszakban egyre több igény merült fel a kórházak szerepével kapcsolatban, nőtt a járóbeteg-rendelés, valamint megnövekedett a speciális feladatkörű szakkórházak száma. Erre az időszakra kialakult a kornak megfelelő, modern kórházhálózat Magyarországon (Kiss, 2015). A II. világháborút követő évtizedekben – az egészségügyi rendszer egészéhez hasonlóan – itt is problémássá vált a finanszírozás. Ennek következtében a kórházak állapota folyamatos romlásnak indult, az intézmények felszerelése, berendezései egyre inkább elavulttá váltak (Orosz, 2018).

2.2. Egészségügyi „rendszerváltás”

A rendszerváltozást követően (1990 után) átalakult az egészségügyi rendszer, melynek fő jellemzői a mai struktúrára is igazak (Forgács, 2004). Az intézményi rendszerben felosztották a hatalom és a felelősség körét: decentralizálttá vált. A magánszektornak egyre nagyobb szerep jutott az egészségügyben is, 1993-ban kiadták az önkéntes pénztárakra vonatkozó törvényt. Az új modell ellenére a rendszer pénzügyi problémái nem szűntek meg (Orosz, 2018).

A kilencvenes évek közepétől kezdődően többször is felmerült a kórházi struktúra átalakítása, a gazdasági változásokhoz való alakítása (Orosz, 2009). Több makro- és mikroszintű reformprogram is terítékre került az elmúlt két-három évtized során, ezek változó formában valósultak meg. Mindenek ellenére a legfontosabb, hogy a magyar egészségügy válságban van. Ennek okait sok mindenben lehet keresni – az egészségügyi intézmények pénzhiányában, a szakképzések romlásában és az egészségügyi dolgozók kivándorlása is hozzájárul (Major-Ozsvald, 2018).

Az egészségügyi adatok kezelésére vonatkozó első és azóta hatályban lévő törvény az 1997. évi XLVII. törvény *az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről* (rövidítve: Eüak. tv.). A törvény megalkotása létfontosságúvá vált, hiszen a technika fejlődésével már nem volt megoldható az adatok magasszintű védelme, mint korábban, amikor az adatokhoz való hozzáférés nehézsége (porosodó kórlap- és kartotékraktárak) természetes védelmet nyújtott (Feith et al., 2021). A törvény mindenkinek, aki kapcsolatba került vagy kerül az egészségügyi ellátó-hálózattal, védi adatait az illetéktelen hozzáféréssekkel

szemben. A törvény komplex módon jogot képzett az egészségügyi adatokra vonatkozóan, melyek a különlegesen személyes adatok kategóriájába tartoznak (Fodorné, 2021). Különleges adatnak minősülnek az alábbi területekre vonatkozó adatok:

- faji eredet,
- nemzetiség,
- politikai vélemény vagy pártállás,
- vallás és más világnézet,
- érdekképviseleti szervezeti tagság,
- szexuális élet,
- egészségi állapot,
- kóros szenvedély és bűnügy (NAIH, é.n.).

A jogszabály a nem egészségügyi szerveknek is irányadó, amennyiben egészségügyi adatokkal is dolgoznak. A törvény a betegek és adataik védelméről szól, nem az egészségügyi dolgozókról rendelkezik (Feith et al., 2021).

Az egészségügyi adatok kezelésére vonatkozóan a mai napig ez a törvény van hatályban. A törvény hatályba lépése óta (1998) történtek apróbb változtatások benne a digitalizáció és adatvédelem fejlődésével párhuzamban. Bár nem csak erre a területre fókuszálnak, de egészségügyi adatvédelemre vonatkozó szabályokat tartalmaz még az Info tv. és a GDPR is. A 2011-es Info tv. az egészségügyi adatok szigorúbban kezeli, mint a többi személyes adatot, különleges adat besorolásuk végett (Info tv., 2011). A GDPR is megalkotta a személyes adatok különleges kategóriáit, amelybe beletartoznak az egészségügyi adatok is. A GDPR különösen szigorúan rendelkezik a különleges adatokról, főszabályként tiltja ezek kezelésél, kivétel bizonyos esetkörökben. Az érintett hozzáférhet a rá vonatkozó adatokhoz, mint vizsgálati leletekhez vagy diagnózisokhoz, de csak személyi azonosítást követően (GDPR, 2016).

Jogrendszeri sajátosság miatt az Eüak. tv. szabályai szerint szükséges eljárni, még akkor is, ha ez ellentmond a fentebb megnevezett két törvény bármelyikének. Amennyiben viszont nincs ellentmondás, az adatkezelési gyakorlat során mindhárom jogszabály rendelkezéseit figyelembe kell venni, és ez alapján eljárni (Feith et al., 2021).

3. E-EGÉSZSÉGÜGY

3.1. Az új fogalom: digitális egészségügy

Az e-egészségügyben számtalan lehetőség rejlik, ugyanakkor rendkívül összetett. A globalizációval együttesen berobbanó digitalizáció jelentős kihívások elé állít minden ágazatot, így az egészségügyet is. Különösen nagy nehézséget okoz, hogy az innovatív megoldásokat nem lehet feltétlenül beilleszteni a meglévő körülmények közé – gyakran egy teljesen új rendszert követelnek meg. Az egészségügy pedig nem a legkönnyebben átalakítható területek egyike.

Ha a digitalizáció magyarországi hatásait szeretnénk megvizsgálni – bármely oldalról, bármely részletre fókuszálva –, először tágabban, európai uniós szinten kell szétnéznünk. Nem meglepő, hiszen az Európai Unió tagországai kötelesek annak szabályozása szerint eljárni.

Mi is valójában a digitális egészségügy (*e-health*)? Az Európai Bizottság meghatározása szerint minden olyan eszköz és szolgáltatás, amelyek „*információs és kommunikációs technológiák révén tökéletesítik a megelőzést, a diagnosztizálást, a kezelést, az egészséggel kapcsolatos kérdések nyomon követését és kezelését, valamint felügyelik és kezelik az egészség és az életmód kölcsönhatását*” (Európai Bizottság, é.n.). Fontos kiemelni, az e-health eredeti jelentése elektronikusan elérhető egészségügyi szolgáltatás volt, napjainkra azonban már egybeolvadt az e-egészségügy kifejezéssel (Fodorné, 2021).

Uniós szinten az e-egészségügy már a 2000-es évek elején előkerült, mint kiaknázatlan szakpolitika. 2004-ben fogadták el az első uniós e-egészségügyi cselekvési tervet, majd 2012-ben a másodikat. 2011-ben egy e-egészségügyi munkacsoporttal bővítették ki ilyen irányú cselekvéseiket, melynek első ülése Budapesten volt (Szabó et al., 2021). Ugyanebben az évben egy e-egészségügyi hálózatot hoztak létre, mely összekapcsolja az e-egészségügyért felelős nemzeti hatóságokat, ezzel segítve az Unión belüli egység megteremtését (Európai Bizottság, é.n.).

A következő nagyobb lépést 2018-ban tette meg a Bizottság, amikor közleményt tett közzé az egészségügyi és az ellátási ágazat digitalizálásnak fokozására vonatkozóan. A célok érdekében az alábbi három pillérre építkeztek:

1. biztonságos adatlekérdezés és -megosztás;
2. az egészségügyi adatok összekapcsolása és cseréje a kutatás, a gyorsabb diagnózis és az egészségügyi szolgáltatások javításának érdekében;

3. az egyéni szerepvállalás és a személyre szabott ápolás megerősítése a digitális szolgáltatások révén (Európai Bizottság, é.n.).

Az Európai Unió 2021-ben elindította a „digitális évtized" nevű átfogó programját. A célkitűzések a tagállamok együttműködésével valósulhatnak meg, számos projekt több tagországra terjed ki. A projektben nagy szerepet játszott a COVID-19 pandémia okozta, kényszeres digitális átállás is. A szakpolitikai program részeként terítékre került az európai egészségügyi adattér létrehozása. Az adattér teljes körű ellenőrzéssel rendelkezne az uniós polgárok adatai felett. Egy közös európai szabvány segítségével pedig megvalósulhatna egy Unió-szerte egységesebb egészségügyi ellátás a polgárok részére (Európai Tanács, é.n. *b*).

Az európai egészségügyi adattér, mint egészségügyi ökoszisztéma lehetővé tenné az egyének számára a saját adataik feletti nemzeti és uniós szintű hozzáférést és ellenőrzést, valamint egységes piacot alakítana ki a releváns orvostechnikai eszközöknek. Az egészségügyi adattér az uniós adatstratégia első, egy konkrét területen létrejövő közös adattere. Kiemelt helyet foglalnak el a tervezésben az adatvédelmi eljárások betartása és megfelelő szabályozása (Európai Bizottság, é.n.).

Kiemelendő, hogy az adattér még nem valósult meg, bevezetése már több tagországban részlegesen elkezdődött. A teljes program megvalósulási határideje 2030, így ezzel a dolgozat nem foglalkozik.

3.2. E-egészségügy Magyarországon

Az Uniós rendelkezéseken, programokon túl természetesen minden tagországnak vannak egyéni fejlesztései is. A digitális fejlődés nem egyszerű, hiszen az anyagi terhek mellett hihetetlen mértékű kutatás-fejlesztés is szükséges hozzá.

Az Elektronikus Egészségügyi Szolgáltatási Tér (továbbiakban EESZT, eTér) 2017 óta szolgál Magyarország e-egészségügyi rendszereként (EESZT, é.n.). Az uniós támogatással megvalósult rendszer célja az egészségügyi ágazaton belüli kommunikáció biztosítása egy egységes felületen keresztül. Az EESZT megalkotásában fontos szempont volt a magas fokú adat- és kibervédelem (Balogh et al., 2020). Az EESZT-hez az évek előrehaladtával folyamatosan csatlakoztak a különböző egészségügyi szolgáltatók és ellátók (EESZT, é.n.). Az eTér szerepe a Covid-19 járvány elindulásával nőtt meg. A pandémia az élet számos területén kényszerítette a lakosságot a digitális átállásra – így az egészségügyben is, már amennyire ez lehetséges volt. Az EESZT rendszere elsősorban az oltásokra vonatkozó időpontfoglalás miatt került előtérbe.

Az EESZT két felülettel rendelkezik: az egészségügyi dolgozók és az intézményi alkalmazottak számára elérhető ágazati portállal, és a lakosságnak kialakított portállal. Kiemelendő, hogy az ágazati portált használók eltérő adatmennyiséghez férnek hozzá és különböző műveleteket végezhetnek el a rendszeren belül (Jinda, 2022). A lakossági portált használhatja bárki, aki rendelkezik társadalombiztosítási jogviszonnyal Magyarországon. A lakossági portálba való bejelentkezés kétlépcsős: az Ügyfélkapun keresztüli azonosítás után a TAJ szám is szükséges a profil megtekintéséhez.

A rendszerben van lehetőség a digitális önrendelkezésre. Ennek lehetőségét *az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló* 1997. évi XLVII. törvény 2015. évi CCXXIV. törvényben módosított rendelkezései teszik lehetővé. A digitális önrendelkezés célja, hogy a felhasználók saját igényeik és biztonságtudatosságuk alapján állítsák be, hogy a személyükhöz kapcsolódó adatokat ki és milyen szinten tekintheti meg. Ha valaki nem szeretné ezt egyénileg szabályozni, az aktuális adatvédelmi korlátozások lesznek érvényben. A betegadatokhoz csak a háziorvos és a kezelőorvos fér hozzá, a különösen érzékeny adatokat a szakterületi kezelőorvos láthatja. (EESZT, é.n.)

A rendszerben visszakövethető, milyen orvosi ellátásokban vett részt a beteg, milyen beutalókkal és receptekkel rendelkezett. A rendszer bevezetését megelőző időkből származó adatokat azonban nem lehet megkeresni a rendszerben, ezeknek kezelése és tárolása hagyományosan, papíralapon történik (Feith et al., 2021). A személyes adatot nem tartalmazó, publikus törzsadatokat (nyilvántartások és kódtörzsek) bárki számára áttekinthetők. Lehetőség van COVID-oltásra időpontot foglalni és digitális oltási igazolványt kiállítani. Az EESZT rendszere elérhető mobilapplikáción keresztül is.

3.3. Adatvédelem az egészségügyben

Az egészségügyi rendszerre vonatkozóan már a bevezetése környékén felmerültek adatvédelmi aggályok. Kezdetben a magyar és az európai uniós jogszabályok összehangolásának hiánya jelentett problémát több területen is, azonban ezeket az előírásokat az elmúlt évben egységesítették. Nyitott kérdések azonban továbbra is maradtak: szembemegy-e az orvosi titoktartással egy olyan online rendszer, amelyben a beteg adatai egészen könnyen elérhetők? A beteg halála után miért szükséges az adatainak öt éven keresztüli megőrzése? Valamint miért van lehetősége egy kezelőorvosnak a páciens teljes profiljához hozzáférni életveszélyes állapot esetén (Jinda, 2022)?

Az EESZT rendszer szükségessége tagadhatatlan. Bár nem támogatja mindenki, de a digitalizáció fontos. Meglátásom szerint az EESZT segíti az egészségügyi rendszer átláthatóbb működését, hiszen jelentősen csökkenti a fizikai dokumentáció mennyiségét, viszont az online dokumentáció magasabb szintű védelmet igényel, mint a papíralapú.

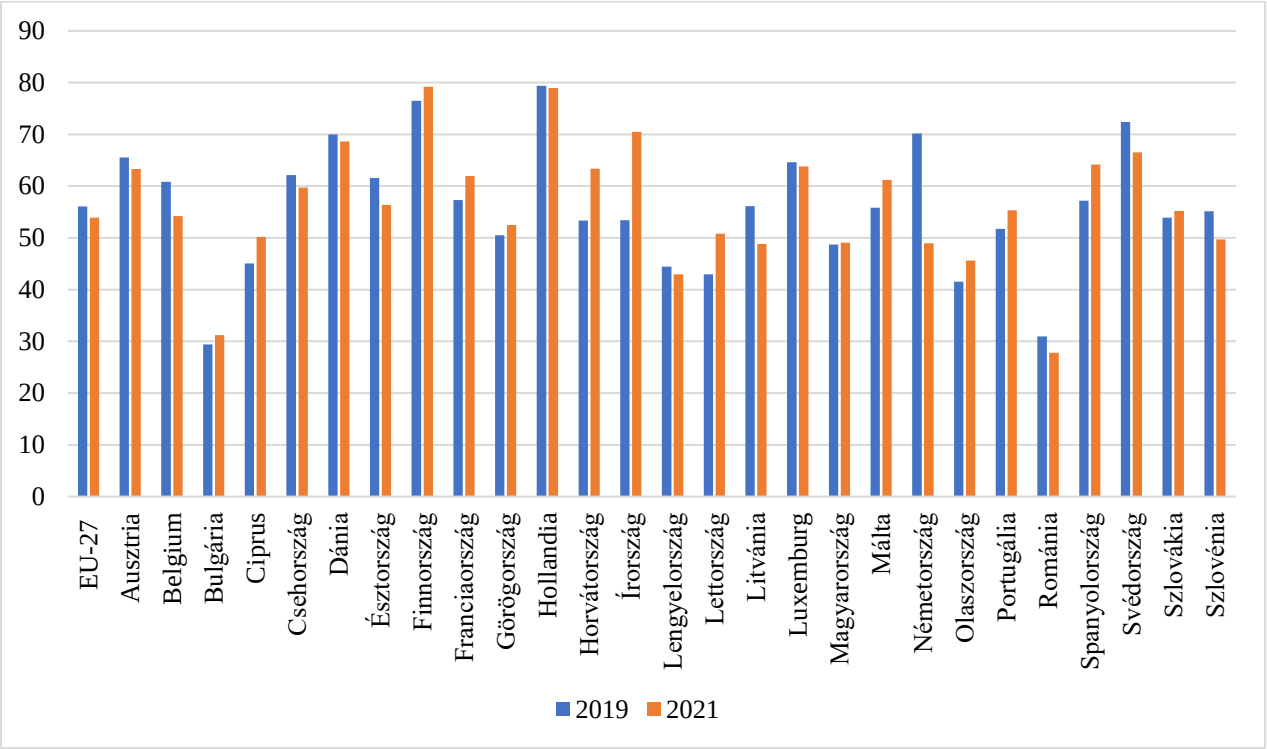
Az egészségügyi adatkezelésnek az egyik legfontosabb aspektusa a titoktartási kötelezettség betartása. A gyógykezelést végző orvos és mindenki más, aki jelen volt ezalatt, valamint a gyógyszerész és az egészségügyi személyzet köteles a kezelés során tudomására jutott információkat megtartani – erre utal az „orvosi titoktartás" kifejezés, mely nem csak az orvosokra vonatkozik (Feith et al., 2021). Ennek a szabálynak a betartása nem feltétlenül csak az EESZT-re vonatkozik, hanem bármiféle kommunikációs formára.

A rendszer sikeres (és biztonságos) működésének egy további feltétele is van: a felhasználók digitális készségeinek megléte. A digitalizáció egyik állandó velejárója, hogy a technológiák fejlődését nem képesek az emberek követni, így a kifejlesztett rendszer működtetése feleslegessé válik, annak kihasználatlansága miatt.

Érdekes emiatt megfigyelni az orvosok korfáját és a digitális készségek kor alapú szintjét. 2019-ben a 65 év feletti Magyarországon dolgozó orvosok száma 8766 fő volt, amely az orvosok 21,23% - át tette ki (KSH, 2023). Az ebbe a korosztályba tartozó hazai lakosságnak azonban 65%-a nyilatkozott arról, hogy digitális ismereteik átlag alattiak (KSH, 2021). Ezen valószínűleg nem segített a hirtelen betörő koronavírus-járvány sem. A sokk után bár mindenki próbált átállni a digitalizációra, hosszú hónapokra volt szükség, hogy felkészüljenek az emberek. Adatvédelem szempontjából, haa nem megfelelően képzett munkaerő kezel egy rendszert, az esetleges hibákhoz vezethet. Természetesen, ha egy orvos digitális készségei elmaradnak a szükségestől, még mindig ott a lehetőség, hogy az ő munkáját segítő asszisztens megfelelően tudja használni a rendszert.

Összefoglalva, az e-egészségügy és a digitalizáció bármely más részének zökkenőmentes működése nem csak a rendszer kialakításán, de a felhasználókon is múlik. Fontos az EESZT – és bármely más egészségügyi rendszer esetén – az esetleges biztonsági rések folyamatos keresése, a rendszer egészének ellenőrzése, a felmerülő problémákra való azonnali reagálás. Az egészségügyi adatok különlegesek, emiatt a kibervédelemre fokozottan ügyelni kell. A felhasználói oldalról pedig külön elemezhetjük az egészségügyi dolgozókat és a lakosságot. Szükséges lenne egy egységesített felkészítés a digitális egészségügyre minden egészségügyben dolgozó személy számára, ezzel csökkentve az emberi hibából keletkező problémákat az EESZT rendszerében.

A lakosság digitális készségei szintén fontosak az adatvédelemben. Az Eurostat felmérései alapján – melynek adatai az 1. ábrán láthatóak - 2019-ben a magyar lakosság átlagos digitális készségszintje 48,68% volt, 2021-re ez 49,09%-ra emelkedett (Eurostat, 2023a, 2023b). Mind a koronavírus-járvány előtt és alatt is elmaradt az uniós átlagtól (2019-ben 56,06% volt, 2021-ben 53,9% volt az EU-27 eredmény). A személyi biztonságtudatosság fontos: egy hibátlan e-egészségügyi rendszer esetén is kibervédelmi problémát jelenthet, ha a felhasználó, az adat tulajdonosa nem kezeli megfelelően saját adatait.



1. ábra: Az egyének átlagos digitális készségszintje az Európai Unió tagállamaiban

Forrás: Saját szerkesztés Eurostat adatok alapján

3.4. Adatlopás – az e-egészségügy legnagyobb kockázata

Az adat értéke felbecsülhetetlen, a digitalizáció térnyerése óta szerepe pedig folyamatosan csak növekszik. Ha valaminek nagy értéke van, akkor egyre többen akarják megszerezni – többnyire illegális módon. A bűnözés jelensége egyidős az emberiséggel, a kiberbűnözés a digitalizáció negatív hozadéka. A folyamatos technológiai fejlődés ugyanannyi kockázatot és kihívást rejt magában, mint lehetőséget. A kiberbiztonság így egyre fontosabbá és bonyolultabbá válik mind egyéni, mind szervezeti, mind állami, mind globális szinten.

Kiberbűnözésnek nevezünk minden, a kibertérben (cyberspace) elkövetett bűncselekményt. A bűntett áldozata lehet bárki, aki valaha is használta az internetet, sőt az is, aki sosem.

Ugyanis például az adatainak eltulajdonítása akkor is megtörténhet, ha nem ő tárolja. A kritikus infrastruktúrák ágazatai, köztük az egészségügy is a fő célpontok közé sorolódnak. A legjellemzőbb támadási módszer a zsarolóprogramok[1] használata, melyek komoly károkat okoznak a megtámadott szervezet számára, és emellett egyre nagyobb bevételt biztosítanak a kiberbűnözőknek. A kiberbűnözés mára már globális iparággá nőtte ki magát, a különböző szolgáltatásokat[2] gyakran állami megrendelésre készítik el, hírszerzés céljából (Selján, 2021).

Az egészségügyi kiberbiztonság célja a hitelesség, elszámoltathatóság és auditálhatóság. Az egészségügyi dolgozók és a betegek bizalma miatt az egészségügyi adatok eredetisége, hitelessége elengedhetetlen. Az elszámoltathatóság biztosítja az adatokhoz való hozzáféréseket lekövethetőségét, jogsértés esetén az elkövetők elszámoltathatóságát. Az auditálhatóság a rendszereken végrehajtott kiberbiztonsági intézkedések, adatkezelési gyakorlatok ellenőrzését és az esetleges hibák javítását, kockázatok kezelését jelenti. Kiemelten fontos a magas színvonalú IT-biztonság garantálása, mivel az egészségügyi rendszerek nagyrészt különleges adatokból állnak. Emiatt célszerű a kibervédelmet a rendszer kialakításával párhuzamosan felépíteni (Bódi et al., 2020). A probléma azonban gyakran nem oldható meg ennyivel: egy rendszer hibái sokszor csak egy-egy kibertámadás után derülnek ki, amikor már késő.

A COVID-19 járvány kitörése megrázta az egész világot – a kiberbűnözőknek pedig kedvező lehetőséget nyújtott az addigiaknál is összetettebb és károsabb bűncselekményekre. Könnyen ki tudták használni a társadalom megnövekedett szorongását és a digitális megoldásokra való folyamatosan növekvő igényt, nem csak magánszemélyeknél, hanem az egészségügyben is (Gárdos-Orosz – Lőrincz, 2020). Az egészségügyi intézmények különösen „jó" célpontoknak bizonyultak a bűnözők számára: titkosított fájlokkal és érzékeny adatokkal is tudták/tudják zsarolni az áldozatokat.

Az Európai Uniós Kiberbiztonsági Ügynökség (European Union Agency for Cybersecurity – ENISA) működésének célja az egységes kiberbiztonsági szint elérésének elősegítése egész Európában. A 2004-ben alapított ügynökség folyamatosan azon dolgozik, hogy egy biztonságos digitális Európát biztosítson a lakosság számára (ENISA, é.n.). A szervezet 2012 óta évente adja ki az úgynevezett fenyegetettségi környezet - „threat landscape" - publikációt. A

[1] A zsarolóprogram (ransomware) egy olyan rosszindulatú szoftver, mely biztonsági támadást indít a számítógép ellen. Korlátozza a megfertőzött gépen található adatokhoz való hozzáférést. A kiberbűnöző egy bizonyos összeg megfizetése ellenében oldja fel az adatok, dokumentumok titkosítását. A zsarolóprogramok többnyire applikáción vagy e-mail csatolmányon keresztül fertőzik meg a számítógépet (HTE, é.n.).

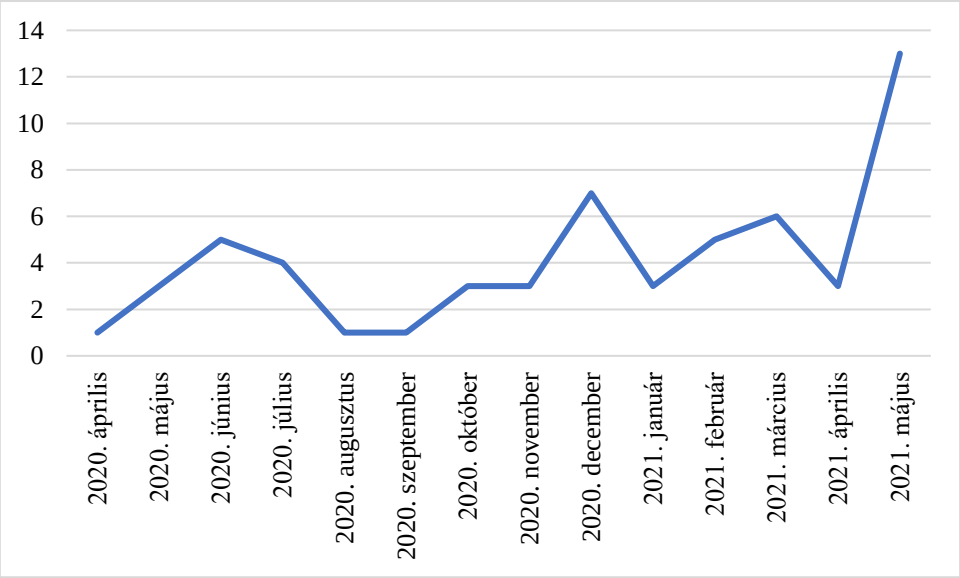
[2] A kiberbűnözők sokszor nem is professzionális hackerek. A kiberbűnözés terjedésével egy olyan szolgáltatói szektor jött létre, amely a rosszindulatú szoftverek (pl. zsarolóprogramok) kereskedelmére koncentrál. Ezáltal hozzáértés nélkül, bárki hozzájuthat káros kódokhoz az ár megfizetésével (Grund, 2021).

„fenyegetettségi környezet” kifejezés arra utal, hogy milyen típusú és mértékű veszélyek és fenyegetések vannak jelen egy adott területen vagy szektorban. Az ENISA kiadványa esetében ez a kibertérre vonatkozik, és hogy a kiberbűnözés különböző formái milyen gyakorisággal fordultak elő. Ez az elemzés segíthet felmérni a kiberbiztonság aktuális szintjét, illetve felhasználható a jobb védelmi stratégiák kialakításához.

A kutatásom középpontjában álló egészségügyi adatvédelem miatt az adatlopásokra helyezem a hangsúlyt. Az ENISA éves publikációi[3] alapján az adatlopás, mint kiberbűnözési forma nem volt mindig ennyire hangsúlyos: 2018-ban a 8. leggyakoribb bűnözési módnak számított, míg 2023-ra a 4. helyre került (ENISA, 2020, 2023a). A koronavírus-járvány kapcsán a vakcina fejlesztő laboratóriumok, kutatóintézetek adatai váltak kulcsfontosságúvá. Emellett az egészségügyi szektorban történő adatszivárgás is jelentősen megnőtt, a legveszélyeztettebb szektorrá vált a kibertérben. A pandémia miatt az e-egészségügyi rendszerek használata középpontba került, így egyre több adat vált elérhetővé digitálisan (ENISA, 2021).

A 2. ábra jól szemlélteti az egészségügyi intézményeket érintő adatlopások számának alakulását 2020 áprilisától 2021 májusáig. A pandémia kezdedétől fogva történtek kiberbűntények az egészségügyi adatokra vonatkozóan, havonta 4-5 egészségügyi rendszert támadtak meg. 2021 májusától kezdődöen pedig minden addigit meghaladó mértékben nőtt meg a bűntettek száma.

[3] Az éves beszámoló kifejezés nem teljesen pontos megnevezés: a kiadványok gyakran hosszabb időtartamot ölelnek fel, mint 12 hónap. Például, a 2020-as publikáció 2019. január – 2020. április közötti eseményekkel és statisztikákkal foglalkozik.



2. ábra: Az egészségügyi adatokat érintő támadások száma az OSINT (nyílt forrású hírszerzés) felhasználásval 2020 áprilisától 2021 májusáig

Forrás: Saját szerkesztés az ENISA adatai alapján

2021 januárjától 2023 márciusáig az Európai Unióban az egészségügyi szolgáltatókat érte a kibertámadások több, mint fele (53%), különösen a kórházak voltak célpontban (42%). Az Unión belül különösen sok támadás érte a francia, spanyol és német intézményeket. 99 incidens, az egészségügy elleni kibertámadások 46%-a irányult adatlopásra (ENISA, 2023b).

A pandémia alatt megfigyelhető kiberbűnözési trend volt az európai polgárok betegadatainak kiszivárogtatása. Ezek az adatok főként a COVID-19 elleni védőoltás vagy a fertőzés kimutatására szolgáló elvégzett tesztek információi voltak. A kibervédelmi intézkedések hiányosságát hangsúlyozza, hogy az adatok kiszivárgásának leggyakoribb oka a gyenge biztonsági rendszerek voltak (ENISA, 2023b).

A pandémia csendesedésével csökkenni látszódtak az egészségügy elleni kibertámadások, de a legújabb adatok újra egy emelkedő tendenciát mutatnak (ENISA, 2023b). 2022 II. és 2023. I. felében az egészségügyi szektor elleni adatra vonatkozó támadások globális szinten a zsarolótámadások 10 %-át tették ki, azaz minden 10. zsarolótámadás egészségügyi adatok megszerzésére irányult (ENISA, 2023a).

Az ENISA forrásai alapján Magyarországon nem történt az egészségügyi szektor ellen kibertámadás a pandémia alatti időszakban.

4. A LAKOSSÁG BIZTONSÁGTUDATOSSÁGA

4.1. Biztonság és magánszféra

A biztonság az emberi lét egyik legalapvetőbb elvárása és joga. A biztonsági szabályozások elsődlegesen az állampolgárok érdekeit, életét védi bel-és külföldi veszélyektől egyaránt, ezzel biztosítva a nemzeti jólétet. A biztonság hiánya az emberi jogok korlátozásához, valamint az egyéni és a kollektív érdekek meg nem valósításához vezet. A biztonság, mint az állam elsődleges feladata, jogi védelmet élvez. A teljes biztonság azonban nem valósítható meg, erre csak törekedni lehet (Révész, 2013).

Minden egyén rendelkezik saját magánszférával, melybe csak a jog által meghatározott mértékben és módon lehet betekinteni. A magánszféra három különböző dimenzióban létezik: fizikai, pszichikai és virtuális szinteken. A testi közelség, mint fizikai szint, a mások általi befolyás, pedig mint pszichikai aspektus jelenik meg. A virtuális dimenzió bármilyen, az egyénre hatással lévő digitális műveletre utalhat (Klein - Tóth, 2018). A magánszférát azonban nehéz meghatározni: lehet érték, jog, követelés, de állapot is. Szerepe viszont minden esetben központi, hiszen hiánya megnehezítené a személyes és nyilvános élet közti különbségtételt. Továbbá a magánszféra együtt jár emberi mivoltunkkal, így létét tagadni nem lehet (Raab, 2017).

Az infokommunikációs technológiák a magánszféra mindhárom dimenziójára hatással vannak, azok mindegyikéből adatokat dolgoznak fel. Itt kapcsolódik be az adatvédelem a folyamatba, mint a magánszféra tiszteletben tartásának eszköze. Az adatvédelmi szabályozás keretét pedig maga a magánszféra határai adják meg (Klein és Tóth, 2018). Az adatvédelem magába foglalja mindazon alapelveket, szabályokat, eljárásokat, adatkezelési eszközöket és módszereket, amelyek az érintett személyek védelmét biztosítják (NAIH, é. n.). Ezenfelül olyan jogi eszközöket biztosít a polgároknak, amelyek szükségesek az információs önrendelkezési jog hatékony gyakorlásához. Garanciát nyújt a háborítatlan magánélet mellett a jogosulatlan információgyűjtések és az adatokkal való visszaélés ellen is (Révész, 2013).

A biztonsághoz és a magánszférához való jog összefonódik: „az egyén akkor érezheti magát biztonságban, hogyha egyben szabad is, illetőleg akkor lehet szabad, hogyha biztonságban érzi magát” (Révész, 2013 24.o.).

4.2. Kérdőíves felmérés

A biztonságos adatkezelés nem csak a szabályokon múlik, hanem az egyének saját tudatosságán is. Az előző fejezetekben az egészségügyi adatokról és az azokra vonatkozó jogi keretekről,

adatvédelmi előírásokról volt szó, azonban hiába minden törvény és előírás, ha az adatalany felelőtlenül bánik saját adataival. Kérdőívemben a magyar lakosság egészségügyi adatokra vonatkozó biztonságtudatosságát vizsgáltam meg. A tárgykör teljeskörű megvilágításához általános internetes adatkezelési szokásokra is rákérdeztem.

4.2.1. Demográfiai adatok

A kérdőív elengedhetetlen részét képzik a demográfiai adatok, enélkül az adatok értékelhetetlenek lennének. A felmérés alatti időszakban 161 fő töltötte ki a kérdőívet. Minden kitöltő Magyarországon él, a lakóhely típusát és a munkaviszony meglétét és formáját nem kérdeztem meg, nem éreztem relevánsnak kutatásomhoz.

Az 1. táblázatban jól látható, hogy a kitöltök több, mint háromnegyede nő volt. Életkor tekintetében a 18 – 25 év közöttiek, valamint a 46 – 65 év közöttiek vettek részt legnagyobb arányban a felmérésben. A kérdőívet csak 18 éves kor felettiek tölthették ki, kiskorúak szülői vagy gondviselői beleegyezés nélkül nem rendelkezhetnek saját adataik felhasználásáról. A kitöltő személyek 53 %-a középiskolai végzettséggel (beletartozik a szakközépiskolai, szakgimnáziumi és gimnáziumi képzés is) rendelkezett a kitöltés időpontjában. A megkérdezettek közel 50 %-a végzett el főiskolai/egyetemi alapképzést vagy ennél magasabb képesítéssel is rendelkezik. Mindösszesen 1 fő nyilatkozott arról, hogy legmagasabb iskolai végzettsége az általános iskolai képzés.

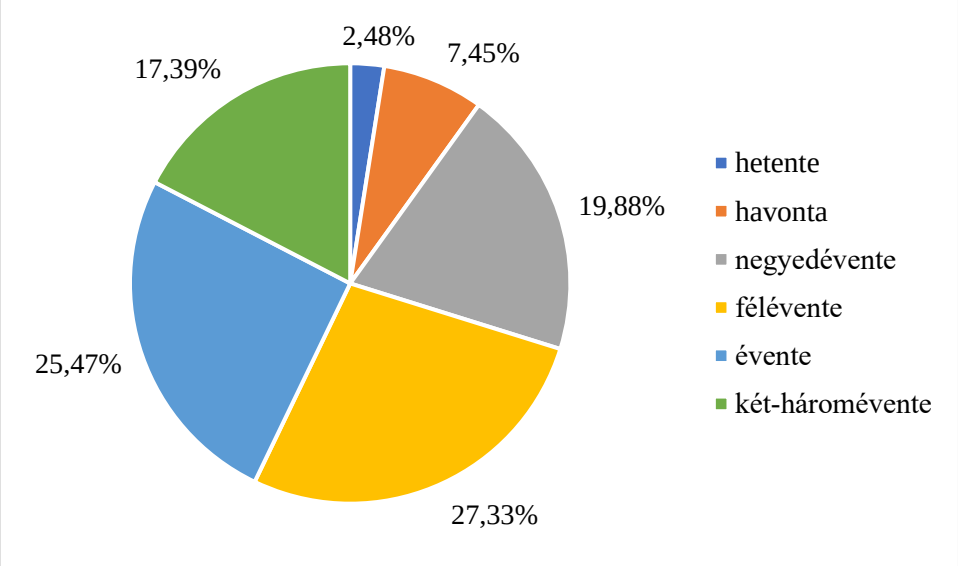
1. táblázat: Demográfiai adatok

Demográfiai adatok		**Minta elemszám**	**Százalékos megoszlás (%)**
Nem	Férfi	37	22,98
	Nő	122	75,78
	Nem adta meg	2	1,24
Életkor	18 – 25 év között	52	32,30
	26 – 35 év között	17	10,56
	36 – 45 év között	14	8,70
	46 – 65 év között	64	39,75
	65 év felett	14	8,70
Legmagasabb iskolai végzettség	Általános iskola	1	0,62
	Középiskola	86	53,42
	Főiskola vagy egyetemi alapképzés	43	26,71
	Egyetemi mesterképzés	19	11,80
	Doktori iskola	12	7,45

Forrás: Saját kérdőíves adatok

A vizsgált minta nem reprezentálja az alapsokaságot, azaz Magyarország lakosságát. A Központi Statisztikai Hivatal demográfiai adataira támaszkodva megállapítható, hogy saját kutatásomban erősen túlreprezentált a 18-25 éves korosztály, és jelentősen alul reprezentált a 65 év feletti korosztály. A nők és férfiak aránya se tükrözi a népességre jellemző tulajdonságokat (KSH, 2023). A válaszadók iskolai végzettségeinek megoszlása se reprezentálja a magyarországi adatokat. 2022-es adatok alapján a középfokú vagy főiskolai képzettséggel rendelkezők a leginkább túlreprezántáltak (KSH, 2022).

Az alapvető demográfiai adatok mellett fontosnak gondoltam felmérni a válaszadók magatartását az egészségügyi intézmények látogatására vonatkozóan, ezt a 3. ábra szemlélteti. A megkérdezettek közül négyen (2,48%) heti szinten járnak orvosi vagy kórházi kezelésre, ahogy azt az 1 ábra szemlélteti. Háromszor ennyien, 12-en (7,45%) havonta látogat egészségügyi intézményeket. Az idősávok szélesedésével nő a válaszok száma is: 32 fő (19,88%) negyedévente, 44 fő (27,33%) félévente vesz igénybe egészségügyi szolgáltatást. A félévi és évi látogatások mennyisége hasonló, utóbbit 41 fő (25,47%) nyilatkozta magáról. Ennél ritkábban az összes válaszadó 17,39 %-a, azaz 28 fő látogat egészségügyi intézményeket.



3. ábra: Egészségügyi intézmények látogatásának gyakorisága

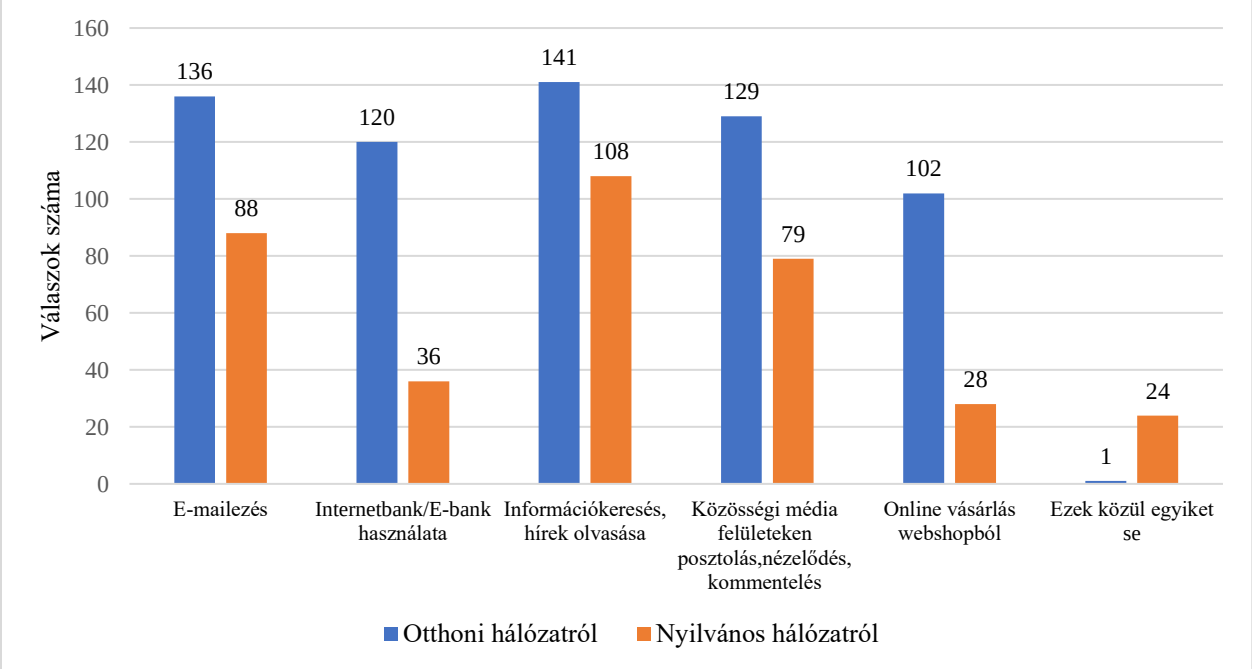
Forrás: Saját kérdőíves adatok

4.2.2. Internethasználati szokások

Kevesebb, mint egy órát internetezik napi szinten a kitöltők 9,94%-a (16 fő). A válaszadók 34,78%-a (56 fő) saját bevallása alapján naponta 1-3 órahosszát tölt el internethasználattal. Kicsivel kevesebb, 54 fő, azaz a megkérdezettek 33,54%-a 3-5 órát, míg a résztvevők 21,74%-a (35 fő) több, mint napi öt órát internetezik. A magas napi óraszám azonban nem csak a

szabadidős tevékenységet fedi le, beletartozhat ugyanúgy a munka vagy tanulmányok miatti internethasználat is. A két területet (munka és szabadidő) azért nem vizsgáltam meg külön szempontokként, ugyanis mindkét esetben előkerülhetnek személyes adatok.

Fontosnak tartottam megvizsgálni és összehasonlítani az általános internethasználati szokásokat, ha otthoni Wi-Fi hálózatra vagy nyilvános Wi-Fi hálózatra csatlakoztatva történik, a kapott eredmények a 4. ábrán láthatóak. A tisztább adatgyűjtés érdekében a nyilvános hálózatot olyan példákkal jellemeztem, mint munkahelyi, iskolai, könyvtári, éttermi internethálózat. A 161 megkérdezettből az összes megadott tevékenység otthoni Wi-Fi hálózaton keresztüli használata legalább 102 főre, azaz a kitöltők minimum 63,35%-ra igaz. 1 fő nyilatkozott arról, hogy ő Wi-Fi hálózatra nem kapcsolódik sem odahaza, se nyilvános helyeken. A nyilvános hálózat esetében jobban megoszlottak az eredmények. 108 fő, azaz a válaszadók 67,08%-a használja információkeresésére és hírek olvasására a nyílt hálózatokat. Az e-mailezés és közösségi média felületeken való posztolás és nézelődés mértéke egymáshoz közeli, a kitöltők körülbelül felére jellemző. Hasonlóság fedezhető fel az internetbankok használata és az online vásárlás között is, amely az összes válaszadó 22,36%-ára, illetve 17,39%-ára igaz. Ez az alacsonyabb érték az adatok pénzzel való kapcsolatával függhet össze. Nyilvános hálózatok esetén sokkal többen, 24 fő egyik tevékenységet sem folytatja.



4. ábra: Internethasználati szokások otthoni és nyilvános hálózatról

Forrás: Saját kérdőíves adatok

A feltett kérdésekre egyéni válaszok is érkeztek. Otthoni Wi-Fi hálózatra csatlakozva további tevékenységként megjelenik a munkavégzés, az online kapcsolattartás és videóhívások és az internetes szórakozási formák, mint a streaming-szolgáltatások igénybevétele filmnézésre, zenehallgatásra, valamint az online videójátékok használatára. Nyilvános hálózatok esetén nem neveztek meg egyéb tevékenységeket a válaszadók.

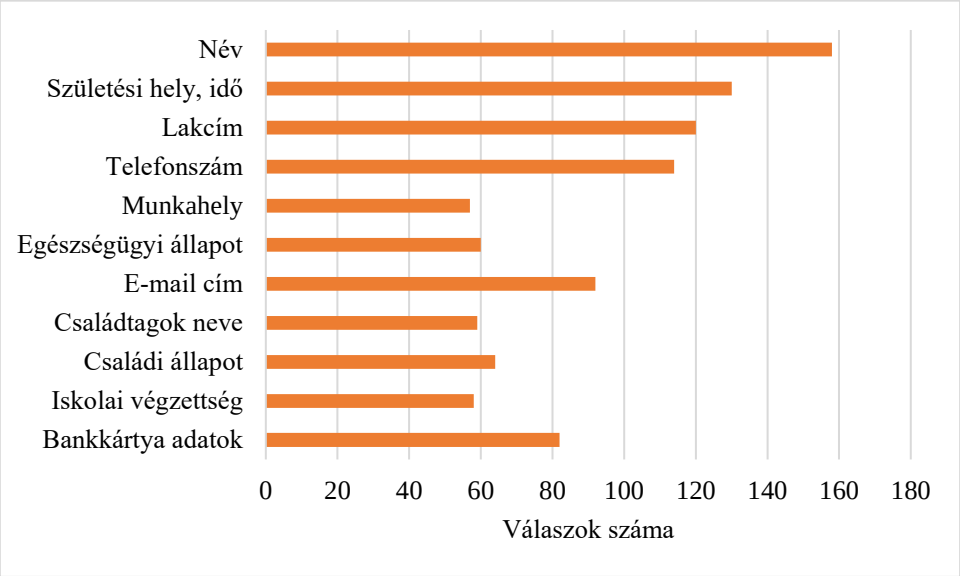
4.2.3. Általános biztonságtudatosság

A tudatos internethasználat rendkívül fontos, nem csak akkor, ha egészségügyi adatokról van szó. Ennek egyik sarkalatos pontja a jelszavak kezelése. A jelszó az egyik alapvető titkosítási módszer, bármilyen online felületen (közösségi média, webshop, internetbank, blog, stb.) hozunk létre egy profilt, szükségünk van egy jelszóra. Egy jelszó annál erősebb, minél komplexebb, azaz tartalmaz kis-és nagybetűket, numerikus és egyéb karaktereket és írásjeleket is. A komplex jelszavak hátránya, hogy bonyolult megjegyezni, minden egyes alkalommal meg kell adni, így a felhasználók sok esetben inkább elmentik a böngészőben – ez azonban felelőtlen, kiberbiztonsági szempontból kritikus lépés. A kérdőívet kitöltők közül 81 fő, azaz az összes válaszadó 50,31%-a el szokta menteni a különböző profiljaihoz tartozó jelszavakat. Jelszavak esetén másik fontos kritérium lenne, hogy mindegyiket csak egy felületen használjuk, ugyanis, ha egy felület belépési adatai illetéktelenek kezébe kerülnek, akkor sokkal könnyebben férhetnek hozzá más adatainkhoz is azonos jelszóhasználat esetében. A felmérés során 110 „igen" válasz – az összes válasz 86,32%-a -érkezett a kérdésre, hogy „Használja-e ugyanazt a belépési jelszót több weboldalon, fiókban?". A jelszóvédelem a tudatos internethasználat alapját képezi, így ezeknek a biztonsági lépéseknek a figyelmen kívül hagyása magasfokú kockázatokat rejt magában a személyes adatokra vonatkozóan is.

A biztonságtudatosság részét képezi továbbá az is, hogy tisztában vagyunk adataink fontosságával, így megvizsgáltam, melyik adatokat gondolják személyesnek a felhasználók. A dolgozat korábbi részében már ismertetésre került, hogy személyes adat lehet bármely olyan adat, amellyel az adatalany azonosítható, vele kapcsolatba hozható. A személyes adatok speciális típusa a különleges adat, amelybe tartoznak többet között az egészségügyi adatok is.

A 5. ábrán láthatjuk, hogy a kérdőívemet kitöltők hogyan vélekedtek erről a kérdésről. A válaszadók 98,14%-a saját nevét egyértelműen személyes adatnak tartja. A születési hely, idő, a lakcím és a telefonszám 130, 120, illetve 114 fő számára sorolható ebbe a kategóriába, ezek 70% feletti értékek még. A megkérdezettek több, mint fele gondolta az e-mail címét, valamint bankkártya adatait személyesnek. A további megadott tételek, azaz a munkahely (57 fő,

35,40%), az egészségügyi állapot (60 fő, 37,27%), a családtagok neve (59 fő, 36,65%), a családi állapot (64 fő, 39,75%) és az iskolai végzettség (58 fő, 36,02%) külön-külön kevesebb, mint 65 fő szerint számítanak személyes adatoknak.



5. ábra: „Melyek tartoznak a személyes adatok közé?" kérdésre érkezett válaszok

Forrás: Saját kérdőíves adatok

4.2.4. Egészségügyi adatok megosztása

Az általános biztonságtudatosságra vonatkozó kérdések után már egészségügyi fókusszal folytatódott a felmérés. Először is fontosnak tartottam megvizsgálni, milyen közegben osztanak meg az emberek egészségügyi információkat másokkal. Itt nem csak az online térre korlátoztam le a válaszadás lehetőségét, hiszen egészségügyi adataink -a digitális térben kifejezetten,- de persze a fizikai térben is rendkívül érzékenyek, szóban való megosztásukkal is privát információt adunk meg másoknak magunkról. A családtagokkal való információmegosztás a leggyakoribb, 130 kitöltőre (80,75%) jellemző. A családunk általában a legközelebbi szeretteinkből áll, így az irányukba történő adattovábbítás teljességgel érthető és elfogadható. A válaszadók körülbelüli egyharmada, 54 fő (33,54%) beszél egészségügyi információiról közvetlen munkatársaival, főnökével is. Ez sok esetben lehet valamilyen szinten kötelező, hiszen egy betegség hatással lehet a munkavégzésünkre is. Továbbá a kollégák sokszor baráti, jó ismerősi viszonyt ápolnak egymással, így az információmegosztás bizalmon is alapulhat. A felmérésben résztvevők 14,91%-a, azaz 24 fő szívesen beszélget saját egészségi állapotáról orvosi vagy kórházi várótermekben is. Ez egy általános jellemző, azonban adataink ilyen mértékű megosztása főleg idegen személyekkel számos kockázatot rejt magában.

Ha csak digitális adatmegosztásra koncentrálunk, összesen 7 fő (4,35%) posztolt már a közösségi médiában egészségügyi információiról, vagy írt ezzel kapcsolatban online (egészségügyi) fórumokon. 26 fő (16,15%) nyilatkozta azt, hogy ő semmilyen formában nem osztotta meg ezek közül még az egészségügyi információit másokkal. Egyéni válaszként többször megjelentek a barátok, mint adatmegosztási közeg. A családtagokhoz hasonlóan, a baráti kapcsolatok is erős bizalmon alapulnak, így az ilyen típusú információátadás alapvető emberi létünk része.

A 2. táblázatban az adatok kor alapú megoszlását láthatjuk. Az egészségügyi intézmények várótermében való információmegosztás – kissé meglepően – a fiatalabb generációkra jobban jellemző. Egészségi állapotról a családtagokkal mindegyik korosztály hasonló mértékben beszélget (saját résztvevői arányához viszonyítva). A munkatársakkal az aktív dolgozói réteg osztja meg leginkább egészségügyi információit, míg az online adatmegosztás a 18-45 közötti korosztályt jellemzi.

2. táblázat: Egészségügyi információk megosztási közege kor alapján

KOROSZTÁLY	**Milyen közegben oszt meg másokkal részletes információkat egészségi állapotáról? (fő)**					
	Orvosi/Kórházi váróteremben várakozókkal	**Családtagokkal**	**Közvetlen munkatársakkal**	**Közösségi médiában posztolom**	**Online fórumokon**	**Egyik se jellemző rám.**
18-25	11	45	12	1	1	5
26-35	4	16	8	3	1	1
36-45	5	14	6	2	0	1
45-65	3	45	22	0	0	12
65 felett	1	9	4	0	0	5

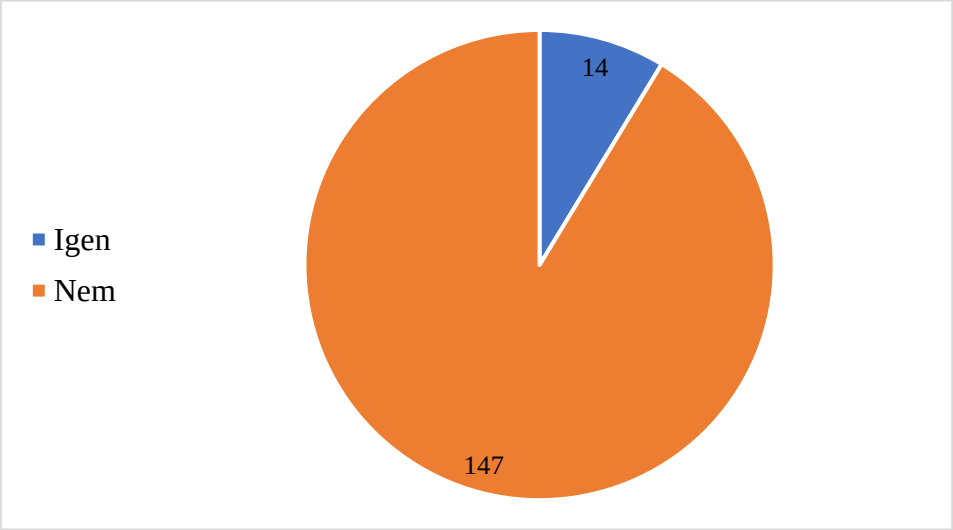
Forrás: Saját kérdőíves adatok

4.2.5. Egészségügyi adatok a közösségi médiában

A közösségi média a modern kor egyik legveszélyesebb eszköze. Rengeteg lehetőség rejlik benne, tudjuk tartani a kapcsolatot messze lakó családtagjainkkal, barátainkkal, megkönnyíti a kommunikációt. Egy online naplóként használják sokan, ahol megoszthatják képeken, rövid szövegeken keresztül életük minden egyes apró változását. A benne rejlő kockázatok száma

viszont rendkívül magas, sokszor olyan információkat is megosztanak a felhasználók, amelyek ilyen szintű nyilvánossá tétele kiszolgáltatottá teszi az adat tulajdonosát.

A 6. ábra alapján látható, hogy 14 válaszadó (8,70%) saját bevallása szerint már osztott meg az interneten szöveges vagy képi információt saját egészségügyi állapotával kapcsolatban. Az eredmény olyan szempontból meglepő, mivel az egyik előző kérdésemnél csupán 7 fő – pont a fele – válaszolta azt, hogy egészségügyi információit közösségi médián vagy online fórumon keresztül másoknak kiadta volna. Az eltérés oka lehet, hogy információ alatt konkrét betegségek, szükséges gyógyszerek nevét, kezeléseket értettek a kitöltők, amit sokkal érzékenyebbnek gondolnak, mint kitenni egy képet egy kórházi ágyról. Valójában minden felsorolt tétel ugyanolyan különleges egészségügyi adat saját személyünkről.

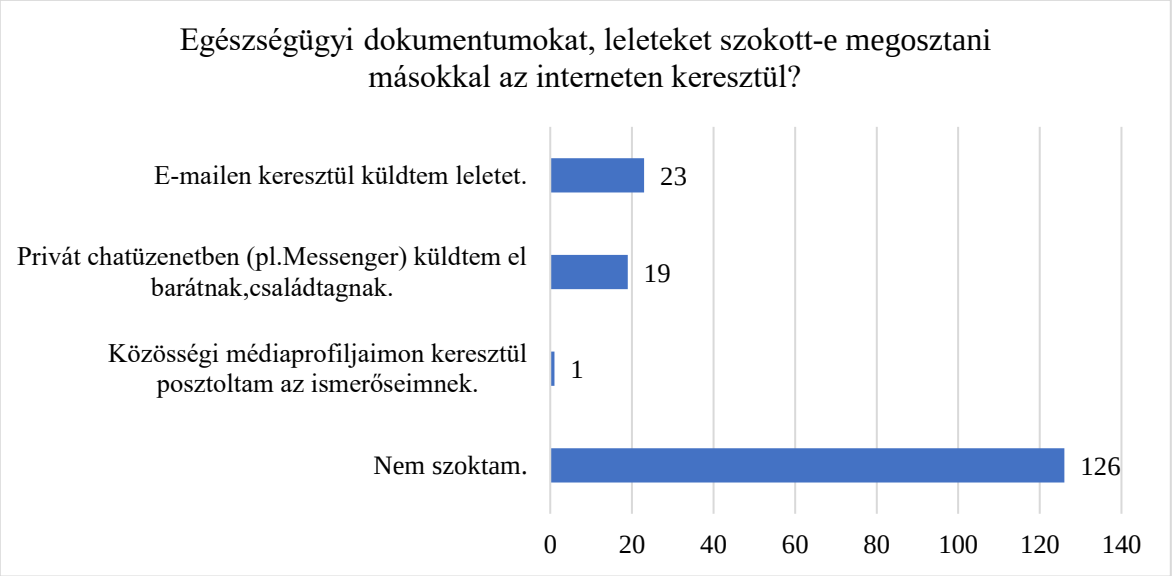


6. ábra: „Posztolt-e már hírt/fotót közösségi média felületeire saját egészségi állapotával kapcsolatban (kórházi ágyról, otthonában lábadozva stb.)?" kérdésre adott válaszok

Forrás: Saját kérdőíves adatok

Az 7. ábra már egy, a konkrét egészségügyi dokumentumok megosztására vonatkozó kérdésre érkezett válaszokat vizualizálja. A kitöltők jelentős része, 78,26%-a semmilyen formában nem továbbította még mások felé online az egészségügyi leleteit. E-mailen és privát chatüzenetben való leletküldésről hasonló értékeket kaptam, 23 (14,29%) és 19 fő (11,80%) válaszadó állította ezt magáról. 1 fő (0,62%) posztolt már nyilvánosan saját profilján egészségügyi dokumentumot, leletet. Ehhez kapcsolódóan megkérdeztem, hogy a COVID-19 oltottsági igazolványról készült fotót megosztották-e a válaszadók valamely online felületeken. Az előbbi kérdésben kérdezett egészségügyi dokumentációkhoz hasonló mértékben, 80,75%-a válaszadóknak nem tett fel képet igazolványáról egyik online felületre se. 7 fő (4,35%) e-mailen, 5 fő (3,11%) Facebook Messengeren és 1 fő (0,62%) Instagrammon keresztül osztotta meg

másokkal (privát) üzenetben az igazolványáról készült fotót. Azok közül, akik e-mailen elküldték mások számára az oltottsági igazolvány fényképét, majdnem minden második személy Facebook Messengeren is továbbította ismerőseinek. Ebből következtetve, egy privát chatüzenetet ugyanolyan biztonságosnak ítéltek meg, mint egy e-mailen küldött levelet.



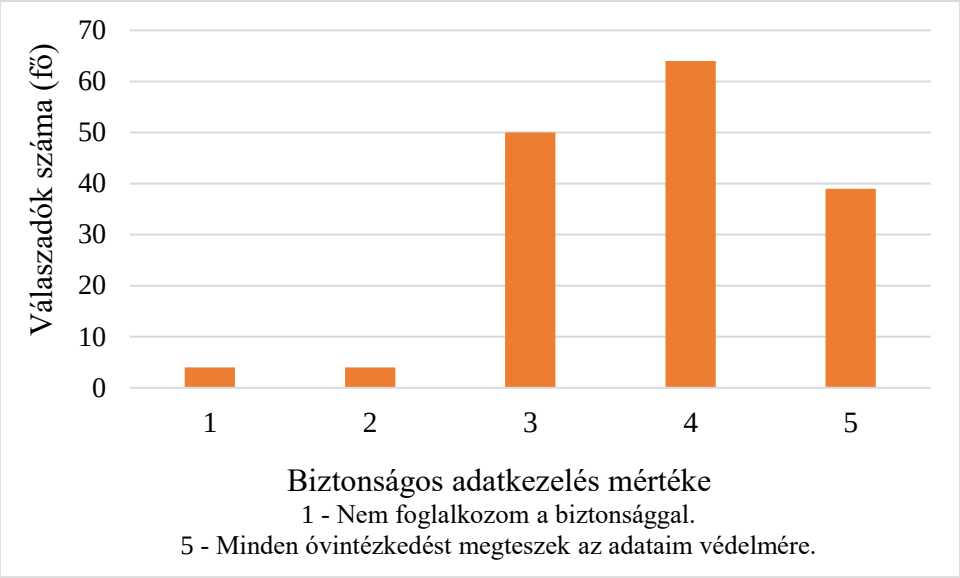
7. ábra: Egészségügyi dokumentumok megosztása az interneten keresztül

Forrás: Saját kérdőíves kutatás

4.2.6. Biztonságtudatosság mértéke

A biztonságtudatosság valódi mértéke és az, amit mi gondolunk magunkról, sokszor eltérhet. Fontos, hogy reálisan ítéljük meg saját magunkat, és amennyiben nem vagyunk elégedettek teljesítményünkkel, keressünk megoldásokat annak javítására. Ennek méréséhez Likert-skálát alkalmaztam.

A 8. ábrán látható eredmények elsőre meglepőek voltam számomra. 4 fő (2,48%) saját bevallása szerint egyáltalán nem foglalkozik a biztonsággal az online térben, ugyanennyien pedig csak minimálisan figyelnek oda rá. A kitöltők közel egyharmada, 50 fő (31,06%) úgy ítélte meg, hogy foglalkozik vele, de messzemenőleg nem tesz meg mindent az adatvédelem érdekében. A legtöbben, 64 válaszadó (39,75%) nagyrészt tudatos, adatait többnyire biztonságosan kezelőnek vallotta magát. A kitöltők 24,22%-a, azaz 39 fő minden óvintézkedést megtesz az adatai védelméért. A felmérésben résztvevők közel egyötöde teljesen tudatos internetfelhasználónak tartja magát.



8. ábra: Biztonságtudatosság mértéke, saját megítélés alapján

Forrás: Saját kérdőíves adatok

Összefoglalva, a kérdőíves felmérés megmutatja, hogy a válaszadók digitális biztonságtudatossága kisebb, mint ahogy az ők magukról gondolják. A jelszavak érzékenységére, valamit a nyilvános hálózatok használatában rejlő veszélyekre sokan nem figyelnek oda megfelelően. A személyes adatokat nem kezelik eléggé szigorúan, érzékeny információkat gyakran adnak meg magukról, nem felismerve az ebben rejlő kockázatokat.

Ezzel szemben, az egészségügyi adatok megosztása inkább bizalmi alapon történik, de a várótermekben való egészségügyi állapotmegosztás is nagymértékben van jelen. Az interneten keresztüli adatküldés többnyire privát csatornákon valósul meg, a valóságban azonban ennek is megvan a kibervédelmi kockázata.

5. KÖVETKEZTETÉSEK ÉS JAVASLATOK

Kutatásomban az egészségügy kibervédelmi kockázataira kerestem a választ. Kutatásom elején három kutatási kérdést állítottam fel, ebből egy az egészségügy intézményi kibervédelmére irányult, a másik két kérdés a lakosság egészségügyi biztonságtudatosságára. Utóbbi két kérdésre hipotéziseket is megfogalmaztam. Az egészségügy digitális fejlődését megvizsgálva, és a lakosság biztonságtudatosságát saját felméréssel elemezve sikerült dolgozatomat megírni és kutatási kérdéseimet megválaszolni.

1. Milyen szinten valósul meg a kibervédelem a hazai e-egészségügyi rendszerekben és ezek milyen további lehetőségeket rejtenek magukban?

A digitális egészségügy létezik, és folyamatosan fejlődik, mind nemzetközileg, mind hazai szinten. A Magyarországon használatos e-egészségügyi rendszer (EESZT) elméleti síkon egy rendben működő, felhasználóbarát felület, a gyakorlatban azonban felmerülnek problémák kibervédelmi szempontból. Az EESZT rendszer bizonyos esetekben indokolatlanul sok adatot enged láttatni olyan személyeknek, akiknek munkáját nem érintik az adott információk. Az emberi tényező szintén kockázatot rejt magában, az egészségügyben dolgozók nem rendelkeznek elegendő digitális tudással a rendszer teljeskörű, megfelelő használatához, ami adatszivárgáshoz vezethet. Hatással van a kiberbiztonságra továbbá a hazai informatikai szakemberhiány és az intézményekre jellemző elavult géppark.

Az e-egészségügy biztonsági fejlesztése elengedhetetlen és kötelező. Fontos lenne nem csak technikai, hanem emberi tudás tekintetében is magasabb szintre emelni a védelmét.

2. Hol húzza meg a lakosság a magánszféra határát a személyes adatokra vonatkozóan?

A magánszféra határa az egyénen múlik, de általánosságban elmondható, több információt és adatot osztunk meg másokkal, mint amennyit kellene. Személyes adataink legféltettebb értékeink közé tartoznak, a gyakorlatban sokszor mégis mások kezébe adjuk őket. A bizalom fontos szerepet játszik az információmegosztásban, de nem csak ezen múlik. Az Internet elterjedése, különösen a közösségi média felületek megjelenése jelentősen csökkentette a magánszféra mértékét, hiszen sokan úgy vélekednek, – hogy meg kell osztani híreket, információkat másokkal, aktuálisnak kell maradni mások szemében. Személyes adatainknak kisebb jelentőséget tulajdonítunk, mint amekkorával valójában bírnak.

3. Mennyire van tisztában a lakosság egészségügyi adataik érzékenységével?

Az általános digitális kompetencia a felmért adatok alapján fejlesztendő, de az egészségügyi adatok védelmére jobban figyelnek a felhasználók. Összevetve az általános adatvédelemmel, az egészségügyi adatok kisebb mértékű online megosztása nem az adatok érzékenysége, inkább tartalma miatt tartom valószínűbbnek. Egészségügyi dokumentumaink, leleteink általában egészségi problémákat írnak le, így ezeket inkább megtartják maguknak a felhasználók,

mint például egy általános adatot (például telefonszám) vagy egy pozitív történést (például nyaraláson készült fotók).

A primer kutatási kérdéseimre az alábbi hipotéziseket állítottam fel, amelyeket a felmért adatok segítségével értékeltem:

H2.1: Az idősebb generációkba tartozó személyek kevesebb információt osztanak meg magukról.

A khi négyzet próba alapján a két változó között szignifikáns közepes kapcsolat van, ahogy az a 3. táblázat első sorában látszik. Ez alapján függ az életkortól, hogy milyen közegben, mennyi információt osztanak meg az emberek másokkal. A hipotézisben megfogalmazottokkal azonban nem tudok egyetérteni, a kereszttáblás kimutatások alapján a 46 - 65 és 65 év feletti korosztály személyes adatait különböző közegekben (az interneten és a hétköznapokban is) gyakrabban osztja meg másokkal, mint a 18-45 év közötti válaszadók. A hipotézisemet cáfolom.

H2.2: A magasabb iskolai végzettséggel rendelkezők több adatot tartanak személyesnek.

A két változó között szignifikáns erős kapcsolat van. A felmérés alapján, arányaiban nézve minél magasabb iskolai végzettséggel rendelkezett a válaszadó a kitöltés idején, annál több megadott lehetőséget tartott személyes adatnak. Ennek oka lehet, hogy a tanulmányai során informatikai és információbiztonsági ismereteket szerzett, ezáltal jobban tisztában van az adatvédelem jellemzőivel. A hipotézisemet elfogadom.

H3.1: Azok a személyek, akik gyakrabban látogatnak egészségügyi intézményeket, nagyobb valószínűséggel osztanak meg másokkal részletes információkat egészségi állapotukról.

A két változó között nincs szignifikáns kapcsolat, azaz nem befolyásolja az egészségügyi intézmények látogatásának gyakorisága az egészségügyi adatokra vonatkozó tudatosságot. A felmérés során összegyűjtött adatok szerint hasonló mértékben osztanak meg információkat egészségügyi állapotukról azok, akik negyedévente látogatnak meg egészségügyi intézményeket, mint akik 2-3 évente mennek csak el vizsgálatokra. Természetesen, aki gyakrabban jár, többször van lehetősége beszélni egészségügyi állapotáról másokkal, de maga a megosztási szándék ettől független. A hipotézisemet cáfolom.

H3.2: A magukat biztonságtudatosabbnak valló személyekre kevésbé jellemző, hogy saját egészségügyi állapotukat vagy egészségügyi dokumentumaikat, leleteiket megosszák másokkal az interneten keresztül.

A khi négyzet próba alapján a két változó, azaz a biztonságtudatosság és az egészségügyi dokumentumok, leletek interneten keresztüli megosztása között szignifikáns gyenge kapcsolat van. A felmérés eredményeit megvizsgálva, azok, akik saját megítélésük szerint minden vagy szinte minden biztonsági óvintézkedést megtesznek az adataik védelméért, valóban kisebb arányban osztották meg egészségügyi adataikat azokhoz a válaszadókhoz képest, akik saját biztonságtudatosságukat gyengébbre értékelték. Más kérdésekre vonatkozóan megkérdőjelezhető a saját biztonságtudat megítélése, de az egészségügyi adatok aspektusából van összefüggés. A hipotézisemet elfogadom.

3. táblázat: Hipotézisvizsgálat

Hipotézis száma	**Hipotézis**	**Szignifikancia szint értéke ($\chi 2$)**	**Cramer együttható értéke (V)**	**Értékelés**
2.1	Az idősebb generációkba tartozó személyek kevesebb információt osztanak meg magukról.	92,575 $p < 0,001$	0,379	szignifikáns közepes kapcsolat
2.2	A magasabb iskolai végzettséggel rendelkezők több adatot tartanak személyesnek.	413,498 $p<0,001$	0,801	szignifikáns erős kapcsolat
3.1	Azok a személyek, akik gyakrabban látogatnak egészségügyi intézményeket, nagyobb valószínűséggel osztanak meg másokkal részletes információkat egészségi állapotukról.	86,595 $p > 0,005$	-	nincs kapcsolat
3.2	A magukat biztonságtudatosabbnak valló személyekre kevésbé jellemző, hogy saját egészségügyi állapotukat vagy egészségügyi dokumentumaikat, leleteiket megosszák másokkal az interneten keresztül.	52,765 $p<0,001$	0,286	szignifikáns gyenge kapcsolat

Forrás: Saját szerkesztés

A dolgozat megírásával és a kérdések megválaszolásával az egészségügy kibervédelmének kérdéskörét és a felhasználók biztonságtudatosságát az egészségügyi adatokra vonatkozóan behatóbban látom. Intézményi (egészségügyi) oldalról a technológiai fejlődést nemcsak kutatási szinten, hanem a géppark szempontjából is biztosítani kell. Elengedhetetlen a munkaerő

digitális készségeinek fejlesztése, az adatvédelem fontosságának érzékeltetése. Az egészségügyi adatok védelmét másik oldalról a lakosság (digitális) kompetenciáinak fejlődése biztosítaná. A a tudatos internethasználatot, a személyes és különleges adatok védelmét, az adat értékét nemcsak az oktatási rendszerben, hanem azon kívül, egyéb formákban is tanítani kell a lakosságnak, hiszen -, mint ahogy más területeken is beigazolódott, ebben az esetben is az ember a leggyengébb láncszem.

ÖSSZEFOGLALÁS

Az egészségügy, mint a kritikus infrastruktúrák egyike, régóta fontos az állam működésében. Jelentősége nem csökken, azonban működési formája, szervezeti felépítése átalakult, és külső tényezők hatására fog is még változni. Az egyik legmeghatározóbb hatás a digitalizáció, melynek mindent felforgató ereje az egészségügy ágazatát is érintette. Előtérbe került az adat, a XXI. század legnagyobb értékeinek egyike. Az adatok, különösen a személyes adatok rendkívül érzékenyek: az adatlopás, adatokkal való visszaélés a digitalizáció egyik legnagyobb kockázata.

Az egészségügyi szervezetek ilyen szempontból különösen veszélyeztetettek: a polgárok legérzékenyebb adataikkal dolgoznak, egyre több országban – köztük Magyarországon is – online felületen. Az EESZT kiberbiztonsága ezáltal kiemelten fontos. A rendszerben minden óvintézkedés ellenére is lehetnek problémák, a folyamatos felülvizsgálat és fejlesztés elengedhetetlen egy ilyen, különleges adatokat tároló rendszer esetében. A magas szintű technológia háttér mellett a kiberbiztonságban meghatározó az emberi digitális kompetencia, az egészségügyre és az EESZT rendszerre vonatkoztatva ez a dolgozók digitális készségeinek fejlesztését jelenti.

Az egészségügyi adatok védelme felhasználói oldalról se elfelejtendő: a lakosság ugyanúgy felel saját adataiért, mint az adatkezelők. A biztonságtudatosság nem csak a fizikai térben, de az online felületeken is elsődleges tényező. Kiberbűncselekmény áldozata bárki válhat, így az a legjobb, ha minél kevesebb támadási felületet hagyunk, csökkentve az adatlopás kockázatát. Ugyanúgy, mint a dolgozók esetében, a lakosság digitális kompetenciáját is fontos felmérni, szükség esetén lehetőséget biztosítani annak fejlesztésére.

Az internethasználat és annak veszélyei, adataink fontossága az online és a fizikai térben mind-mind olyan téma, melyről fontos beszélni, fontos oktatni. A jövőben egyre inkább digitálisan lesz elérhető minden, az adat pedig a digitális arany lesz – vagy már most is az. Az egészségügyi adatok, különleges adatok lévén pedig mindennél nagyobb védelmet követelnek meg, mindkét oldalról

IRODALOMJEGYZÉK:

1998. évi VI. törvény (1998). https://net.jogtar.hu/jogszabaly?docid=99800006.tv .Letöltés dátuma: 2023.10.06.

2008/114/EK irányelv (2008). https://eur-lex.europa.eu/HU/legal-content/summary/protecting-critical-infrastructure.html Letöltés dátuma: 2023. 10. 26.

2012. évi CLXVI. törvény (2012). https://net.jogtar.hu/jogszabaly?docid=a1200166.tv Letöltés dátuma: 2023. 10. 26.

Avtv (1992): 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról. https://mkogy.jogtar.hu/jogszabaly?docid=99200063.TV .Letöltés dátuma: 2023. 10. 06.

Balogh S. et al. (2020): *Népegészségtan 1*. https://mersz.hu/forrai-barcs-nepegeszsegtan-1// . Letöltés dátuma: 2023. 10. 20.

Bódi A. et al. (2020): *Az IBTV. Gyakorlata - Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2020*. https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/18027/Az%20Ibtv%20gyakorlata%20-%2050%20%C3%B3r%C3%A1s_220525.pdf?sequence=3 Letöltés dátuma: 2023. 10. 26.

CFREU (2009): *EU Charter of Fundamental Rights*. https://fra.europa.eu/en/eu-charter . Letöltés dátuma: 2023. 10. 07.

Dr. Buda J. (2018): *Az egészségtudomány története*. https://www.etk.pte.hu/public/upload/files/oktatas/Dr_Buda_Jozsef_Egeszsegtudomany_tortenete.pdf . Letöltés dátuma: 2023. 10. 16.

EESZT (é.n.): *Mi az az EESZT?* https://e-egeszsegugy.gov.hu/mi-az-eeszt- . Letöltés dátuma: 2023. 10. 20.

Egészségügyi Tudományos Tanács (2015): *Az Egészségügyi Tudományos Tanács története*. https://ett.okfo.gov.hu/ett_tortenete/ . Letöltés dátuma: 2023. 10. 16.

ENISA (é.n.): *About ENISA - The European Union Agency for Cybersecurity.* https://www.enisa.europa.eu/about-enisa Letöltés dátuma: 2023. 10. 27.

ENISA (2021): *ENISA Threat Landscape 2021.* file:///C:/Users/ASUS/Downloads/ENISA%20Threat%20Landscape%202021.pdf Letöltés dátuma: 2023. 10. 27.

ENISA (2022): *ENISA Threat Landscape 2022.* file:///C:/Users/ASUS/Downloads/ENISA%20Threat%20Landscape%202022.pdf Letöltés dátuma: 2023. 10. 27.

ENISA (2023a): *ENISA Threat Landscape 2023*. file:///C:/Users/ASUS/Downloads/ENISA%20Threat%20Landscape%202023.pdf Letöltés dátuma: 2023. 10. 27.

ENISA (2023b): *ENISA Threat Landscape: Health sector.* file:///C:/Users/ASUS/Downloads/Health%20Threat%20Landscape.pdf Letöltés dátuma: 2023. 10. 27.

Európai Bizottság (é.n.): *E-egészségügy: digitális egészségügy és ellátás*. https://health.ec.europa.eu/ehealth-digital-health-and-care/overview_hu . Letöltés dátuma: 2023. 10. 20.

Európai Bizottság (2022): *Adatvédelem az EU-ban*. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_hu . Letöltés dátuma: 2023. 10. 06.

Európai Tanács (é. n. *a*): *Adatvédelem az EU-ban*. https://www.consilium.europa.eu/hu/policies/data-protection/ . Letöltés dátuma: 2023. 10. 01.

Európai Tanács (é.n. *b*): *Az EU egészségügyi politikája*. https://www.consilium.europa.eu/hu/policies/eu-health-policy/ . Letöltés dátuma: 2023. 10. 20.

European Comisson (2022): *Data protection in the EU*. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en . Letöltés dátuma: 2023. 10. 07.

European Data Protection Supervisor (é.n.): *The History of the General Data Protection Regulation.* https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en . Letöltés dátuma: 2023. 10. 06.

Eurostat (2023a): *Individuals' level of digital skills (until 2019).* https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i__custom_8083077/default/table?lang=en .Letöltés dátuma: 2023. 10. 24.

Eurostat (2023b): *Individuals' level of digital skills (from 2021 onwards)*. https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i21/default/table?lang=en .Letöltés dátuma: 2023. 10. 24.

Feith H. et al. (2021). *Egészségügyi jog*. https://mersz.hu/hivatkozas/m860ej_book1 Letöltés dátuma: 2023. 10. 25.

Fodorné Z.O. (2021): *Az egészségügyi adatok védelme az e-health technológiák tükrében*. In: Baráth N. – Mezei J. (szerk.):Online konferenciakötet 2021. A rendészettudomány a fiatal kutatók szemével. Budapest, DOSZ. p. 159-168. https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/17921/18_fodorne.pdf?sequence=1&isAllowed=y . Letöltés dátuma: 2023. 10. 20.

Forgács A. (2004*): Egészségügyi rendszerek mai hatékonyságának történeti gyökerei.* Doktori (PhD) értekezés. Budapest, Pázmány Péter Katolikus Egyetem BTK Történettudományi Doktori Iskola Gazdaságtörténeti Műhely

Gárdos-Orosz F. és Lórincz V. (2020): *Jogi diagnózisok - A COVID–19-világjárvány hatásai a jogrendszerre.* https://jog.tk.hu/uploads/files/jogi_diagnozisok_covid19_teljes.pdf Letöltés dátuma: 2023. 10. 26.

GDPR (2016): *General Data Protection Regulation*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679 Letöltés dátuma: 2023. 10. 16.

Grund B. (2021): *A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról*. In:Kecskés G. (felelős szerk.): MTA Law Working Papers 2021/21. o.n. https://jog.tk.hu/mta-lwp/a-kiberter-buncselekmenyeirol-es-a-kiberbunozes-hazai-gyakorlatarol . Letöltés dátuma: 2023. 10. 29.

HTE (é.n.): *Fogalomtár.* https://www.fogalomtar.hte.hu/wiki/-/wiki/HTE+Infokommunikacios+Fogalomtar/zsarol%C3%B3program Letöltés dátuma: 2023. 10. 29.

Iötv. (2011): *2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.* https://net.jogtar.hu/jogszabaly?docid=a1100112.tv .Letöltés dátuma: 2023.10. 06.

Jinda A. (2022): *Az Elektronikus Egészségügyi Szolgáltatási Térrel (EESZT) kapcsolatos elméleti és gyakorlati kérdések.* Szakdolgozat. Budapest, NKE ÁNTK. https://antk.uni-

nke.hu/document/akk-copy-uni-nke-hu/Op_Iuv_Ex_2022_3_Jinda%20Adrienn.pdf .Letöltés dátuma: 2023. 10. 21.

Jóri A. (2009): *Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése.* Szakdolgozat. Pécs, PTE ÁJK Doktori Iskola

Kende T. (szerk.) (2015): *Bevezetés az Európai Unió politikáiba.* Budapest, Wolters Kluwer Hungary.

Kiss L. (2015): *A magyar közegészségügy fejlődése a közegészségügyi gondolkodás kialakulásától az állami közegészségügyi rendszer kiépítéséig.* Doktori (PhD) értekezés. Budapest, ELTE TTK Szociológia Doktori Iskola

Klein – Tóth (2018): Technológia jog – Robotjog – Cyberjog. Budapest, Wolters Kluwer Hungary.

Kollega Tarsoly I. (főszerk.) (é.n.): *Magyarország a XX. században.* https://mek.oszk.hu/02100/02185/html/index.html . Letöltés dátuma: 2023. 10. 18.

KSH (2021): *Digitális ismeretek.* https://www.ksh.hu/sdg/1-23-sdg-4.html Letöltés dátuma: 2023. 10. 23.

KSH (2023): 4.1.1.6. *A dolgozó orvosok száma korcsoport és nem szerint.* https://www.ksh.hu/stadat_files/ege/hu/ege0006.html .Letöltés dátuma: 2023. 10. 23.

Lakatos M. – Nagy E. (2012): Információszabadság – Adatvédelem – Statisztika. *Statisztikai Szemle*, 90. évf. 1. sz. p. 19-40. https://www.ksh.hu/statszemle_archive/2012/2012_01/2012_01_018.pdf . Letöltés dátuma: 2023. 10. 07.

Major I. – Ozsvald É. (2018): *Google-beteg. Egészségügy a világban az internet korszakában.* Budapest, Akadémia Kiadó.

Mózsa Sz. – Szűcs E. (é.n.): *A magyar egészségügy fejlődéstörténete a honfoglalástól napjainkig.* https://www.arcanum.com/hu/online-kiadvanyok/TenyekKonyve-tenyek-konyve-1/medicina-1B567/orvoskepzes-szakkepzes-szolgalatok-1BFDA/a-magyar-egeszsegugy-fejlodestortenete-a-honfoglalastol-napjainkig-1C039/ . Letöltés dátuma: 2023. 10. 16.

NAIH (é.n.): *Adatvédelmi értelmező szótár*. https://www.naih.hu/adatvedelmi-szotar . Letöltés dátuma: 2023. 09. 30.

NAIH (2013): Nemzeti Adatvédelmi és Információszabadság Hatóság. Éves beszámoló 2012. december 31. Budapest, NAIH

NAIH (2020): *Újabb 9 évre Péterfalvi Attilát nevezték ki a Hatóság elnökének.* https://www.naih.hu/hirek/267-ujabb-9-evre-peterfalvi-attilat-neveztek-ki-a-hatosag-elnoekenek . Letöltés dátuma: 2023. 10. 07.

NAIH (2023): Nemzeti Adatvédelmi és Információszabadság Hatóság. Éves beszámoló 2022. december 31. Budapest, NAIH

OECD (é.n.): *Personal Data Protection at the OECD*. https://www.oecd.org/general/data-protection.htm . Letöltés dátuma: 2023. 10. 08.

Orosz É. (2009): Globális és hazai egészségügyi kihívások és egészségpolitikai törekvések a 21. század elején. *Esély* 20. évf. 6.sz. p. 3-26. https://www.esely.org/kiadvanyok/2009_6/OROSZ.pdf . Letöltés dátuma: 2023. 10. 20.

Orosz É. (2018): Tudománytörténeti adalékok az egészségügy jelenlegi válságának értelmezéséhez. *Esély* 29. évf. 5.sz. 3-24. https://www.esely.org/kiadvanyok/2018_5/esely_2018-5_1-1_orosz_tudomanytorteneti_adalekok.pdf . Letöltés dátuma: 2023. 10. 18.

Orosz É. (2022): Miért buktak el a szervezeti innovációk a magyar egészségügyben? *Esély* 33. évf. 1. sz. p. 3-39. https://www.esely.org/kiadvanyok/2022_1/3-39-orosz-eva-esely-2022-1.pdf . Letöltés dátuma: 2023. 10. 20.

Prof. dr. Balázs P. (2018): *A felvilágosult abszolutizmus egészségügye.* http://real.mtak.hu/132118/1/a_modern_magyar_egeszsegugy.pdf .Letöltés dátuma: 2023. 10. 16.

Raab, C. (2017): A magánszféra mint biztonsági érték. Fordította: Berger Viktor. Replika 2017/3. sz. p. 81-95. https://replika.hu/system/files/archivum/replika_103-05_raab.pdf Letöltés dátuma: 2023. 10. 06.

Révész B. (2013): Magánszféra kontra biztonság – egyensúlyra törekedve. A terrorizmus Rubik-kockája, avagy a fenyegetések komplex megközelítése. Budapest, Belügyminisztérium. p. 76-93. https://bm-tt.hu/wp-content/uploads/2022/02/tanulmanykotet_t3.pdf#page=76 Letöltés dátuma: 2023. 10. 06.

Selján P. (2021): A jelen kiberbiztonsági fenyegetései és a jövő kihívásai – A nemzetállami aktorok tevékenysége és a dezinformációk terjedése. *Nemzet és Biztonság* 9.évf. 4. sz. p. 41-65. http://real.mtak.hu/158358/1/document%20%289%29.pdf Letöltés dátuma: 2023. 10. 26.

Szabó Z. et al. (2021): A digitális egészségügyi ökoszisztéma fogalmának és elemeinek nemzetközi és hazai áttekintése. *Információs Társadalom* XXI. évf. 3.sz. p.47-66. http://real.mtak.hu/148839/1/inftars.XXI.2021.3.3.pdf . Letöltés dátuma: 2023. 10. 20.

Sziklay J. - Bendik T. (2019): *Az adatvédelem hazai és európai uniós szabályozása és alapintézmény*ei. https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/13145/Az%20adatvedelem%20hazai%20es%20europai%20unios%20szabalyozasa%20es%20alapintezmenyei.pdf?sequence=1&isAllowed=y . Letöltés dátuma: 2023. 09. 30.

Szőke G. (2013): Az adatvédelem szabályozásának történeti áttekintése. *Infokommunikáció és jog*. 2013/3. p.107-112. https://infojog.hu/wp-content/uploads/pdf/201356_SzokeGergely-Laszlo.pdf . Letöltés dátuma: 2023. 09. 30.

MELLÉKLETEK:

A primer kutatáshoz elkészített kérdőív és válaszlehetőségei:

Az Ön neme:

- Férfi
- Nő
- Nem szeretném megadni

Az Ön kora:

- 18-25
- 26-35
- 36-45
- 46-65
- 65 felett

Az Ön iskolai végzettsége:

- általános iskolai
- középiskolai
- főiskolai
- egyetemi alapképzés
- egyetemi mesterképzés
- doktori iskola

Az Ön tartózkodási helye:

- Magyarország
- Szlovákia

Naponta hány órát tölt el internethasználattal?

- Kevesebb, mint 1 órát
- 1-3 órát
- 3-5 órát
- Több, mint 5 órát

Milyen funkciókat szokott használni az alábbiak közül, ha az otthoni Wi-Fi hálózatot használja? (Több válasz is megadható.)

- E-mail
- Internetbank/ E-bank
- Közösségi média
- Online vásárlás webshopból
- Ezek közül egyiket se
- Egyéb:

Milyen funkciókat szokott használni az alábbiak közül, ha nyilvános internethálózatot (pl. munkahelyi, iskolai, könyvtári, éttermi stb.) használ? (Több válasz is megadható.)

- E-mail
- Internetbank/ E-bank
- Közösségi média
- Online vásárlás webshopból
- Ezek közül egyiket se
- Egyéb:

Elmenti-e böngészőben a weboldalakon létrehozott profiljához tartozó jelszavait?

- Igen
- Nem

Használja-e ugyanazt a belépési jelszót több weboldalon, fiókban?

- Igen
- Nem

Milyen közegben oszt meg információt magáról, környezetéről? (Több válasz is megadható.)

- Az e-mail címemet, telefonszámomat ügyintézéshez, online vásárláshoz minden esetben megadom.
- Számomra ismeretlen személyeknek megadom a családtagjaim, ismerőseim adatait, elérhetőségeit akár telefonon, akár emailben is.
- Az egészségi állapotomról gyakran beszélek a közvetlen környezetemnek.
- A családi állapotomat közzéteszem és aktualizálom a közösségi médiában.
- Beszélgetés során, ha felmerül, sosem titkolom el a koromat, gyakran megemlítem a születési dátumomat és azt is, hol születtem.

Milyen közegben oszt meg másokkal információkat egészségi állapotáról? (Több válasz is megadható.)

- Orvosi/Kórházi váróteremben várakozókkal
- Családtagokkal
- Közvetlen munkatársakkal
- Közösségi médiában posztolom (Messenger, Facebook, Instagram, TikTok stb.)
- Online fórumokon
- Saját blogbejegyzésben
- A fentiek közül egyik sem
- Egyéb:

Posztolt-e már hírt/fotót közösségi média felületeire saját egészségi állapotával kapcsolatban?

- Igen
- Nem

Egészségügyi dokumentumokat, leleteket szokott-e megosztani másokkal az interneten keresztül? (Több válasz is megadható.)

- Igen, e-mailen keresztül küldtem a leletet.
- Igen, privát chatüzenetben (pl. Messenger) küldtem el barátnak, családtagnak.
- Igen, közösségi média profiljaimon keresztül posztoltam az ismerőseimnek.
- Nem szoktam

Családtagjai egészségügyi állapotával kapcsolatban posztolt-e közösségi média oldalakon (pl. egy műtét, baleset esetén)? (Több válasz is megadható.)

- Igen, a gyermekemről.
- Igen, a páromról.
- Igen, a szüleimről.
- Igen, a tesvére(i)mről.
- Nem posztoltam.

Melyik felületeken osztotta meg a COVID-19 oltottsági -igazolványáról készült fotót az alábbiak közül? (Több válasz is megadható.)

- Messenger
- Facebook
- Instagram
- E-mail
- Egyéb:
- Nem rendelkezem ilyen igazolvánnyal.

Milyen gyakran látogat egészségügyi intézményeket?

- havonta
- negyedévente
- félévente
- évente
- két-háromévente

Ön mit gondol, mennyire kezeli biztonságosan adatait az online térben?

- 1-5 közötti értékelés (Likert-skála)

A kapott eredmények közötti összefüggések vizsgálata az IBM SPSS program segítségével:

1. hipotézishez készült elemzés és kimutatás

CHI-SQUARE TEST			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	92,575	44	<,001
Likelihood Ratio	81,292	44	<,001
N of Valid Cases	161		

SYMMETRIC MEASURES			
		Value	Approximate Significance
Nominal by Nominal	Phi	,758	<,001
	Cramer's V	,379	<,001
N of Valid Cases		161	

Információmegosztás (db válasz)

ISKOLAI VÉGZETTSÉG	E-mail cím, telefonszám megadása	Egészségi állapot megosztása másokkal	Családi állapot megosztása és aktualizálása a közösségi média felületeken	Életkor, születési hely, idő elmesélése beszélgetés közben	Egyik sem
18-25	48	12	2	22	3
26-35	18	8	4	0	0
36-45	14	4	5	3	0
46-65	51	9	5	17	5
65 felett	12	0	4	6	1

2. hipotézishez készült elemzés és kimutatás

CHI-SQUARE TEST			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	413,498	312	<,001
Likelihood Ratio	215,888	312	1,000
N of Valid Cases	161		

SYMMETRIC MEASURES			
		Value	Approximate Significance
Nominal by Nominal	Phi	1,603	<,001
	Cramer's V	,801	<,001
N of Valid Cases		161	

Megjelölt személyes adatok száma (db válasz)

ISKOLAI VÉGZETTSÉG	E-mail cím, telefonszám megadása	Egészségi állapot megosztása másokkal	Családi állapot megosztása és aktualizálása a közösségi média felületeken	Életkor, születési hely, idő elmesélése beszélgetés közben	Egyik sem
18-25	48	12	2	22	3
26-35	18	8	4	0	0
36-45	14	4	5	3	0
46-65	51	9	5	17	5
65 felett	12	0	4	6	1

KOR-OSZ-TÁLY	0-3 db	4-6 db	7-8 db	9-10 db	11 db (összes)
általános iskolai	1	0	0	0	0
középiskolai	16	35	11	8	16
főiskolai /egyetemi alapképzés	8	17	8	8	8
egyetemi mesterképzés	3	3	6	4	3
doktori iskola	0	5	2	2	3

3. hipotézishez készült elemzés és kimutatás

CHI-SQUARE TEST			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	86,595	65	,038
Likelihood Ratio	71,224	65	,278
N of Valid Cases	161		

SYMMETRIC MEASURES			
		Value	Approximate Significance
Nominal by Nominal	Phi	,733	0,38
	Cramer's V	,328	,038
N of Valid Cases		161	

Egészségügyi információk megosztása másokkal (db válasz)

EGÉSZSÉGÜGYI INTÉZMÉNY LÁTOGATÁSÁNAK GYAKORISÁGA	Váróteremben idegenekkel	Családtagokkal	Munkahelyen, kollégákkal	Közösségi médiában	Online fórumon	Barátokkal	Egyik sem
hetente	2	3	0	0	0	0	1
havonta	2	11	3	2	0	0	0
negyedévente	10	28	15	1	2	0	4
félévente	5	33	16	1	0	1	7
évente	4	30	13	1	1	0	8
2-3 évente	2	21	7	1	0	0	6

4. hipotézishez készült elemzés és kimutatás

CHI-SQUARE TEST			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	52,765	16	<,001
Likelihood Ratio	22,727	16	,121
N of Valid Cases	161		

SYMMETRIC MEASURES			
		Value	Approximate Significance
Nominal by Nominal	Phi	,572	<,001
	Cramer's V	,286	<,001
N of Valid Cases		161	

Egészségügyi dokumentumok, leletek megosztása az interneten keresztül (db válasz)

BIZTONSÁGTU-DATOSSÁG MÉRTÉKE	E-mailen ke-resztül	Privát chatüzenet-ben	Közösségi média felületeken, nyilvá-nosan	Egyik sem
1	2	0	1	2
2	0	1	0	3
3	10	6	0	39
4	7	8	0	54
5	4	5	0	28