HADMÉRNÖK
FÓRUM
16. évfolyam (2021) 1. szám 177–184.
DOI: 10.32567/hm.2021.1.11

Fejes Zsolt,[1] Helyes Marcell[2]

A Covid-19-világjárvány hatása a telemedicina védelmi besorolására

The Effect of the Covid-19 Pandemic on the Defence Classification of Telemedicine

A szerzők célja, hogy rávilágítsanak egy jelenleg még határterületi megjelenéssel jellemezhető, de a koronavírus-világjárvány során kiemelt szerepet elnyerő és egyre inkább önálló domén formájában megjelenő rendszer, a telemedicina jelentős térnyerésére.
A betegség természetéből adódó korlátozások és az ezzel egyidőben a lakosság részéről fokozódó egészségügyi ellátási igény együttesen emelte a telemedicinát az egészségügyi ellátás fókuszába. Ennek következményeként jelent meg hazánkban a jogalkotók részéről azon törvényi módosítás, amely a telemedicina működését mind szabályozás, mind finanszírozási oldalról egyaránt támogatta.
A szerzők a tanulmányban arra keresik a választ, hogy a konvencionális egészségügy mellett a telemedicinális rendszer felfogható-e mint önálló entitás, és ennek jogán a közeljövőben alkalmassá válik-e majd arra, hogy a törvényi szabályozás szerint a létfontosságú rendszeri besorolással járó fokozott védelmi prioritást élvezzen.

Kulcsszavak: **Covid-19-világjárvány, kritikus infrastruktúra, létfontosságú rendszer, védekezési stratégia, telemedicina, eHealth, mHealth, kibervédelem, kiberjog**

At the moment, telemedicine can be characterised as a field which lays on the border of multiple specialties, however, in the course of the coronavirus pandemic, it gained a special role and it appears increasingly as a stand-alone domain, therefore, the aim of the authors is to shed a light on its remarkable headway.
The restrictions that arise from the nature of the disease as well as the simultaneously rising need of the population for healthcare collectively turned the focus of the healthcare system to telemedicine. As a result, the national lawmaker assisted

[1] Szövetséges Fegyveres Erők Összhaderőnemi Parancsnokság, Egészségügyi Főnökség, egészségügyifőnök-helyettes, Nápoly, Olaszország; e-mail: fejes.zsolt@hm.gov.hu, ORCID: https://orcid.org/0000-0002-1387-2970
[2] Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, doktorandusz, e-mail: marcell.helyes@gmail.com, ORCID: https://orcid.org/0000-0001-9458-3160

the functioning of telemedicine with a legislative amendment on a regulatory as well as on a financing level.
In this study the authors seek to address the question whether, besides the conventional health, telemedicine can be seen as a stand-alone entity. If so, based on this, it will be suitable to be classified as a critical infrastructrure in the near future, which would mean that telemedicine could enjoy the protection of an increased defence priority.

Keywords: **COVID-19 pandemic, critical infrastructure, defence strategy, telemedicine, eHealth, mHealth, cyber defence, cyber law**

1. Bevezető

Az Egészségügyi Világszervezet (WHO) által 2020. március 11-én kihirdetett[3] globális egészségügyi vészhelyzet földünk valamennyi kontinensét és teljes lakosságát érintette.

A Covid-19-világjárvány kitörésével 2020-ban olyan kihívással szembesültünk, amely megrengette biztonságérzetünket, próbára tette felkészültségünket, és felhívta a figyelmet sebezhetőségünkre.

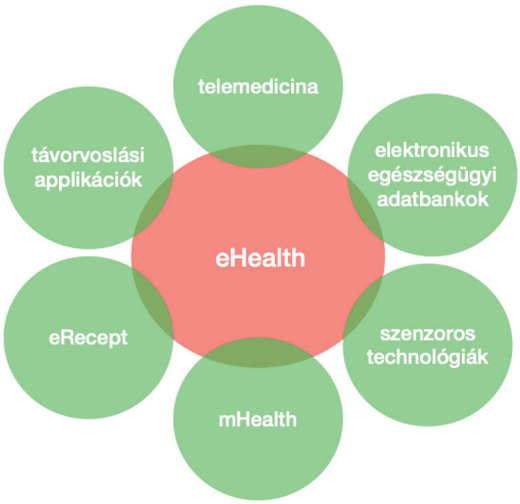
Hónapok óta, eltérő intenzitással, mégis folyamatosan érezzük a járvány közvetlen következményeit, találgatjuk jövőbeni alakulását. Tekintve, hogy hónapokon át zajló eseményről van szó, a pandémia által ténylegesen okozott károkról nincsenek még pontos adataink, ezekre majd csak a későbbi elemzések derítenek fényt.

Jelenünk története megmutatta, hogy hasonló, globális események bekövetkezésével a jövőben is számolnunk kell, ezekre védekezési stratégiákat kell kidolgoznunk. Ezen védekezési stratégiák egyike lehet a lakosság folyamatos és biztonságos egészségügyi ellátásának tervezése a koronavírus által megváltoztatott működési környezetben, ahol a betegellátás egyes elemei (adminisztráció, leletek-eredmények kiértékelése, konzultáció, tanácsadás) a virtuális térbe helyeződnek át, és a telemedicina eszközkészletét használva létesítenek kapcsolatot orvos és beteg között.

A Covid-19-pandémia teljesen felborította a világ korábbi működési rendjét, rövid hónapok leforgása alatt alapjaiban forgatta fel a Föld lakosságának mindennapjait. Azonban úgy tűnik, egy pozitív hozadéka mégiscsak van a járványnak, mégpedig hogy a preventív jelleggel drasztikusan redukált személyes kapcsolatok a korábbinál még jobban előtérbe helyezték az eHealth, mHealth, illetve a telemedicina-szolgáltatások által biztosított forradalmi lehetőségeket. Míg az utóbbi időben elterjedt eHealth a telemedicina egy kitágított meghatározása és így a távdiagnosztika és a távmonitorozás mellett az általános egészségügyi felvilágosítást, prevenciót, illetve terápiás foglalkozásokat is magában foglalja, addig az mHealth kifejezés ezen szolgáltatások mobileszközön történő biztosítását takarja.[4]

[3] World Health Organization: *A 2020. március 11.-én megtartott COVID-19-el kapcsolatos virtuális sajtókonferencia lenyomata*. 2020. március 11.

[4] Varga Zsuzsa – Horváth Tamás: Betegpreferenciák az egészségügyi célú internethasználatban. *Orvosi Hetilap,* 159. (2018), 51. 2175–2182.



1. ábra
Az e-egészségügy különböző területei.
Forrás: a szerzők saját szerkesztése

Cikksorozatunk első részében a telemedicina osztrák és magyar jogi szabályozását vetettük össze. Megállapítottuk,[5] hogy hazánkban az akkori, telemedicinára vonatkozó jogszabályi környezet meglehetősen széttöredezett és hiányos volt, szemben az Ausztriában tapasztaltakkal. Magyarország vonatkozásában jellemzően egymástól különálló törvények tettek említést a telemedicina területéről, mint az egészségügyi rendszer lehetséges szolgáltatási módjáról, azonban önálló telemedicina-törvény nem állt rendelkezésre. Noha számos kérdés továbbra is nyitott a telemedicina gyakorlatával kapcsolatban, azonban a Covid-19-pandémia következtében kihirdetésre került a veszélyhelyzet során elrendelt egyes egészségügyi intézkedésekről szóló 157/2020. (IV. 29.) Korm. rendelet immáron jogalapot biztosít a telemedicinális ellátás teljes spektrumára. A rendelet ugyanis kijelenti, hogy megengedett a telemedicinális szolgáltatások nyújtása, nem szükséges feltétlen a személyes jelenlét, továbbá előírja az egészségügyi szolgáltatók számára az Elektronikus Egészségügyi Szolgáltatási Térben a vizsgálat tényét és szereplőit dokumentáló eseménykatalógus-bejegyzésre, illetve egy, a vizsgálatot szakmai szempontból igazoló elektronikus kórtörténeti dokumentum feltöltésére vonatkozó kötelezettséget. Sőt, arról is rendelkezik, hogy amennyiben állapotromlás vagy akár maradandó egészségügyi károsodás veszélye merül fel, úgy a beteg távellátása megszakítandó.

[5] Fejes Zsolt – Helyes Marcell – Mihók Sándor: A telemedicina jogi szabályozása az Európai Unió két tagországában. *Hadmérnök,* 15. (2020), 4. sz.

Ezen mérföldkő egyértelműsíti, hogy a szakma mellett a jogalkotó is kész a kibertér mint a betegellátás 21. századi módja felé nyitni, azt törvényhozás útján, jogbiztonságot teremtve támogatni, elősegíteni.

Azonban a telemedicina jogszabályba foglalása okán aktuálissá vált a kérdés, hogy az ország egészségügyi rendszerének virtuális kiterjesztése, illetve bizonyos szolgáltatások esetlegesen kizárólag kibertéri biztosítása által keletkező biztonsági kockázatokat hogyan, milyen módon lehetséges jogszabályi úton minimalizálni. Ilyen kockázatként említhető például, hogy a betegellátás nélkülözhetetlensége, de ugyanakkor a rendszer magas fokú sérülékenysége okán Európában az utóbbi évek kibertámadásainak célkeresztjében legnagyobb arányban egészségügyi szolgáltatók, így kórházak, egészségközpontok és különféle egészségügyi adatbankok álltak.[6] További veszélyforrást jelent az is, hogy a telemedicina jellegéből fakadóan együtt jár a páciensek különösen érzékeny egészségügyi adatainak elektronikus úton történő tárolásával, feldolgozásával és továbbításával.

Friss, hazai példaként említendő a Nemzeti Kibervédelmi Intézet által kiadott riasztás,[7] amely az Emotet malware fertőzésre hívja fel a figyelmet. Az eredetileg banki szektorban alkalmazott trójai, amely a személyes adatok ellopásától kezdve zsarolóvírus telepítéséig mindenre alkalmas, az Intézet honlapján közzétett felhívás szerint egy ideje magyar egészségügyi intézmények infrastruktúrája ellen került felhasználásra.

A fentiek tükrében jelen cikk Magyarország létfontosságú rendszereinek szemszögéből kíván rávilágítani a leírt kihívásokra azon kérdéskör elemzésével, hogy az állami telemedicinális szolgáltatásokat a hatályos jogszabályi keret értelmében lehetséges-e létfontosságú rendszereknek minősíteni, részesülhetnek-e ezek a besorolással járó, kiemelt védelemben? Feltételezhető ugyanis, hogy a telemedicinális betegellátás egyes elemeinek és teljes adminisztrációjának kibertérbe helyezésével járó nemzetbiztonsági kockázatot csak ilyen módon lehet kellő mértékben ellensúlyozni. A kijelölési kritériumok mielőbbi kidolgozása azért szükséges, mert ezen keretrendszeren belül állapítható meg, hogy milyen feltételek mellett, mely szolgáltatásokat és mely szolgáltatókat szükséges ebben a védelemben részesíteni.

2. A telemedicina mint nemzeti létfontosságú rendszer

Mind az egészségügy „klasszikus" formája mint infrastruktúra, mind egyes infokommunikációs technológiák (például internet-hozzáférési szolgáltatások, elektronikus hírközlés vagy éppen a kormányzati elektronikus információs rendszerek), külön-külön az ország kritikus infrastruktúráinak részét képezik.[8] Tekintve, hogy a telemedicina ezen két terület határán fekszik, és mindkét ágazati elemhez szervesen kapcsolódik, felmerül a kérdés, hogy a telemedicina mint önálló domén, kritikus infrastruktúraként értelmezhető-e már napjainkban? Amennyiben a telemedicina egy vagy több

[6] Vectra identifies healthcare as the industry most targeted by cyber attacks. *Vectra Networks,* 2017. június 7.
[7] Nemzeti Kibervédelmi Intézet: *Riasztás egészségügyi intézményeket érintő Emotet terjesztési kampánnyal kapcsolatban*.
[8] 2012. évi CLXVI. törvény 1. melléklet.

szolgáltatási altípusa kielégíti a kritikusinfrastruktúra-elem definíciójának megfelelő kritériumokat, akkor a vonatkozó hazai (nemzeti, katonai, egészségügyi) stratégia kialakításának következő lépése annak kidolgozása, hogy milyen módon alkalmazandók az érvényben lévő vonatkozó szabályozások, milyen kiegészítő szabályok megalkotása szükséges, illetve hogy hogyan lehetséges a területvédelmi szempontok – törvényalkotás, jogszabály – szerinti, valamint konkrét fizikai elemekkel történő biztosítása. Ugyancsak eldöntendő kérdés, hogy a pandémia okán a jelenleg kialakult különleges helyzetre reagálva az annak kezelését megkövetelő új szabályrendszer kialakítására célszerűbb-e törekednünk, vagy a meglévő szabályzóinkkal próbálunk egy eddig nem ismert helyzetet hatékonyan kezelni.

A 2008. december 8-i 2008/114/EK, az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló uniós irányelvvel összhangban hazánkban a kritikus infrastruktúrák jogállását a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Lrtv.), valamint a hozzá tartozó, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet (LrtvVhr.) tisztázzák. Emellett a telemedicina vonatkozásában kiemelendő a 246/2015. (IX. 8.) az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló ágazati kormányrendelet is, amely a fent említett általános rendelkezéseket kiegészítve meghatározza az egészségügyre vonatkozó speciális szabályokat.

Érdekesség, hogy a nemzetközileg használatos kifejezésekkel ellentétben ezen szabályzók terminológiájának megfelelően magyar viszonylatban létfontosságú rendszerekről és létesítményekről beszélhetünk, nem pedig kritikus infrastruktúrákról, de ez pusztán megnevezésbeli, nem pedig tartalmi különbség.

Az Lrtv. 1. § *j)* pontjában található meghatározás szerint létfontosságú rendszerelemnek minősül minden olyan szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, és amelyek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna. A törvény továbbiak mellett kifejezetten említi az egészségügyet mint létfontosságú rendszert. A kibertérben megvalósuló betegellátás sajátossága, hogy a szolgáltatás természetéből fakadóan minden esetben két oldalról szemlélendő a tevékenység, hiszen egyszerre alkalmazandóak rá az egészségügyi és az infokommunikációs szabályozások is. Ebből fakadóan, amikor a telemedicinának az Lrtv. 1. melléklete szerinti ágazati besorolását szeretnénk meghatározni, felmerülhet a kérdés, hogy az egészségügyi ágazat mellett esetleg az infokommunikációs technológiák ágazat alá is besorolható-e az e-egészségügy mint létfontosságú rendszer. Bár a szabályozás jelenleg hatályos szövegezése ezt nem teszi lehetővé, viszont tekintettel a telemedicina infokommunikációtól való függésére, elképzelhető, hogy ezen terület a jövőben nemcsak egészségügyi, de elektronikus információs rendszer alapon is védelemre lesz jogosult. Ez a tény a SARS Covid-19-világjárvány idején kiemelt jelentőségű mind jogalkotói, mind egészségügyi vezetés-irányítási és egészségügyi tervezői szempontból egyaránt.

A létfontosságú rendszerelemek (kiber)védelme alatt – de lege lata – azon tevékenységek értendők, amelyek a létfontosságú rendszerelem funkciójának, folyamatos működésének és sértetlenségének biztosítását célozzák, illetve a fenyegetettség, a kockázat, a sebezhetőség enyhítésére vagy semlegesítésére irányulnak.[9] Kiemelendő továbbá a fogalommeghatározások közül az üzemeltető és a rendkívüli esemény kifejezések. Előbbi alá azon természetes és jogi személyek, illetve jogi személyiség nélküli szervezetek esnek, akik vagy amelyek az eszköz, létesítmény, rendszer rendszerelemének tulajdonosai, engedélyesei, rendelkezésre jogosultjai vagy napi működéséért felelősei. Definíció szerint rendkívüli esemény minden olyan külső vagy belső behatás, amely a kijelölt nemzeti vagy európai rendszerelem rendeltetésszerű működését, üzemfolytonosságát jelentős mértékben veszélyezteti, akadályozza.[10]

Az Lrtv. általános jellegű szövegezését a telemedicina kibervédelmének területére vonatkoztatva a következők állapíthatók meg. Legyen szó egy Dos/DDos-támadásról vagy éppen egy, a rendszerbe juttatott zsarolóvírusról, minden, a kiber-egészségügyi rendszer rendszerelemeinek működését negatívan befolyásoló (azt átmenetileg feltartóztató vagy akár teljesen ellehetetlenítő) rendkívüli esemény ellen kiemelt védelemre van szükség. Ugyancsak fontos kiemelni, hogy az egészségügyi szolgáltatók elektronikus adatbázisaiban tárolt, feldolgozott, továbbított érzékeny egészségügyi adatok ellen irányuló behatások, amelyek során elsődlegesen az adatok törlése, lopása, illetve a velük való visszaélés a cél, szintén magasfokú nemzetbiztonsági kockázatot jelentenek, ezért ezen adatbázisok létfontosságú rendszerelemként történő védelmi besorolása szükségszerű.

A biztosítandó kibervédelem köre kiterjed egyfelől a távorvoslás során használt kép-, hang-, fájlmegosztó programok, másfelől az eHealth-rendszer szerves részét képező adatbankok megfelelő szintű kiberbiztonságára is. Ezen kihívások elsősorban az üzemeltető által foglalkoztatott informatikus szakemberek feladatkörét képezik. Ettől függetlenül azonban az e-egészségügyi rendszer egyes létfontosságú rendszerelemeinek résztvevőire vonatkozó biztonsági protokollok kidolgozása is szükséges, ugyanis a legjelentősebb kiberbiztonsági rést továbbra is az emberi komponens jelenti. Jól példázza ezt a fent említett Emotet-ügy is, amely során a vírus elektronikus levelekhez csatolt futtatható állományként lett megküldve a felhasználóknak, akik azt óvatlanságból megnyitották, ezzel utat engedve a kártevőnek. Megfelelő felkészítés és az e-egészségügyi rendszer használatára vonatkozó biztonsági előírások kidolgozása és betartatása mellett az ilyen és ehhez hasonló támadások sikere megelőzhető, de legalábbis drasztikusan csökkenthető.

3. Kijelölési kritériumok

Arra a kérdésre, hogy pontosan milyen eljárásrend lefolytatásával kerülhetnek a jövőben a létfontosságú telemedicinális rendszerelemek kijelölésre, és ennek megfelelően kik jelölhetők meg az eHealth-rendszerek vonatkozásában üzemeltetőnek, terjedelmi

[9] 2012. évi CLXVI. törvény 1. § *i)* pontja.
[10] Uo. 1. § *l)* és *m)* pontjai.

okok miatt jelen cikkünkben nem térünk ki. Általánosságban azonban kijelenthető, hogy az említett ágazati kormányrendelet értelmében[11] a kiberegészségügyi rendszerelemek kijelölése során az Állami Egészségügyi Ellátó Központ, illetve a hamarosan helyébe lépő Országos Kórházi Főigazgatóság (aktív fekvőbeteg-ellátás és a működtetéséhez szükséges szolgáltatások; egészségügyi tartalékok), az Országos Mentőszolgálat (mentésirányítás), az Országos Vérellátó Szolgálat (vérkészletek), az országos tisztifőorvos (magas biztonsági szintű biológiai laboratóriumok), illetve az Országos Gyógyszerészeti és Élelmezés-egészségügyi Intézet (gyógyszer-nagykereskedelem) az illetékes javaslattevő hatóságok. Az ágazati kijelölő hatósági feladatokat pedig az egészségügyért felelős miniszter látja el.

A klasszikus ágazati egészségügyi kritériumokra[12] alapozva feltételezhető, hogy az egyes távorvoslási rendszerek létfontosságúnak jelölése során az általuk kiszolgált felhasználók száma, illetve a szolgáltatás zavartalan biztosításának fontossága lesznek a mérvadó szempontok. Ezen ágazati kritériumok közül egy teljesülése elegendő, azonban a létfontosságúvá nyilvánításhoz meg kell felelnie a teleszolgáltatásnak egy horizontális kritériumnak is. Az LrtvVhr. 1. melléklete értelmében a lehetséges kategóriák a következők:

- gazdasági hatás kritériuma,
- politikai hatás kritériuma,
- társadalmi hatás kritériuma,
- környezeti hatás kritériuma,
- veszteségek kritériuma,
- védelem kritériuma.

Az e-egészségügy vonatkozásában elsősorban a védelem kritériuma releváns, amely a törvény értelmében akkor teljesül, ha az infrastruktúrában bekövetkező sérülés, zavar, állapot, esemény vagy folyamat következtében a rendszerelem ellátási láncban betöltött szerepét nem tudja ellátni, illetve sérülése vagy megsemmisülése esetén a beavatkozás, mentés vagy kárfelszámolás ideje aránytalanul megnövekszik. Amennyiben a betegellátás egy jelentős része átkerül az online térbe, és a páciensek számára például csak virtuálisan elérhetők egészségügyi adataik, vagy éppen csak videótelefonon tudnak konzultálni kezelőorvosukkal, nem is kérdés, hogy milyen károkat okozhat ezen rendszerek átmeneti vagy tartós elérhetetlensége.

Emellett – bár a szerzők elismerik ezen szcenárió bekövetkeztének jelenlegi valószínűtlenségét – egy jövőbeni, az ország mostaninál szélesebb körű és meghatározóbb e-egészségügyi rendszere ellen irányuló, szervezett kibertámadás okozhat olyan, nagy mértékű leállást, amely kétségkívül a nagyvárosok köznyugalmának súlyos megzavarásához vezethet. Így, bár a jelenleg alkalmazott egészségügyi technológiai rendszerek és elterjedtségük szintje ezt nem indokolja, a jövőben mégis elképzelhető, hogy a védelem kritériuma mellett a társadalmi hatás kritériuma szintén alapot biztosíthat a telemedicinális szolgáltatások létfontosságúvá nyilvánításához.

[11] 246/2015. (IX. 8.) Korm. rendelet 2. §.
[12] 246/2015. (IX. 8.) Korm. rendelet 4. §.

4. Összegzés

Összességében megállapítható, hogy nincs elvi akadálya annak, hogy az e-egészségügy rendszerének egyes szolgáltatásait, így bizonyos telemedicinális eljárásokat is, létfontosságú rendszereknek minősítsenek. Annak érdekében, hogy a technológiai fejlődéssel együtt járó, biztonsági kihívásokra reagáló védelmi mechanizmusok is kialakuljanak, a cikk szerzői fontosnak látják telemedicinális kibervédelmi stratégia megalkotását. Ennek feltétele, hogy első lépésben a telemedicinális szolgáltatások egyre szélesebb körű biztosításával párhuzamosan szisztematikusan kijelölésre kerüljenek a létfontosságú rendszereknek minősülő e-egészségügyi szolgáltatók és szolgáltatások. Olyan stratégiai elképzelések kialakítására van szükség nemzeti, katonai és egészségügyi szinten egyaránt, amelyek az érvényben lévő jogszabályi keretek kiegészítésével és továbbfejlesztésével a jövőben kritikus infrastruktúraként definiálják a telemedicinát.

A szerzők ugyancsak megfontolásra javasolják a vonatkozó jogszabályok által előírt védelmi képességek létrehozása és fenntartása érdekében használati protokollok kidolgozását egyes telemedicina-médiumokra, valamint a felhasználók rendszeres és folyamatos képzését, kibervédelmi tudatosságuk folyamatos növelését.

Felhasznált irodalom

157/2020. (IV. 29.) Korm. rendelet a veszélyhelyzet során elrendelt egyes egészségügyi intézkedésekről.

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.

Fejes Zsolt – Helyes Marcell – Mihók Sándor: A telemedicina jogi szabályozása az Európai Unió két tagországában. *Hadmérnök,* 15. (2020), 4. sz. Online: https://doi.org/10.32567/hm.2020.4.13

Nemzeti Kibervédelmi Intézet: *Riasztás egészségügyi intézményeket érintő Emotet terjesztési kampánnyal kapcsolatban*. Online: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-egeszsegugyi-intezmenyeket-erinto-emotet-terjesztesi-kampannyal-kapcsolatban/

Varga Zsuzsa – Horváth Tamás: Betegpreferenciák az egészségügyi célú internethasználatban. *Orvosi Hetilap,* 159. (2018), 51. 2175–2182. Online: https://doi.org/10.1556/650.2018.31210

Vectra identifies healthcare as the industry most targeted by cyber attacks. *Vectra Networks,* 2017. június 7. Online: www.vectra.ai/news/vectra-networks-identifies-healthcare-as-the-industry-most-targeted-by-cyber-attacks

World Health Organization: *A 2020. március 11.-én megtartott COVID-19-el kapcsolatos virtuális sajtókonferencia lenyomata*. 2020. március 11. Online: www.who.int/docs/default-source/coronaviruse/transcripts/who-audio-emergencies-coronavirus-press-conference-full-and-final-11mar2020.pdf?sfvrsn=cb432bb3_2