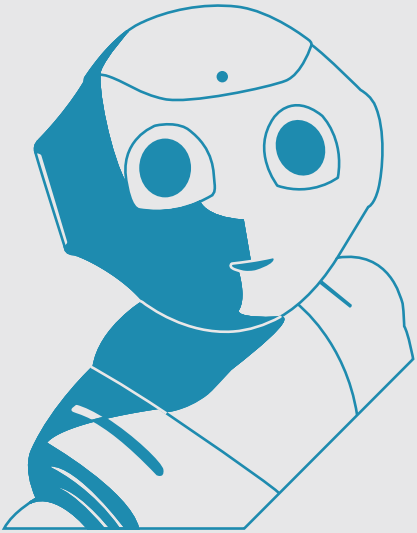
PÉCSI TUDOMÁNYEGYETEM
UNIVERSITY OF PÉCS

A TECHNOLÓGIA ÉS A JOG KORRELÁCIÓJA



Szerkesztette:
BÉKÉSI GÁBOR
KISS MÁTYÁS
VÁRALLAI LUCA

Pécsi Tudományegyetem Állam- és Jogtudományi Kar
Irás Nándor Szakkollégium

Pécsi Tudományegyetem Állam- és Jogtudományi Kar
Óriás Nándor Szakkollégium

A technológia és a jog korrelációja

Pécs, 2022

Szerkesztette:

Békési Gábor
Kiss Mátyás
Várallai Luca

A kötetet lektorálták: Csoknya Tünde Éva, Hengl Melinda, Kis Kelemen Bence, Mohay Ágoston (PTE ÁJK), és Pál Előd (Sapientia EMTE)

ISBN 978-963-429-989-9

Kiadja a Pécsi Tudományegyetem Állam-és Jogtudományi Kar Óriás Nándor Szakkollégiuma.

Székhely: 7622 Pécs, 48-as tér 1

Felelős kiadó: Dr. Fábián Adrián, dékán

Pécs, 2022

Technikai szerkesztő, fedélterv: www.netglobal.hu

Készült az Emberi Erőforrások NTP-SZKOLL-21-0018 sz. Nemzeti Tehetség Program pályázat keretében.

Tartalomjegyzék

Szerkesztői előszó

A Pécsi Tudományegyetem Állam- és Jogtudományi Kar Óriás Nándor Szakkollégiuma a pécsi jogi kar legkiválóbb hallgatóinak önszerveződő csoportja. A szakkollégium célja és rendeltetése az, hogy a tagok szakmai fejlődésében segítséget nyújtson, hozzásegítse a tagokat korszerű és magas színvonalú elméleti és gyakorlati tudás megszerzéséhez, és egyidejűleg pozitív közösségi élményekkel gazdagítsa tagjainak életét, valamint társadalmi szerepvállalás keretében támogassa a rászorulókat és egyúttal fejlessze a hallgatók szociális érzékenységét. A Szakkollégium négy tagozatban folytatja tevékenységét: Bűnügyi, Civilisztika, Elméleti-történeti és Közjogi tagozat.

A jelen kötet az Emberi Erőforrások NTP-SZKOLL-21-0018 sz. Nemzeti Tehetség Program pályázati projekt keretében készült, amelyben a Szakkollégium arra vállalkozott, hogy egy egyéves kutatás során különböző szempontokon keresztül vizsgálja a technológia és a jog kapcsolatát, amelyhez remek alapot ad a Szakkollégium négy tagozatában, mint műhelyekben folyó szakmai munka. A kötetbe azonban nem csak az Óriás Nándor Szakkollégium tagjai, hanem a kolozsvári Collegium Iuridicum szakkollégistái is küldtek írásokat. A Collegium Iuridicum hallgatói a két szakkollégium között kialakult, és reményeink szerint egyre intenzívebbé váló együttműködés okán kaptak lehetőséget a kötetben történő publikálásra.

A tanulmányok számos különböző témát dolgoznak fel, amelyek között az összekötő kapcsot a technológia jogi dimenziói jelentik. Szerzőink vizsgálták többek között az országgyűlési választások digitalizációjának lehetőségét Magyarországon, a véleménynyilvánítás szabadsága és a gyűlöletbeszéd közötti határ kérdéskörét az online térben, valamint a kiberbűncselekmények elleni küzdelem eseteit. Ezek mellet olyan írások is helyet kapnak a kötetben, melyek például a pénz fogalmával foglalkoznak a modern számítástechnikai vívmányok fényében, vagy a jogos védelem kibertéri vonatkozásait vizsgálják, illetve az online vitarendezéssel kapcsolatos kérdéseket tárják fel az 524/2013/EU rendelet tükrében. A kötetben a szerzők foglalkoznak továbbá a szuperintelligens robotok jogalanyiságának egyes kérdéseivel a klasszikus magánjogi gondolkodás tükrében, a félvezetők topográfiájának védelmével, valamint az otthonunkban fellelhető smart megoldások adatvédelmi, energiajogi vonatkozásaival.

Bízunk benne, hogy a kötettel hozzájárulunk egy olyan komplex és sok vitás kérdést felvető kapcsolatrendszer bemutatásához és jobb megértéséhez, mint a technológia és a jog egyes kapcsolódási pontjai.

Szeretnénk köszönetet mondani minden szerzőnek, lektornak és a Collegium Iuridicum tagjainak és vezetőségének. Reméljük, hogy e kötet hozzájárul a technológia és a jog problémakörének árnyalt szakmai elemzéséhez.

Kelt Pécsett, 2022. május 24. napján

A Szerkesztők

Balla Bulcsú
szakkollégista, Collegium Iuridicum

Szabó Kriszta
szakkollégista, Collegium Iuridicum

Jogos védelem a kibertérben

I. Bevezetés

A 21. század számtalan kihívást rejt magában, de talán napjaink egyik legnagyobb kihívását mégiscsak az internet, a kibertér és az eköré csoportosuló problémák jelentik. Az információs forradalomnak köszönhetően új szemléletek, értékrend változások láttak napvilágot, a prioritások felcserélődtek, az egyén figyelme pedig a digitális eszközök és azoknak köszönhetően az internet köré összpontosult. Mi magunk ennek a népességnek az alakjaiként muszáj realizálnunk a téma fontosságát és fontos, hogy tisztában legyünk az erre vonatkozó jogi szabályozásokkal.

Az információs társadalom fogalma kapcsán jelenleg sem alakult ki konszenzus, hiszen eltérően értelmezi az információelmélet, az informatika vagy a társadalomteória. A legtöbbek által elfogadott és idézett meghatározást Fodor István fogalmazta meg, aki szerint az információs és kommunikációs technológia térhódításának és elterjedésének következményeképpen kialakult egy új társadalmi berendezkedés, új világlátás, ehhez való alkalmazkodás pedig kihatott a gyártó-és szolgáltató ipar, valamint a média területére is. Egy globális jelenséggel állunk szemben, ezt „a széles körben új életmódot, magatartást, információs technológiával átszőtt gazdaságot nevezzük információs társadalomnak".[1]

Az okos eszközök révén könnyedén hozzáférhetővé vált internet, magában rejt bizonyos veszélyeket, gondolhatunk itt a megbízhatóság kérdésére, a hitelesség és identitás elvesztésére vagy az agresszió jelenlétére.[2] Ezekből kifolyólag, az információs

[1] *Jakobi* Ákos: Az információs társadalom térbelisége. ELTE Regionális Tudományi Tanszék, Budapest 2007. 10. o.

[2] *Pintér* Róbert: Úton az információs társadalom megismerése felé. In: Az információs társadalom (szerk. *Pintér* Róbert). Gondolat – Új Mandátum, Budapest 2007. 12. o.

társadalom legfőbb értékét nem más képezi, mint maga az információ, elsősorban annak védelme azokkal szemben, akik jogosulatlanul férnek hozzá, használják fel azt. Felmerült többek között az a dilemma is, hogy lehetséges-e a jogos védelem a kibertérben, és ha igen milyen feltételek kell, hogy teljesüljenek ennek megvalósulásához. A kérdés vizsgálata a továbbiakban a Román Büntető törvénykönyv (a továbbiakban Rbtk.) előírásain alapszik, ugyanis a jogalkotó egzakt módon mindeddig nem tért ki ennek szabályozására.

A kibertérhez szorosan kapcsolódó mesterséges intelligencia (MI) fejlődése olyan, eddig ismeretlen kérdéseket vet fel, mint például az ilyen entitások büntetőjogi felelősségre vonása. Az MI által elkövetett cselekedetek tekintetében különbséget kell tennünk, hogy mikor minősül az MI az elkövetés eszközének és mikor válik ő maga elkövetővé.

II. A jogos védelem fogalma a román büntetőjogban

Mielőtt megvizsgálnánk a kibertérben jogos védelemben való fellépés lehetőségét, indokoltnak tartom az Rbtk. előírásainak rövid ismertetését. A jogos védelmet az Rbtk. a jogellenességet kizáró okok közt a 19. cikkben szabályozza, amelynek (1) bekezdése szerint nem minősül bűncselekménynek a jogos védelemben végrehajtott cselekedet. A (2) bekezdés szerint „*[j]ogos védelemben cselekszik az a személy, aki azért követi el a cselekményt, hogy elhárítsa az ellene, más személyek vagy azok jogai ellen, illetve a közérdek ellen irányuló fizikai, közvetlen, azonnali és jogtalan támadással keletkezett veszélyt, amennyiben a védelem arányos a támadással.*" A jogos védelmi helyzet fennállásához, az előbb említett törvényszövegbe foglalt összes feltétel egyidejű teljesülése szükséges, ellenkező esetben a védekező személyt cselekedeteiért büntetőjogi felelősség terheli. A jogos védelemben való cselekvés legelső feltétele, az azt megelőző fizikai jellegű támadás, amely bármilyen a büntetőjoggal ellenkező cselekedet formáját magára öltheti. Fizikai támadásnak minősül, bármilyen olyan magatartás, amely a megtámadott érték fizikai megnyilvánulását fenyegeti.[3] Nem keletkeztet jogos védelmi helyzetet sem az írásban vagy szóban megnyilvánuló támadás[4], illetve a védekező személy azon szub-

[3] *Udroiu* Mihail: Drept penal: partea generală; Noul Cod penal [Büntetőjog: Általános rész; Új Büntető törvénykönyv]. C.H. Beck, Bukarest 2014. 61. o.

[4] Bukaresti Ítélőtábla, I. büntetőjogi kollégium, 120/A//2003. döntés; *Streteanu* Florin: Tratat de drept penal. Partea generală. Volumul I. [Büntetőjogi kézikönyv. Általános rész. I. kötet]. C.H. Beck,

jektív meggyőződése sem, hogy amennyiben nem cselekszik, a másik fél támadásba lendülhet. Fontos kiemelni azt is, hogy a támadás nem csak aktív magatartás formájában képzelhető el, mivel bizonyos esetben a mulasztás is minősülhet támadásnak, amennyiben a támadó személy nem tesz eleget egy cselekvési kötelességnek (klasszikus példaként hozható fel az az eset, ha az anya nem táplálja gyermekét). A veszély közvetlenségét illető feltétel teljesüléséhez szükséges, hogy a támadás közvetlen veszélyt jelentsen valamilyen társadalmi érdekre nézve, ne legyen semmilyen olyan akadály a támadó és a védekező között (például fal vagy ajtó), ami ellehetetlenítené a támadás tényleges kimerülését a védekező személlyel szemben. Azonnalinak tekinthető a támadás, abban az esetben, ha valamilyen veszéllyel fenyegeti a védelmezett társadalmi értéket és ennek kialakulása már megkezdődött vagy biztos. Minden olyan magatartás és cselekedet tehát, ami veszély kialakulását vonja maga után azonnali támadásnak minősül, kivéve, ha a veszélyhelyzet kialakulása csak esetleges, ugyanakkor nem keletkeztet jogos védelmet a támadás akkor sem, ha ennek megkezdése és a veszély kialakulása közti idősáv elég tág ahhoz, hogy azt törvénybe nem ütköző módon is el lehessen hárítani.[5] Azonnali támadások esetén a jogos védelem általában a támadás kimerülésének pillanatáig áll fenn (amíg védekező személy objektíven tarthat attól, hogy a támadás megkezdődik vagy folytatódik), illetve bizonyos esetekben ennek kimerülése után is, ha a védekező objektíven feltételezheti, hogy a támadás újra kezdődik (például az agresszor lefegyverzése után, a fegyver visszakerül hozzá). A támadás jogtalan jellege, annak a jogrendbe ütköző voltából következik, vagyis jogtalan támadásnak minősül bármely cselekedet, ami a hatályos jogrend által nem engedélyezett. A jogos védelmi helyzetet keletkeztető támadás utolsó feltétele, hogy az a védekező személy ellen, más személy ellen, ezek jogai ellen vagy egy általános érdek ellen irányuljon. Mivel az Rbtk. lemondott, a veszély súlyosságának követelményéről, így gyakorlatilag bármilyen támadás elhárítható jogos védelem keretében, amennyiben a veszély és a védekezés közti arányosság feltétele teljesül.

A védelemre vonatkozó feltételeket a jogszabály szövege nem sorolja fel tételesen, ezek a támadásra vonatkozó feltételekből következnek. Az első feltétel, hogy a védelem legyen szükséges, vagyis előzze meg egy olyan fenyegető támadás, ami veszélyhelyzet kialakulását eredményezi. A védelem akkor tekinthető szükségesnek, ha az elhárítási

Bukarest 2008. 478. o.

[5] *Pașca* Viorel: Drept penal: partea generală Ed. a 4-a [Büntetőjog: általános rész 4. kiadás]. Universul Juridic, Bukarest 2015. 205. o.

aktusra a támadás befejezése előtt kerül sor, ha a védekezés elkésett és a támadás már tekinthető valós veszélynek az adott értékre a védekező személyt büntetőjogi felelősség terheli. Fontos kiemelni, hogy a szükségesség nem jelenti azt, hogy a bűncselekmény elkövetése a védekező személy egyetlen menekülési vagy mentési lehetősége kell legyen. Felmerül a kérdés, hogy felróható-e egy cselekedet, amelyet a támadóval szemben jogos védelemben követnek el, de az harmadik személyek számára is károkat keletkeztet (például egy botnet hálózat teljes kiiktatása, amely a fertőzött számítógépekben is kárt okoz). Véleményem szerint, ilyen esetben inkább a végszükségre lehet hivatkozni, ugyanakkor ennek hatása a jogos védelméhez hasonlóan, a büntetőjogi szankció kiszabásának ellehetetlenítése. Nem tekinthető jogos védelemben elkövetett cselekedetnek a védekezés, ha az a támadó személye helyett, annak tárgyai ellen irányul, kivéve ha a védekezés olyan eszközöket céloz, amelyeket az agresszor a támadás megvalósítására használ (például a támadás megvalósítására használt informatikai eszköz megrongálása).[6] A védelemre vonatkozó második feltétel, hogy a védekezés legyen arányos a támadással, vagyis a védekező személy által elkövetett cselekedet legyen kisebb vagy azonos súlyosságú mint a támadás.[7] Az arányosság vizsgálatakor figyelembe kell venni a támadás konkrét körülményei mellett a használt eszközöket és a támadó és megtámadott személy közti erőviszonyokat is. Az arányosság feltételének fontossága abban rejlik, hogy az Rbtk. lemondott a veszély súlyosságának követelményéről, így bármilyen intenzitású veszély elháríthatóvá vált jogos védelem keretében, a támadás és védekezés közti arányosság megtartásával.

III. A kibertér fogalma

William Gibson tudományos-fantasztikus szerző nevéhez kapcsolódik a kibertér, mint fogalom, aki a 1984-es Neurománc (*angolul: Neuromancer*) című regényében hivatkozik a kifejezésre.[8] Az általa leírt világot a számítógép-hálózatok alakították ki, a felhasználók milliárdjai mellett mesterséges intelligenciával ellátott lények is helyet kapnak benne.[9] Többek között az író a globális internet társadalmát vetíti elő. Az angolszász cyberspace

[6] *Streteanu*: i. m. 492. o.

[7] *Udroiu*: i. m. 64. o.

[8] *Mezei* Kitti: A kiberbűnözés szabályozási kihívásai a büntetőjogban. Ügyészek lapja 2019/4–5 sz. 21. o.

[9] *Berki* Gábor: A kibertér, annak veszélyei és kibervédelem jelenlegi helyzete Magyarországon. Nemzetbiztonsági Szemle 2018/3. sz. 5–21. o.

szóból honosodott meg a kibertér, ahogyan a cybercrime kifejezésből a kiberbűnözés. Hétköznapibb megfogalmazással élve a kibertér egy olyan virtuális valóság világa, ahol a számítógépek, az összekötő kommunikációs csatornák, a különböző alkalmazások és tárolt adatok egyaránt megtalálhatóak.

Több nézőpontból is találunk meghatározást erre vonatkozóan, gondolhatunk itt az Egyesült Államok haderejére vagy a NATO-ra. Az előbbi szerint „*a kibertér az információs környezet (information environment) részét képező globális tartomány (domain), ahol az információs környezet az információt gyűjtő, feldolgozó, terjesztő, és felhasználó személyek, szervezetek, és rendszerek összessége, a tartomány kifejezés pedig hadviselési tartományt (warfighting domain) jelöl.*"[10] A kibertér azt a virtuális teret írja le, ahol különböző információs folyamatok (adatszerzés, adatfeldolgozás) mennek végbe, valamint az elektronikai rendszerek elleni tevékenység és a védelem is valóra válik.[11]

Tehát a kibertér összekapcsolt információs rendszerek és hálózatok összessége. Ennek nem képezi részét a hálózatba nem csatolt számítógép. Önmagában az összeköttetés formája lényegtelen, legyen szó vezetékesről vagy vezetéknélküliről. Elmondható róla, hogy állandó változásban van, hiszen fejlődnek az okoseszközök, illetve egyre jobban elterjednek, továbbá átalakuláson mennek át a szolgáltatások, folyamatosan bővülnek az adatok. Az ekkora mértékű térhódításnak köszönhetően a felhasználók száma jelentősen megnövekedett. Ennek következményeként megjelentek a rosszindulatú felhasználók is, vagyis a támadás a kibertérből az egyszerű felhasználó ellen is egyre gyakoribbá és jelentősebbé válik.

IV. A kibertér a klasszikus bűncselekmények elkövetésének helyszíne vagy eszköze?

A kibertérből újabbnál újabb fenyegetések érkezhetnek. Ezen támadások alapvető célja az adatszerzéshez, -módosításhoz, annak bizalmasságához, sértetlenségéhez és rendelkezésre állásához köthető.[12] A körülmények, az elkövetők, az indítékok, valamint egyéb közrejátszó tényezők fényében több csoportba rendezhetőek ezek a bűncselekmények. A tanulmány alapjaiban elemzi a kiberbűnözést és a kapcsolódó leggyakoribb bűncse-

[10] *Munk* Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. Hadtudomány 2018/1. sz. 113–131. o.

[11] *Haig* Zsolt – *Kovács* László: Fenyegetések a cybertérből. Biztonságpolitikai szemle 2008/5. sz. 61–69. o.

[12] *Berki*: i. m. 5–21. o.

lekményeket, a kiberkémkedést, a kiberterrorizmust és a kiberhadviselést.

IV.1. Kiberbűnözés

Elsőként a vizsgálatom tárgyát a kiberbűnözés képezi, amelyet a következőképpen definiálhatunk: „számítógépen, illetve számítógépes rendszerek ellen elkövetett bűncselekmények."[13] Két fő csoportot különböztethetünk meg ezen belül. Az egyik azokat a bűncselekményeket összesíti, amelyeket kizárólag információs rendszerek segítségével lehet elkövetni – pl. számítógépekkel –, ezt nevezzük cyber-dependent crime-nak, azaz informatikai bűncselekményeknek. Ide sorolhatjuk a különböző vírusokat, kártevő programokat (*angolul*: *malware*), sőt, a hackertámadásokat is. Ettől szükségszerű megkülönböztetni a cyber-enabled crime kategóriát, amely a hagyományos bűncselekményeket öleli fel, (lásd: zsarolás, szerzői jogok sértése, zaklatás, csalás) és amelyek elkövetésének csupán az eszközét jelenti az információs rendszer.[14] Ezáltal a kiberbűnözés számtalan jogsértést és bűncselekményt magába foglalhat, nem csak az információs rendszer segítségével elkövetettek tartoznak ide, hanem a klasszikus bűncselekmények is.

Az informatikai bűncselekmények megnövekedése a digitalizációhoz kapcsolódó okos eszközök és net alapú szolgáltatások jelentős elterjedésének következménye, hiszen ezeket elsősorban számítógépek segítségével lehet végrehajtani. A kiberbűncselekményeknek két célja van: a számítógépes hálózatokba való jogellenes behatolás (például hackelés) és a számítógépes funkciók és a hálózati tér megzavarására vagy leépítése (például vírusok és DDoS-támadások).

A leggyakoribb megjelenési formái közé sorolható a malware típusú bűncselekmények, magyar terminológiában a kifejezés alatt mindenféle rosszindulatú szoftvert értünk.[15] Legismertebb fajtái a trójai, vírusok, férgek és banki kártevők, kémszoftverek. A malware mellett helyet kap a hackelés is, amelyet részletesebben tárgyalok a későbbiekben. Gyakori jelenségek a DoS és DDoS támadások (szolgáltatásmegtagadási vagy elosztott szolgáltatásmegtagadási támadás), ezek alatt azt a folyamatot értjük, amikor az internetes szervereket annyi kéréssel árasztják el, hogy azok nem tudnak időben

[13] lexiq.hu (2022. 05. 09)

[14] *Mezei*: i. m. 69. o.

[15] Malware – rosszindulatú alkalmazások. https://www.eset.com/hu/malware/ (2022. 05. 09.)

reagálni. Ennek következménye az összeomlás vagy lefagyás.[16]

További megjelenési forma a spam, azaz a kéretlen e-mail, amelyet álltalában tömegesen küldenek a címzetteknek, gyakorta pedig adathalász céllal vagy rosszindulatú szoftverek küldésére. Ezen e-mailek kiküldésére használják a rosszindulatú szoftverrel fertőzött számítógépeket, amelyek csoportját nevezik „botneteknek".[17]

Mielőtt rátérnék a cyber-enabled bűncselekményekre a hacktivizmus pár esetét szeretném kiemelni. A kibertérből érkező fenyegetések közül kiemelkedő helyet foglal el, a legtöbb beavatkozást a szólásszabadság, az információ szabad áramlásának és az emberi jogok védelmének jegyében követik el. Az egyik ilyen közismert csoport az Anonymous, amelynek tevékenysége az orosz-ukrán háborúban is megnyilvánult.[18] Már többször is előfordult, hogy a szóban forgó internetes közösség felkarolt egy ügyet és ennek kapcsán támadásokat indított cégek és kormányzatok ellen. Rendszerint túlterheléses támadással megbénítják a weboldalakat, amelyek ettől összeomlanak. Ismeretes esemény volt 2010-ben a Wikileaks-ügybe való beavatkozásuk. Wikileaks több ezer titkos amerikai diplomáciai és katonai iratot, információkat osztott meg a szólásszabadságra hivatkozva. Ezen cselekmény és az amerikai kormány politikai megnyilvánulásainak köszönhetően problémák adódtak finanszírozási téren, ugyanis a Visa, a MasterCard, valamint a PayPal is felfüggesztette a Wikileaks számláira való átutalásokat. Erre reagálva az Anonymous támadássorozatot indított az előbbiekben említettek ellen, jelentős károkat okozva.[19]

Az információs rendszer felhasználásával ugyancsak számtalan visszaélés történik nap mint nap. A hagyományos bűncselekmények elterjedése az interneten nehezíti úgy a jogalkotó mint a jogalkalmazó munkáját. Leggyakoribb megjelenési formái: elektronikus pénzügyi csalások, csalárd értékesítés online aukciós vagy kiskereskedelmi oldalakon keresztül, tömeges marketingcsalások és fogyasztói csalások, adathalászás (*angolul: phishing, pharming*), zsaroló vírusok, „online románc" (vagy közösségi oldalakon/

[16] Mike *McGuire* – Samantha *Dowling*: Cyber crime: A review of the evidence. Chapter 2: Cyber-dependent crimes https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf (2022. 05. 03.)

[17] Uo.

[18] *Králl* Bernarda: Egyre szélesedik a kiberháború Moszkva ellen. Index. 2022. március 8. https://index.hu/techtud/2022/03/08/haboru-orosz-ukran-anonymus-hacker/ (2022. 05. 03.)

[19] *Berki*: i. m. 5–21. o.

társkereső oldalakon történő) csalások.[20]

Az FBI jelentése alapján egy általános képet kaphatunk a kiberbűnözésről. A 2021-es év három legjelentősebb csalástípusa az adathalász üzenetek, a nemfizetéses/nemszállításos csalások, valamint a személyes adatszivárgások voltak.[21] A jelentés kitér egzakt módon a zsarolóvírusokra is, amelyek miatt összesen 49,2 millió dolláros kár keletkezett.

Először magát a bűncselekményt, a támadást kell megvizsgálni, utána beszélhetünk a védelem megvalósulásáról. Ki szeretném emelni a fentiekben felsorolt formákból, a klasszikus zsarolás egy újabb formáját, amely vírusként realizálódik. A hagyományos bűncselekmény modern változatáról beszélhetünk, ami az online térben bontakozik ki legtöbbször fenyegetés formájában. Ha az áldozat nem tesz eleget az elkövető követelésének, akkor következhet be a kár. Hatalmas veszélyt jelentenek manapság ezek a zsarolóvírusok, amelyek úgy működnek, hogy a megfertőzött információs rendszerben tárolt fájlokat, adatokat, vagy akár az egész állományt titkosítják, elérhetetlenné téve azokat a felhasználó. Következő lépés pedig már a váltságdíj követelése a feloldó kódért cserében, hiszen nagy értékű információk forognak kockán a legtöbb szituációban. Ez testet ölthet úgy is, hogy a virtuális betörést követően kép- videó- vagy hanganyagot gyűjtenek be, amelyek később a fenyegetés alapját jelentik. Gyakorta előfordul az is, hogy az elkövetők hozzáférésnek különböző személyes adatokhoz, pl. e-mailcím, telefonszám, amelyekre elküldik a kényes és kompromittáló információkat, anyagokat.[22]

A 2017-es év kiberbűncselekményei közül a WannaCry néven elhíresült zsarolóvírus világszerte okozott problémákat. Számtalan gép adatait titkosította ez a rosszindulatú kód, többek között a brit kórházakban is felfordulást okozott. Ennek köszönhetően több műtétet is el kellett halasztani. Az arra vonatkozó adatok, hogy hány

[20] Mike *McGuire* – Samantha *Dowling*: Cyber crime: A review of the evidence. Chapter 2: Cyber-enabled crimes – fraud and theft. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf (2022. 04. 19.)

[21] Ezek a főbb kiberbűnözési trendek az FBI szerint. Nemzeti Kibervédelmi Intézet. https://nki.gov.hu/it-biztonsag/hirek/ezek-a-fobb-kiberbunozesi-trendek-az-fbi-jelentese-szerint/ (2022. 04. 20.)

[22] A világ legnagyobb adatlopásai: a Yahoo áll az élen. Növekedés. 2019. szeptember 1. https://novekedes.hu/tech/a-vilag-legnagyobb-adatlopasai-a-yahoo-all-az-elen (2022. 05. 09.)

áldozat fizetett és kapta ezáltal meg a feloldó kódot nem ismert.[23]

A téma kapcsán az átlagember számára a személyes adatokkal való visszaélés juthat eszébe, akár a személyazonosságlopás is. Uniós szinten elsőként az Európai Parlament és Tanács 2013/40/EU irányelve szabályozta az információs rendszerek és adatok integritását érő támadásokat.[24] Releváns bűncselekmények a személyazonosság lopás és csalás. A hódító közösségi felületek megkönnyítik az adathalászást és az így nyert információk felhasználást is. A Legfőbb Semmítő- és Ítélőszék 2021. évi 25. döntésében kimondta, hogy más személy személyes adatainak (pl. név, e-mail cím, képek) az interneten való felhasználása kimeríti a Román Büntető törvénykönyv 325. cikkébe foglalt informatikai hamisítás bűncselekményének tényállását.[25] A személyazonosság lopás, mint bűncselekmény jellemzően olyan személyes adatokat érint, amelyekkel már születésünktől fogva rendelkezünk, mint pl. név, születési hely, idő, egyedi tulajdonságainkat, mint a DNS, ujjlenyomat, írisz. Az életünk során bekövetkezett életesemények is itt említhetőek, pl. iskolai végzettség, munkahely, családi állapot stb. Az utolsó csoport az általunk választott személyes információk, gondolhatunk itt a jelszavakra, felhasználónevekre. Fontos megemlíteni, hogy a személyazonosság-lopás sok esetben nem egyedülálló bűncselekményként jelenik meg, hanem „ezt az elnevezést a különböző büntetendő magatartások körének gyűjtőfogalmaként használják."[26]

Az ehhez hasonló bűncselekmények sorát még bőven lehetne folytatni, viszont a tanulmány nem hivatott a teljesség igényével bemutatni ezeket, csupán kiragadni a gyakran elkövetett bűncselekményeket és azok lényeges tulajdonságait.

IV.2. Kiberterrorizmus

Míg a 70-es években csekély mértékben jelentett problémát, addig napjainkban világméretű problémákat okoz a kiberterrorizmus. Alapjaiban a klasszikus terrorizmust is súlyos bűncselekményként tartjuk számon, viszont az új technológiák kihasználásával még inkább hatékonyabban és sikeresebben végrehajthatóvá válik. A terrorista szervezetek interneten való kommunikációja a decentralizált, peer to peer titkosítást használó

[23] *Berki*: i. m. 5–21. o.

[24] *Mezei*: i. m. 73. o.

[25] Decizia nr. 4 din 25 ianuarie 2021. Portal Legislative.

[26] Uo.

szoftvereken keresztül egy időben teszik könnyebbé az ilyen szervezetek tagjai közötti kommunikációt és nehezíti meg egyben a hatóságok munkáját.

A végtelen információszerzés lehetősége és az ehhez való egyszerű, gyors hozzájutás lényegesen megkönnyíti a terroristák dolgát. Elég arra gondolnunk, hogy a bombakészítésről hány videó és instrukció található meg, nem beszélve a Google Maps azon funkciójáról, amely 3D-s látképet tesz nyilvánossá. Céljaik, eszméik és nézeteik népszerűsítésére is tökéletes eszközként szolgálhatnak weboldalaik, hiszen a hagyományos média nem közvetítené gondolataikat. Legnagyobb fegyverük a pszichológiai hadviselés, erre megfelelő példa az Iszlám Állam által alkalmazott taktika. Több olyan videó került a világ elé, amelyekben elrabolt emberek lefejezése és katonák kivégzése szerepelt.

Az Amerikai Egyesült Államok Szövetségi Nyomozó Irodája szerint a kiberterrorizmus alá tartozik minden olyan „előre megfontolt, politikailag motivált támadás az információkkal, számítógépes rendszerekkel, számítógépes programokkal és adatokkal, amelyek szubnacionális csoportok vagy titkos ügynökök elleni erőszakot eredményeznek a nem harci célokat illetően”.[27]

IV.3. Kiberkémkedés és kiberhadviselés

A kémkedés, akárcsak ahogyan a terrorizmusnál is láttuk, adaptálódik az új technológiai fejlődésekhez. A kémkedés mindig is létezett, egyes korokban erőteljesebb szerepet játszott. Az ellenséggel szemben számtalan információ releváns és felhasználható lehet, gondolhatunk itt katonai, gazdasági, ipari vagy pénzügyi adatra.

A modern kor velejárójaként a kémkedés is kiterjedt a kibertérre. Remek példa erre az Amerikai Egyesült Államok ellen indított támadás, amely kémkedési célt szolgált és a vizsgálatok alapján Kínához volt köthető. A folyamat tovább fejlődött különböző rosszindulatú programok bevetésével, mint pl. a Gauss kód, amelynek áldozata volt Libanon, Izrael és a Palesztin területek egyaránt. 2012-2018 között is működött egy ehhez hasonló program a Közel-Keleten és Afrikában.[28]

A kiberhadviselés mellett sem lehet szó nélkül elmenni, a fogalom alatt azt a fo-

[27] *Simon* Béla – *Gyaraki* Réka: Kiberbűnözés. In: Kibervédelem a bűnügyi tudományokban (szerk. Kiss Tibor). Dialóg Campus, Budapest 2020. 103. o.

[28] *Berki*: i. m. 5–21. o.

lyamatot értjük, mikor a klasszikus hadviselés a hagyományos fegyverek mellett kiegészül a kibertámadásokkal.[29]A jól meghatározott cél eléréséért minden területen végbemegy a támadás, melynek célja a fontos a számítógépes hálózatok megbénítása, mint pl. a kormányzati szervereké. Erre példa Észtország esete, habár itt Oroszország ezen fajta vétkességét tagadta. A szóban forgó esetben 2007-ben Észtországot hosszan tartó kibertámadás érte, melyet precízség és összehangoltság jellemzett.[30] Szakértők szerint orosz szerverekhez vezethető vissza a támadás forrása és egyértelműen a megbénítás volt az elérni kívánt végcél.[31]

Ahogyan láthattuk a kibertér és a kiberbűncselekmények szorosan összefüggő fogalmak, kapcsolatukat tekintve pedig elmondhatjuk, hogy az illetékesség megállapítása nem egyértelmű ezekben az esetekben. A szakirodalomban felmerült a kérdés, hogy a kibertér maga az elkövetett bűncselekmények egzakt helyeként funkcionál vagy csupán egy eszközként lehet rá hivatkozni.[32] A bemutatottak alapján és személyes véleményemre alapozva válaszként az utóbbi meglátást tartom helyesnek. Maga a helyszín az elkövető, a személy fizikai tartózkodásához kell, hogy köthető legyen, tény, hogy egyes bűncselekmények nem valósulhatnak meg máshol csak a kibertérben, de ez csupán egy nélkülözhetetlen elemként tartható számon. Véleményem szerint, ha elfogadnánk, hogy az elkövetés helyszíne a kibertér, a joghatóság megállapítása komoly gondot okozna, főleg a határokon átnyúló kiberbűncselekmények esetében, ezzel még inkább hozzájárulva, az ilyen bűncselekmények felderíthetetlenségéhez. Azzal, hogy az elkövetés helyszínének, az elkövető fizikai tartózkodási helyét tekintjük, egyszerűbbé válik a joghatóság megállapítása, gördülékenyebbé téve az állami beavatkozást.

V. A jogos védelem kibertérben való alkalmazásának fontosság

Bár a klasszikus értelemben vett jogos védelem, nem alkalmazható tökéletesen, annak egy különleges formájának létjogosultsága vita tárgyát képezi. Az egyre kiterjedtebb és komplexebb kibertérben a jogos védelem használatát leginkább az a tény alapozza

[29] Uo.

[30] Uo.

[31] *Bányász* Péter – *Orbók* Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. Hadtudomány 2013/1. sz.

[32] *Szathmáry* Zoltán: Az internet mint a bűncselekmények elkövetésének helye. In: A bűnügyi tudományok és az informatika (szerk. *Mezei* Kitti). Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, Budapest – Pécs 2019. 201. o.

meg, hogy a bűncselekmény elkövetési módjának atipikus jellege miatt a bűnüldözési és igazságszolgáltatási szervek fellépési képessége korlátozott. Szem előtt kell tartanunk, hogy a kibertérben történő támadások nagy része felderítetlen marad, ezért az állam általi büntetőjogi felelősségre vonás sem valósulhat meg, így a büntetőjog preventív funkciója nem érvényesül, ami akár a bűnözők és bűnszervezetek számára a „tökéletes bűncselekmény" elkövetési eszközévé változtathatja a kiberteret. Elfogadhatatlan lenne egy olyan álláspont, amely szerint a bűncselekmény elkövetésének különös módja és eszköze miatt a sértett vagy akár harmadik személyek elveszítsék a jogukat arra, hogy a kibertérben elkövetett bűncselekmények esetében elsősorban vagyonukat és adataiknak épségét vagy titkosságát megvédjék, mivel ezen jog megvonásának következménye az állami szervek sokszori tehetetlenségével együtt a kockázatmentes elkövetés biztosítása lenne a támadó számára, mintegy ösztönzőként hatva az ilyen jellegű bűncselekmények elkövetésére.[33] Az informatikai rendszerekkel elkövetett támadások esetén (pl. DDoS támadás) előfordulhat, hogy a védekezés nem csak a támadóval szemben fejt ki hatást, például ha a támadó nem csak saját rendszereit és erőforrásait használja, hanem egy más személyek (akiknek esetleg tudomásuk sincs arról, hogy eszközük fertőzött) eszközeiből álló botnetet is bevet, és a támadás elhárítása során harmadik személyek számára is keletkezik kár. Ilyen esetben a támadóval szembeni fellépés jogos védelemben elkövetett cselekedet lesz, a harmadik személyek érdekeinek sérülése tekintetében pedig a végszükség lesz alkalmazandó.[34]

A kibertérben elkövetett támadások sokszori hirtelen bekövetkezése, gyors lefolyása és előreláthatatlan jellege megalapozottá teszi a megelőző jogos védelem alkalmazását ezen a téren is. Bár az Rbtk. konkrétan nem szabályozza a megelőző jogos védelem lehetőségét, a román szakirodalom szerint nem kizárt annak a lehetősége, hogy egy személy egy jövőbeni veszély elhárítása érdekében mesterséges akadályokat állítson fel a támadó útjába, ha ezek az akadályok hatásukat a veszély kialakulásának pillanatában fejtik ki, amikortól a támadás fenyegetővé válik. A megelőző jogos védelem kibertérben való alkalmazása talán könnyebben is megvalósítható, mint a minket körülvevő világban, mivel ott könnyebb az arányosság garantálása. A klasszikus megelőző jogos védelem esetében, a működésbe lépő védekezésre használt eszköz, bizonyos körülmények kö-

[33] *Miskolczi* Barna – *Szathmáry* Zoltán: Büntetőjogi kérdések az információk korában. HVG–ORAC, Budapest 2018. 128. o.

[34] Uo.

zött, vagy akár az eszközt telepítő személy gondatlanságából vagy hozzá nem értéséből eredően könnyen túllépheti az arányosság feltételét (pl. a kertbe való behatolást megakadályozó eszköz az illetéktelen behatoló halálát okozza). Az eszköz véletlen működésbe lépése harmadik személyek számára sérülést vagy kárt okozhat, ezáltal meghaladva a jogos védelem határait, amiért az eszközt telepítő személyt büntetőjogi felelősség terheli. A kibertérben való megelőző jogos védelem alkalmazása kevésbé vet fel hasonló problémákat. A kibertérben való védekezés esetében csaknem kizárt a támadó életének vagy testi épségének veszélyeztetése, ugyanakkor a védekezésre használt programok véletlenszerű működésbe lépése a támadással nem kapcsolatba hozható harmadik személyekkel szemben kizárt.

A kibertérben megvalósuló jogos védelem tehát, inkább a megelőző jogos védelem formáját öltheti magára a kibertérben elkövetett bűncselekmények különleges jellegét szem előtt tartva, ugyanakkor a jogos védelem, mint a már megindult támadás következtében bekövetkezett veszély elhárítására irányuló aktív magatartás, „visszatámadás" (*hacking back*) sem kizárt.[35] A klasszikus jogos védelemhez hasonlóan, a kibertérben megvalósuló jogos védelem feltételeit is pontosan meg kell határozni. A klasszikus jogos védelem feltételeit alapul véve, véleményem szerint jogos védelmet egy közvetlen, azonnali, jogtalan és a védekező személye vagy jogai ellen, illetve harmadik személyek vagy a közérdek ellen elkövetett támadás alapoz meg. A klasszikus jogos védelem kapcsán ezekre a feltételekre vonatkozó szakirodalmi álláspontok alkalmazandók a kibertérben megvalósuló jogos védelem esetében. A kibertérben való védekezés feltételei azonosak a klasszikus jogos védelem keretében megvalósuló védekezés feltételeivel, ugyanakkor még nagyobb hangsúlyt fektetve az arányosság tényleges betartásának vizsgálatára. Az arányosság szigorúbb vizsgálatát a kibertérben elkövetett bűncselekmények elkövetőinek ismeretlenségéből, valamint például a botnet hálózatok használatával elkövetett támadások esetében, a védekezéssel harmadik személyekkel szembeni károkozás lehetősége miatt szükséges. Az arányosság kérdése hangsúlyosan a hacking back védekezés esetében vethető fel, amikor a védekező személy az illetéktelen behatolás megakadályozására, vagy esetleg a behatolás következtében ellopott adatok visszaszerzése, vagy zsaroláshoz használt kompromitáló eszközök egy másik rendszerből való törlése céljából indít egy újabb támadást. Korábban kifejtésre került, hogy a kibertér

[35] *Miskolczi – Szathmáry*: i. m. 129–131. o.

a modern kor hadszínterévé és a kémkedés új módjává vált, ezáltal nem zárható ki az a lehetőség sem, hogy egy-egy kibertámadás mögött államok álljanak, ezért a kibertérben való aránytalan, szükségtelen és ellenőrizhetetlen védekezés súlyos, akár nemzetközi, következményekkel járhat. Megalapozott lenne, ha nem is kimerítő jelleggel, mivel nem is lenne lehetséges, meghatározni a bizonyos jellegű támadásokkal szemben arányosnak tekinthető válaszlépéseket,[36] mint a klasszikus jogos védelem esetében a késsel támadó személy elleni tűzfegyver elsütése esetében például, az agresszor ilyen módon való megölése, csak akkor értékelhető jogos védelemben elkövetett cselekedetnek, ha az agresszor a védekező személy közvetlen közelében tartózkodott, ugyanakkor a távolról támadásba lendült agresszor lábon lövése elégséges és arányos cselekedet, megölése viszont ilyen helyzetben nem értékelhető jogos védelemben elkövetett cselekedetként.

V.1. Az MI mint elkövető

A XXI. századi technológiai fejlődés egyik legnagyobb vívmánya a mesterséges intelligencia (MI), ami hosszútávú elképzelések szerint jobbá fogja tenni az emberek életét azáltal, hogy segít felvenni a harcot a klímaváltozás elleni küzdelemben, hatékonyabbá teszi a mezőgazdaságot, megkönnyíti a betegségek korai diagnosztizálását és még sorolhatnánk.[37] Az MI vezérelte okos eszközök széleskörű elterjedése, valamint a kibertér internet általi egyre nagyobb kiterjedése egyre szorosabban összekapcsolja az MI és a kibertér fogalmát. Felmerül azonban a kérdés, hogy milyen felelősség terheli az MI-t annak cselekedeteiért (például egy önvezető autó okozta halálos közúti baleset esetén) vagy, hogy egyáltalán felelősségre vonható entitás-e az MI, vagy az ez által okozott károkért és elkövetett bűncselekményekért a felelősség az MI megalkotóját terheli. A másik probléma, ami szorosan a büntetőjoghoz köthető, hogy milyen módon védekezhetnek az emberek az MI által okozott veszélyek ellen, az MI ellen kell-e fellépni, vagy pedig az ellen a személy ellen, aki az MI mögött rejtőzik. Egyértelmű, hogy az MI által elkövetett bűncselekmények esetében nem maradhat el az állami reakció. Az angolszász büntetőjogban e terén formálódó vélemény több modellt alakított ki, amelyekből két a román büntetőjog szempontjából releváns modellt fogok bemutatni.

[36] *Miskolczi – Szathmáry*: i. m. 132–134. o.

[37] A mesterséges intelligencia használata és veszélyei. Európai Parlament. https://www.europarl.europa.eu/news/hu/headlines/society/20200918STO87404/a-mesterseges-intelligencia-hasznalata-es-veszelyei (2022. 05. 09)

Az MI *mint önálló entitást büntetőjogi felelőssége*[38] (*direct liability model*) egyelőre nem alkalmazható, mivel a klasszikus büntetőjog csak azon emberi magatartásokat szankcionálja amelyeket bűnösséggel követnek el és az egyénnek felróható. Gless más szerzőkkel együtt úgy fogalmaz, hogy „egy robot nincs tudatában szabadságának, nem képes saját magára egy múlttal és jövővel rendelkező entitásként gondolni, továbbá képtelen megérteni a jogok és kötelezettségek jelentőségét"[39], vagyis cselekedetei nem róhatóak fel számára. Az Rbtk. 15. cikkének (1) bekezdése szerint [a] bűncselekmény a büntető törvény által meghatározott bűnösen elkövetett olyan cselekmény, amely jogellenes és az elkövetőnek felróható", vagyis a felróhatóság hiányában az MI, mint önálló entitást nem vonható büntetőjogi felelősségre.

A második modell szerint a *közvetett tettességre* (*preparation-by-another*)[40] alapozva az MI működtetőjének felelősségre vonását szorgalmazza. A modell lényege, hogy MI csak a bűncselekmény elkövetésének eszközét képezi, a valódi elkövető pedig az MI mögötti ember, akinek cselekedetei ellen fel lehet lépni, illetve akit a büntetőjogi felelősség terhel az MI felhasználásával elkövetett bűncselekmény miatt. Jelen pillanatban, ezen modell alkalmazása tűnik a legalkalmasabbnak, ugyanakkor nem feledkezhetünk meg az MI-t érintő technológia folyamatos fejlődéséről, ami akár a jövőben magától cselekvő MI-k létrehozását is lehetővé teheti, amelyek esetén már nem beszélhetünk közvetett tettességről, ha elfogadjuk, olyan egyelőre a tudományos fantasztikum szintjén létező MI létrehozásának lehetőségét, amely az emberhez hasonlóan képes gondolkodni és egy helyzet önállóan való mérlegelése alapján cselekedni. Ilyen esetben már az MI működése nem egy beszámítási képességgel nem rendelkező személy cselekményéhez hasonlítható, így a felróhatóság, mint a bűncselekmény alkotóeleme megtalálható.

A két modell alapján megállapítható, a technika jelenlegi állapota alapján az MI által, vagy inkább az MI-n keresztül elkövetett bűncselekmények esetében a felelősség az MI-t irányító személyt terheli. A jogos védelem szempontjából tehát az MI cselekedete az állatok cselekedetéhez hasonlítható, amelyek a támadás eszközét jelentik, így egyfelől az MI-vel szembeni fellépés jogos védelemben valósulhat meg, mint az állatok

[38] *Ambrus* István: A mesterséges intelligencia és a büntetőjog. Állam- és Jogtudomány 2020/4. sz. 12. o.

[39] Sabine *Gless* – Emily *Silverman* – Thomas *Weigend*: If Robots Cause Harm, Who is to Blame? Self-Driving Cars and Criminal Liability. New Criminal Law Review 2016/3. sz. 423–424. o.

[40] *Ambrus*: i. m. 12–13. o.

kiprovokált cselekedetei esetében, másfelől a védekező személy nem csak az MI, hanem az azt működtető személlyel szemben is felléphet a veszély elhárítására. A jövőben azonban, amikor az MI önálló cselekvésre is képes lesz a büntetőjognak azzal a kérdéssel kell majd megbirkóznia, hogy büntethető-e egy olyan nem emberi entitás, aminek azonban cselekedete felróható számára. Ehhez szorosan kapcsolódó megválaszolandó kérdés, hogy az MI önálló, spontánnak tekinthető cselekedetei esetén, az állatok spontán viselkedéséhez hasonlóan végszükség keretében lehet-e elhárítani a veszélyt, vagy a felróhatóság következményeként az MI spontán cselekedete jogos védelmi helyzetet keletkeztet majd.

VI. Konklúzió

Vitathatatlan tény, hogy az információs társadalom kialakulása, az internet elterjedése és a kibertér egyre szélesebb kiterjedése a büntetőjog adaptációját teszi szükségessé olyan új kérdések megválaszolására, mint a jogos védelem lehetősége a kibertérben, vagy az MI elleni fellépés lehetősége és annak büntetőjogi felelősségre vonása. A kibertérben elkövetett bűncselekmények és a kibertér kialakulásából eredő új kiberbűncselekmények elháríthatóságának szükségességét támasztja alá a büntetőjog preventív funkciójának hatástalansága, ha a kiberteret a bűnelkövetés tökéletes eszközévé tesszük azáltal, hogy nem adjuk meg a jogot a potenciális sértetteknek arra, hogy elhárítsák az őket fenyegető veszélyeket. Bár a klasszikus értelemben vett jogos védelem tökéletesen nem alkalmazható a kibertérben, erre alapozva kidolgozható annak egy olyan formája, ami kifejezetten az ott jelentkező veszélyek elhárítását szolgálná. A büntetőjognak tehát reagálnia kell az új kérdésekre és joghézagokra, ugyanakkor nem elhanyagolható az a tény sem, hogy a kibertérben való védekezés még inkább elvékonyítja a határvonalat a jogos védelem és a végszükség között.

Farcádi Attila-Dániel
szakkollégista, Collegium Iuridicum

Kerekes Ákos-Benjámin
szakkollégista, Collegium Iuridicum

Torjai Gergő-Zoltán
szakkollégista, Collegium Iuridicum

A véleménynyilvánítás szabadsága és a gyűlöletbeszéd közötti határ az online térben

I. A véleménynyilvánítás szabadsága

A véleménynyilvánítás szabadsága a személyiségi jogok közül az egyik legfontosabbnak tekinthető, hiszen bármely személy számára lehetőséget biztosít arra, hogy a világban zajló történésekről, eseményekről, magatartásokról alkotott véleményét szabadon, állami és más közhatósági beavatkozásoktól mentesen kinyilváníthassa. Olyannyira fontos, hogy az Emberi Jogok Egyetemes Nyilatkozatában is helyet kapott.[1] Mára már mindenképpen alapjognak minősül, s egy demokratikus politikai berendezkedéssel rendelkező államban a közügyekkel kapcsolatos, tisztelettudó stílusban megvalósuló párbeszéd kialakításához létfontosságú.

I.1. A véleménynyilvánítás szabadsága a nemzetközi jogban

A véleménynyilvánítás szabadsága elengedhetetlen feltétele az ember teljes körű szellemi kibontakozásának. Az adott jog szükséges a társadalom számára, mivel ez alkotja minden szabad és demokratikus társadalom alapkövét. A véleménynyilvánítás szabadsága az átláthatóság és az elszámoltathatóság elvei megvalósításának létfontosságú feltétele, amely nélkülözhetetlen az emberi jogok előmozdításához és védelméhez. A véleménynyilvánítás szabadságának tiszteletben tartása minden ENSZ tagállamra nézve kötelező.[2]

[1] Emberi Jogok Egyetemes Nyilatkozata. General Assembly, resolution 217 A (III), A/RES/3/217 A, 10 December 1948. 19. cikk

[2] Az Egyesült Nemzetek Közgyűlése XXI. ülésszakán, 1966. december 16-án elfogadott Polgári és Politikai Jogok Nemzetközi Egyezségokmánya kihirdetéséről szóló 1976. évi 8. törvényerejű rende-

Az állam minden ága (végrehajtó, törvényhozó és igazságszolgáltató) és más állami vagy kormányzati hatóságok nemzeti, regionális vagy helyi szinten is képesek vállalni a részes állam felelősségét. A kötelezettség azt is előírja a tagállamok számára, hogy biztosítsák a személyek védelmét minden olyan magánszemély vagy szervezet által elkövetett cselekménnyel szemben, amely hátrányosan befolyásolná a szabad véleménynyilvánítás gyakorlását, amennyiben ezek a jogok természetes személyek vagy más jogalanyok között alkalmazhatók.[3]

I.2. Jog a szabad véleményhez

A Polgári és Politikai Jogok Nemzetközi Egyezségokmánya (a továbbiakban PPJNE) 19. cikkének (1) bekezdése megköveteli a vélemény tiszteletben tartását. Ez egy olyan jog, amelyre nézve az Egyesült Nemzetek Szervezete (a továbbiakban: ENSZ) nem engedélyez kivételt vagy korlátozást. Senkit sem érhet a Szövetségből eredő bármely jog sérelme tényleges vagy vélt véleménye alapján. A vélemények minden formája védett, beleértve a politikai, tudományos, történelmi, erkölcsi vagy vallási jellegűt is.

Az (1) bekezdéssel összeegyeztethetetlen a vélemény fenntartásának bűncselekménnyé nyilvánítása. Egy személy zaklatása, megfélemlítése vagy megbélyegzése, ideértve letartóztatását, őrizetbe vételét, bíróság elé állítását vagy bebörtönzését a fenntartott véleménye miatt, a 19. cikk (1) bekezdésének megsértését jelenti. Tilos bármilyen erőfeszítés a vélemény elhallgatásának kikényszerítésére. A véleménynyilvánítás szabadsága szükségszerűen magába foglalja a véleménymegtartás jogát, ami azt jelenti, hogy senki sem kényszeríthető véleményének kinyilvánítására.[4]

I.3. A szabad kifejezés joga

A (2) bekezdés előírja a részes államok számára, hogy garantálják a véleménynyilvánítás szabadságához való jogot, ideértve a határoktól függetlenül mindenféle információ és ötlet keresésének, fogadásának és terjesztésének jogát. Ez a jog magába foglalja a formanyomtatványok terjesztését és fogadását, amely a 19. cikk (3). bekezdésének és a 20. cikk rendelkezéseinek értelmében azt jelenti, hogy bárkinek joga van megosztani másokkal a politikai beszédet, a saját véleményt, valamint a közügyekről, az ügyvédelemről, az

let. (a továbbiakban: PPJNE) 19. cikk.

[3] Uo.

[4] Uo.

emberi jogok megvitatásáról, az újságírásról, a kulturális és művészeti önkifejezésről, a tanításról és a vallási beszédről szóló információkat egyaránt. A (2) bekezdés hatálya magába foglalja azokat a kifejezéseket is, amelyek mélyen sértőnek tekinthetők, bár ezek a kifejezések korlátozhatók a 19. cikk (3) bekezdése és a 20. cikk rendelkezései alapján.[5]

I.4. A véleménynyilvánítás és a média szabadsága

Egy szabad, cenzúrázatlan sajtó vagy más média fogalmába beletartozó intézmény elengedhetetlen minden társadalomban a véleménynyilvánítás szabadságának, valamint az ENSZ által biztosított más jogok érvényesüléséhez. Ez a demokratikus társadalom egyik alappillére. A PPJNE magába foglalja azt a jogot, amely alapján a média információkat kaphat, amelyek alapján rendeltetésének megfelelően működhet. A polgárok, a jelöltek és a megválasztott képviselők között elengedhetetlen a nyilvános és politikai kérdésekkel kapcsolatos információk és ötletek szabad kommunikációja. Ez magába foglalja a szabad sajtót és más médiát, amely képes cenzúra és korlátozás nélkül kommentálni a közéleti kérdéseket, és tájékoztatni a közvéleményt. A médiahasználóknak, köztük az etnikai és nyelvi kisebbségek tagjainak a sokféle információ és ötlet megszerzéséhez fűződő jogainak védelme érdekében a részes államoknak különös gondot kell fordítaniuk a független és sokszínű média ösztönzésére.[6]

Figyelembe kell továbbá venniük, hogy az információs és kommunikációs technológiák, például az internet és a mobil alapú elektronikus információterjesztési rendszerek fejlődése mennyiben változtatta meg a kommunikáció gyakorlatát a világban. Ma már létezik globális hálózat az eszmék és vélemények cseréjéhez, amely nem feltétlenül támaszkodik a hagyományos tömegmédia-közvetítőkre. A részes államoknak minden szükséges lépést meg kell tenniük ezen új média függetlenségének előmozdítása és a hozzáférés biztosítása érdekében. A részes államoknak biztosítaniuk kell, hogy a nyilvános műsorszolgáltatások független módon működjenek. Ebben a tekintetben a részes államoknak garantálniuk kell a szerkesztőségek önállóságát és szabadságát. Olyan módon kell finanszírozást nyújtaniuk, amely nemássa alá függetlenségüket.[7]

[5] Uo.
[6] Uo.
[7] Uo.

I.5. Az információkhoz való szabad hozzáférés joga

A PPJNE 19. cikkének (2) bekezdése magába foglalja az állami szervek birtokában lévő információkhoz való hozzáférés jogát. Ezek az információk tartalmazzák az állami szervek által kezelt iratokat, függetlenül az információk tárolásának formájától, azok forrásától és az előállítás dátumától. Amint már megjegyeztük, az Egyezségokmány 25. cikkének értelmében az információkhoz való hozzáférés joga magába foglalja azt a jogot, amely révén a média hozzáférhet a közügyekkel kapcsolatos információkhoz, valamint a nagyközönségnek azt a jogát, hogy médiatermékeket kapjon. Az információkhoz való hozzáférés jogának elemeivel a Szövetség másutt is foglalkozik. Amint azt a bizottság az PPJNE 17. cikkével kapcsolatos 16. sz. általános megjegyzésében megállapította, minden egyénnek joga van érthető formában meggyőződni arról, hogy az automatikus adatállományokban milyen személyes adatokat tárolnak és mi célból. Minden egyénnek tudomása kell legyen arról, hogy mely állami hatóságok, magánszemélyek vagy szervek ellenőrzik vagy ellenőrizhetik iratait. Ha ezek az okiratok helytelen személyes adatokat tartalmaznak, vagy azokat a törvény rendelkezéseivel ellentétesen gyűjtötték be, illetve dolgozták fel, akkor bármely személynek joga van a nyilvántartás helyesbítését kérni. A PPJNE 10. cikke értelmében a fogvatartott nem veszíti el az orvosi nyilvántartásokhoz való hozzáférés jogát. A bizottság a 14. cikk 32. számú általános megjegyzésében meghatározta a bűncselekménnyel vádoltak információval kapcsolatos különböző jogosultságait.[8]

Az információkhoz való hozzáférés jogának érvényesítése érdekében a részes államoknak proaktív módon kell nyilvánosságra hozniuk a közérdekű kormányzati információkat, és mindent meg kell tenniük az ilyen információkhoz való könnyű, gyors, hatékony és gyakorlati hozzáférés biztosítása érdekében. A részes államoknak meg kell hozniuk továbbá a szükséges intézkedéseket, amelyek révén az információkhoz való hozzáférést garantálják. Ez információszabadságra vonatkozó jogszabályok alkalmazása révén kivitelezhető. Az eljárásoknak biztosítaniuk kell az információ iránti kérelmek időben történő feldolgozását a PPJNE-vel összeegyeztethető szabályok szerint. Az információkérések díja nem lehet az információkhoz való hozzáférés jogának az akadálya, továbbá a hatóságoknak meg kell indokolniuk az információkhoz való hozzáférés megtagadását.[9]

[8] Uo.

[9] Uo.

I.6. A véleménynyilvánítással kapcsolatos tolerancia eltérés

A szabad véleménynyilvánítás a közszereplőkkel szemben sokkal magasabb tolerancia-küszöböt igényel, mint a magánszemélyeknél. Közszereplőnek számít mindenki aki a közszereplés igényével lép fel, ezáltal vállalva egy magasabb ingerküszöböt mások véleménynyilvánításával szemben, mint a magánszemélyek. Az állami és helyi önkormányzati feladatokat ellátó szervek és személyek tevékenységének nyilvános bírálhatóságához kiemelkedő alkotmányos érdek fűződik. A személyiségvédelem nem biztosított védelmet az olyan értékítéletekkel szemben, amelyek a közügyek véleményezése során látnak napvilágot, még abban az esetben sem, ha azok túlzóak. A polgári jogból a személyiségi jogok védelmének szempontjából hiányzik egy olyan irányelv, amely segítene a jogalkalmazónak a közéleti szereplők személyiségi jogainak sérelmét jelentő mérce felállításában.[10]

I.7. A véleménynyilvánítás szabadsága a belső jogban

Az alkotmányos normatartalom strukturálásának módja a szólásszabadság kérdésköréhez nagymértékben hozzájárult és hozzájárul, az elv (a véleménynyilvánítás szabadságának a nyilvános kommunikáció bármely eszközével való érinthetetlensége) felelevenítésével együtt a modern alkotmányok szövegei tartalmazzák a cenzúra tilalmának a szabályozását, a sajtószabadság hangsúlyozását, a szólásszabadság korlátait.[11]

Eleinte az alkotmányos véleménynyilvánítás szabadságának fő kedvezményezettjeinek köre nem volt pontosan meghatározva a magánélethez való jog szempontjából. Írók, újságírók, filozófusok és politikusok eszmecseréiket a társadalom főbb politikai kérdéseire összpontosították, amelyek – bár főként a közérdekhez kötődtek – esetenként a magánszférába is betolakodtak. A társadalmi osztályrétegződés pedig a régi konvenciók és szokások révén biztosított elegendő védelmet az intimszféra, illetve a magánélet területét érintő jogsértésekkel szemben. A sajtószabadság a sajtókiadványok megalapításának jogát is feltételezi, ezáltal semmilyen kiadványt nem lehet betiltani, a törvény által kifejezetten előírt kivételektől eltekintve. A tömegtájékoztatási eszközök

[10] *Barzó* Tímea: A közéleti szereplők és a magánélethez fűződő jog. In: MultiScience – XXXII. microCAD International Multidisciplinary Scientific Conference (szerk. *Kékesi* Tamás). Miskolci Egyetem, Miskolc 2018. 3. o.

[11] Uo.

vezetői kötelezhetők, hogy nyilvánosság elé tárják ezek finanszírozási forrását.[12]

„A *köztudomásra hozott információért vagy alkotásért a polgári jogi felelősség a kiadót vagy az alkotót, a szerzőt, a művészeti esemény szervezőjét, a sokszorosító eszköz, a rádió- vagy televízióállomás tulajdonosát terheli, a törvényes feltételek között. A sajtóvétket törvény állapítja meg.*"[13]

A véleménynyilvánítás szabadsága az Emberi Jogok Európai Egyezményében is fel van tüntetve.

Az Egyezmény 10. cikkének (1) bekezdésében rögzíti, hogy „*Mindenkinek joga van a véleménynyilvánítás szabadságához*". Ebbe a jogba beletartozik a véleményalkotás szabadsága és az információk, eszmék megismerésének és közlésének szabadsága, országhatárokra való tekintet nélkül és anélkül, hogy ebbe hatósági szerv beavatkozhatna. Ez a cikk nem akadályozza meg, hogy az államok a rádió-, televízió- vagy mozgóképvállalatok működtetését engedélyezéshez kössék.[14] A médiajogot és a sajtójogot is érinti az a beleegyezési vélelem, amely akkor áll fenn, amikor az a jogalany, akire valamely információ vonatkozik, ilyen és bármilyen más típusú információt tartalmazó anyagot ad át olyan természetes vagy jogi személynek, akinek tevékenysége a köztájékoztatás. Következésképpen ezek felhasználásához nem szükséges az illető írásos beleegyezése.[15]

II. A véleménynyilvánítás szabadságának határai – a gyűlöletbeszéd

A véleménynyilvánítás szabadságának vannak-e határai? A válasz az, hogy a demokrácia összes formája tiltja vagy legalábbis korlátozza egyes párbeszédtípusok kialakulását, vagy a bizonyos stílusban megvalósuló közéleti diskurzust.[16] Az Emberi Jogok Európai Bírósága (EJEB) szerint a gyűlöletbeszéd jogi szabályozása azért szükséges, hogy az intoleranción alapuló uszítás minden formáját lehetőleg megelőzzük, illetve amikor ez

[12] *Kokoly* Zsolt: Személyiségi jogok a román polgári jogban. Forum Iuris Könyvkiadó, Kolozsvár 2018. 6. o.

[13] Uo.

[14] Uo.

[15] Uo.

[16] Daniela *Angi* – Gabriel *Badescu* – Cynthia Carmen *Curt* – Carmen Gabriela *Greab*: Discursul instigator la ură în România. Research Gate 2014. https://www.researchgate.net/publication/333811833_Discursul_instigator_la_ura_in_Romania (2022. 04. 19.)

már nem lehetséges, megfelelően szankcionáljuk azt.[17]

A gyűlöletbeszéd és a véleménynyilvánítás szabadsága közötti határvonal megállapításával azért érdemes foglalkozni, mert a gyűlöletbeszéd társadalomra gyakorolt hatása igen jelentős. Ha az áldozatok szemszögéből vizsgáljuk a kérdést, akkor az emberi méltóság sérelmével, az önbecsülés rombolásával, valamint az érintett társadalmi csoportok elszigetelésével számolhatunk. A társadalmi kohézió szintjén pedig hatásként merülhet fel a kizárás, a társadalom szélére sodródás, a sztereotípiák és az előítéletek meghonosítása, a csoportok közötti társadalmi különbség mélyülése.

Annak ellenére, hogy világszerte létezik olyan közmegegyezés, amely a véleménynyilvánítás szabadsága és az uszító kifejezéseket tartalmazó diskurzus közötti határmezsgye kialakítására törekszik, a gyakorlatban ez országonként eltérő, s nagyban függ az adott állam történelmi és társadalmi berendezkedésétől. Vannak, akik úgy gondolják, hogy a gyűlöletbeszéd egy szükséges rossz, amelynek szigorúbb szankcionálása károsabb lenne magánál a jelenségnél.[18] Azok a személyek, akik ezt a tábort erősítik, azzal szoktak még érvelni, hogy a gyűlöletbeszéden kívül vannak még más, erkölcsileg elítélt magatartások, amelyek nincsenek inkriminálva. Egy ezzel az állásponttal szinte megegyező vélemény szerint az uszító kifejezések jogi úton történő szankcionálása kormányzati túlkapásokhoz, visszaélésekhez vezethet abban az esetben,[19] ha a végrehajtó hatalom birtokosai a velük szembeni kritikusabb véleményekben potenciális veszélyt, valamint a pozícióik gyengülését vélik felfedezni.

A fentebbi véleményektől eltérő meggyőződésű szerzők úgy vélik, hogy a véleménynyilvánítás szabadsága és az uszító, agresszív hangvételű megjegyzések között lehetőség van az úgynevezett „arany középút" kialakítására. Véleményük szerint ezzel elsősorban azok nyernek, akik a társadalom perifériájára szorultak, s akiknek hangja éppen ezért elvész a tömegben,[20] továbbá a gyűlölködő, uszító magatartás ellehetetleníti a kifinomult, érdemi diskurzust a közügyek terén, s kizárólag az így is virágkorát élő gyűlölködést, sárdobálást erősíti. Végső soron tehát a gyűlöletbeszéd inkriminálá-

[17] Uo.
[18] Uo.
[19] Uo.
[20] Uo.

sa az egész társadalom érdekeit szolgálná.[21] Véleményünk szerint ez utóbbi álláspont ideológiai felfogásában lehetővé tenné a közügyekről történő viták kifinomultabbá válását, amely össztársadalmi fejlődéshez vezetne.

Egy olyan szabályozás, amely a gyűlöletbeszédet komolyabban szankcionálná, nagyban hozzájárulna ahhoz, hogy érdemben, a tárgytól történő minimális eltéréssel lehessen a közügyekről vitázni. Meglátásunk szerint, számos esetben ugyanis az agresszszív, uszító magatartás ellehetetleníti egy polémia kibontakozását, hiszen amint az egyik fél úgy véli, hogy ellenfele jobban érvel, mint ő, rögtön arra fog késztetést érezni, hogy e hátrányát a gyűlölet szításával kompenzálja.

Nem elhanyagolható az az aspektus sem, hogy a szóbeli agresszió könnyen torkollhat tettlegességbe.[22] Annak az esélye pedig, hogy a fizikai agresszió célpontjai a már emlegetett társadalmi perifériára szorult, védtelen személyek vagy csoportok legyenek, igen magas.

Elég, ha csak megnézzük azt, hogy mi történt a XX. századi Európában. A gyűlöletbeszéddel átitatott náci, nyilas vagy vasgárdista propaganda vezetett ugyanis ahhoz a történelmi tragédiához, amelyet ma holokausztként ismerünk, s amelyből okolnunk kell. Ezzel az eszmefuttatással csak azt kívánjuk szemléltetni, hogy milyen súlyú bűncselekmények származhatnak a gyűlöletbeszéd legitimizálásából. Témánk szempontjából ez azért nagyon fontos, mert a gyors ütemű technikai fejlődés következtében a gyűlöletbeszéd jelentős része az online térbe tolódott át. De tudnunk kell, hogy egy közzétett, uszító tartalommal ellátott facebook poszt ugyanolyan fajsúlyúnak tekinthető, mintha egy személy egy város emberekkel megtömött főterén állna neki gyűlölködő tartalmú diskurzust tartani.

De melyek azok a konkrét feltételek, amelyek együttes teljesülése szükséges ahhoz, hogy gyűlöletbeszédről lehessen szó. Az ebben a kérdéskörben talán legtöbbet idézett szerző, Bikhu Parekh szerint 3 elem együttes jelenléte kell a gyűlöletbeszédhez.[23]

Az első differenciálást szolgáló követelmény az, hogy a gyűlöletkeltő, uszító

[21] Uo.

[22] Uo.

[23] Bikhu *Parekh:* Hate Speech. Is there a case for banning? Public Policy Research 2006/12. sz. 214. o.

megnyilvánulások egy egyént vagy egyének csoportját célozzák meg bizonyos jellemzők alapján; a második az, hogy ez megbélyegezze az ádozatot azáltal, hogy olyan tulajdonságokat tulajdonít neki, amelyek általában mélyen nemkívánatosnak tartandók; a harmadik pedig az, hogy mindezt olyan megnyilvánulási stílusban tegye, amelyben a célcsoport a társadalmi viszonyok határain kívül helyeződik.[24] E kritériumok együttes teljesülése esetén gyűlöletbeszéddel állunk szemben, így még a véleménynyilvánítás szabadsága sem hozható fel mentségként, mivel ezáltal mások jogainak és szabadságainak megsértését idézzük elő.

Összegezve az e fejezetben tárgyaltakat, kijelenthető, hogy a véleménynyilvánítás szabadsága és a gyűlöletbeszéd között elhelyezkedő képzeletbeli határ még ha nehezen is, de megállapítható. Véleményünk szerint az egyének, illetve csoportok akkor vannak kitéve gyűlöletbeszédnek, amikor az elkövető bizonyos közös jellemzőkre hivatkozva lealacsonyító, degradáló szóhasználattal igyekszik a társadalmi értékek határain kívül helyezni a szóban forgó egyént vagy csoportot, történjen ez akár szemtől szemben, akár internetes platformokon keresztül.

III. Véleménynyilvánítás és gyűlöletbeszéd a közösségi platformokon

A globálisan elterjedt, több világrészt egymással összekötő közösségi oldalak esetében a felhasználási feltételek esszenciálisak. Ezek azok az irányelvek, szabályok, amelyek magatartásunkat hivatottak igazgatni az adott közösségi felületen. A gyűlöletbeszéd, mint jelenség sokkal inkább az online térbe tolódott át, mivel a becsületsértők enyhébb következményekre számítanak a közösségi platformokon. Ezért lényeges témánk szempontjából a közösségi felületek felhasználási felételeinek vizsgálata.

Az említett közösségi oldalakon tanúsított magatartásunk közvetlen módon ezeknek az irányelveknek van alávetve, a világ bármely részéről is használjuk az alábbi platformokat. Ilyen tényállásban feltételezhetjük, hogy ezeknek az oldalaknak a szabályai az államok törvényei felett állnak, azonban ez nem teljesen állja meg ilyen formában a helyét. Az viszont bizonyos, hogy amennyiben megsértünk valamiféle irányelvet egy közösségi oldalon, abban az esetben az oldal szolgáltatója szankcionálhat bennünket, hiszen a regisztráció során beleegyeztünk a szolgáltató feltételeibe. A szankciók sokfélék lehetnek, a legdrasztikusabb lépés általában a felhasználói fiókok felfüggesztése, tör-

[24] Uo.

lése. A napjainkban jól ismert közösségi oldalak általában ilyen formában büntetik azokat a felhasználókat, akik ismétlődő módon hajtanak végre gyűlöletbeszédet. A következőkben vizsgáljuk meg három legnépszerűbb közösségi platform felhasználási feltételeit.

III.1. A Facebook és az Instagram felhasználási feltételei

Amennyiben vesszük a fáradtságot, és elolvassuk a Facebook felhasználási feltételeit, rögtön megértjük az oldal nem titkolt üzleti modelljét is. Az ismertetőben rögtön azzal találkozunk, hogy a szolgáltató tudatja velünk, az oldalon ingyenes, azonban személyre szabott hirdetésekkel fogunk találkozni, amiket a rólunk begyűjtött adatok segítségével hoznak létre. Ezekért a hirdetésekért különböző szervezetek, vállalatok fizetnek a szolgáltatónak. A következőkben hivatkozott ismertetőben a szolgáltatást illetően részletes leírást találunk, amelyben a szolgáltató megosztja velünk, hogy milyen hasznos a terméke a kapcsolatteremtés, ismerősökkel, barátokkal, távoli családtagokkal való kapcsolatfelvétel tekintetében. Azonban az ismertető első részében, amelyben a szolgáltató a termékét mutatja be, arról is biztosít bennünket, hogy fellép a káros viselkedéssel szemben a közösség védelme és támogatása érdekében.

„Az *emberek csak akkor fognak közösséget építeni a Meta-termékekben, ha biztonságban érzik magukat. Kifejezetten erre a célra foglalkoztatunk csapatokat világszerte, és fejlett műszaki rendszereket fejlesztünk a Termékeinkkel való visszaélések, a mások számára káros magatartás, továbbá az olyan helyzetek azonosítására, amelyekben támogathatjuk és megvédhetjük közösségünket. Ha ilyen tartalomról vagy magatartásról értesülünk, megtesszük a szükséges intézkedéseket – például segítséget kínálunk, eltávolítjuk a tartalmat, letiltunk bizonyos funkciókhoz való hozzáférést, letiltjuk a fiókot, vagy felvesszük a kapcsolatot a bűnüldöző szervekkel. Amikor valamely termékünknél visszaélésszerű használatot vagy káros magatartást tapasztalunk, más Meta-vállalatokkal is megosztjuk az adatokat.*"[25]

Jól látható tehát, hogy komoly fellépésre számíthat a szolgáltató részéről az a felhasználó, akinek magatartása károsnak bizonyul a közösség számára. Viszont mit is értünk a káros magatartás alatt?

Erre a kérdésre választ az ismertető harmadik részében találunk, ami már nem a

[25] Felhasználási feltételek. Facebook. https://www.facebook.com/legal/terms (2022. 04. 18.)

termék bemutatásáról, hanem a felhasználó kötelezettségeinek ismertetéséről szól. Az említett részben felmerül a „Közösségi alapelvek" kifejezés, amely lényegében azokat az alapelveket jelenti, amelyek ellen vétve káros magatartást tanúsítunk a közösséggel szemben. Az ilyen sértő tartalmakat általában törlik, és ahogyan már utaltunk rá, bizonyos esetekben a tartalmakat megosztó fiókokat is felfüggesztik.

A továbbiakban nézzük a Facebook közösségi alapelveit, amelyről részletes leírást ad a szolgáltató. Legfontosabb alapelvként a biztonságot, a hitelességet, a magánélet védelmét és a méltóságot rögzíti. Károsnak tekinti továbbá a következő tartalmakat: erőszak és bűnözői magatartás, uszítás, veszélyes egyének és szervezetek, károkozás koordinálása és a bűnözés elősegítése, tiltott áruk és szolgáltatások reklámozása, csalásra és megtévesztésre irányuló tartalmak, öngyilkosság, gyermekek szexuális bántalmazása, bántalmazás és meztelenség, felnőttek szexuális bántalmazása, zaklatás, gyűlöletbeszéd, erőszakos grafikus tartalom, félretájékoztatás stb.[26] A felsorolásban természetesen helyet kapott a gyűlöletbeszéd is, amelyről a szolgáltató a következőképpen fogalmaz.

„A *gyűlöletbeszédet úgy határozzuk meg, mint az emberek – és nem fogalmak vagy intézmények – elleni közvetlen támadást az általunk védett tulajdonságok alapján: faj, etnikai hovatartozás, nemzeti származás, fogyatékosság, vallási hovatartozás, kaszt, szexuális irányultság, nem, nemi identitás és súlyos betegség. A támadás fogalmát erőszakos vagy dehumanizáló beszédként, káros sztereotípiákként, kisebbrendűségi kijelentésekként, megvetés, undor vagy elutasítás kifejezéseként, káromkodásként és kirekesztésre vagy szegregációra való felhívásként határozzuk meg. Tilalmazzuk továbbá a káros sztereotípiák használatát, amelyeket olyan dehumanizáló összehasonlításként határozunk meg, amelyeket történelmileg bizonyos csoportok támadására, megfélemlítésére vagy kirekesztésére használtak, és amelyek gyakran kapcsolódnak offline erőszakhoz. Az életkort védett tulajdonságnak tekintjük, ha egy másik védett tulajdonsággal együtt hivatkozunk rá. A menekülteket, migránsokat, bevándorlókat és menedékkérőket is megvédjük a legsúlyosabb támadásoktól, bár a bevándorlási politikákkal kapcsolatos kommentárokat és kritikákat megengedjük. Hasonlóképpen bizonyos védelmet biztosítunk az olyan jellemzőknek, mint a foglalkozás, ha egy védett jellemzővel együtt hivatkoznak rájuk. Néha a helyi árnyalatok*

[26] Facebook közösségi szabványok. Meta. https://transparency.fb.com/hu-hu/policies/community-standards/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards (2022. 04. 19.)

alapján bizonyos szavakat vagy kifejezéseket a PC-csoportok kódszavainak tekintünk."[27]

A szolgáltató az erről szóló részben kategorizálja a gyűlöletbeszéd különböző formáit, konkrét és egyértelmű példákat felsorolva. A legnagyobb különbség pedig pont ebben a részletben rejlik az állami szinten történő megközelítéssel szemben, ezek a közösségi platformok nevesítik, nagyon részletesen körvonalazzák a gyűlöletbeszéd gyakorlati eseteit. Az említett kategorizálás például olyan részt is tartalmaz, amelyben a Facebook szolgáltatója megjelöli, hogy milyen dehumanizáló összehasonlítások számítanak gyűlöletbeszédnek. Az egyébként hosszú felsorolásban például a következők kaptak helyet: fekete emberek és majmok vagy majomszerű lények, fekete emberek és mezőgazdasági gépek, fekete emberek karikatúrái blackface formájában, muszlim emberek és disznók, muszlim ember és szexuális kapcsolat állatokkal[28] stb.

Rengeteg tehát a részletes leírás ebben a kérdésben a Facebookon, a következőkben azonban vessünk pár pillantást az Instagram felhasználási feltételeire is.

Az Instagram irányelveinek oldalán rögtön egy aktuális szöveggel találjuk szembe magunkat. Megfigyelhető az online platformok esetében, hogy gyorsan reagálnak a globális történésekre, az ezekhez fűzött megjegyzéseket és tartalmakat pedig akár szabályozzák is. Az Instagram szolgáltatója az irányelvek meghatározásánál fontosnak tartotta kiemelni, hogy fellépnek a jelenlegi COVID-19 vírussal kapcsolatos káros tartalmak ellen. A szolgáltató a következőképpen fogalmaz: „*Mivel az emberek világszerte szembesülnek ezzel a példátlan közegészségügyi vészhelyzettel, biztosítani akarjuk, hogy politikáink segítsenek megvédeni az embereket a COVID-19-hez és a vakcinákhoz kapcsolódó káros tartalmaktól és új típusú visszaélésektől.*"[29]

Míg a közösségi irányelvek hasonlóak a Facebook felületére vonatkozó irányelvekkel, a gyűlöletbeszédre vonatkozó szabályok a két platform esetében megegyeznek, mindkét közösségi felület esetében ugyanaz az ismertető áll a felhasználók rendelkezésére.

---

[27] A gyűlöletet szító nyelvezet. Meta. https://transparency.fb.com/hu-hu/policies/community-standards/hate-speech/ (2022. 04. 19.)

[28] Uo.

[29] Az irányelveinkben szereplő, a COVID 19-re és a vakcinára vonatkozó hírek aktualizálása és az ezeket érintő álhírekkel szembeni védelmi intézkedések. Instagram. https://help.instagram.com/697825587576762?helpref=faq_content (2022. 04. 20.)

Jól megfigyelhető, hogy ezeken a platformokon a gyűlöletbeszéd nemcsak definíció szintjén jól meghatározott, hanem gyakorlati példák, esetek is segítik a pontos határok megszabását. Ennek köszönhetően az algoritmusok, illetve a szűrési célra létrehozott csoportok gyorsan tudnak reagálni bizonyos esetekben. Természetesen ennek a mechanizmusnak érezhetjük a hátrányait is.

Elvégre olyan ügyek is vannak, amelyek nem feltétlen szerepelnek a tételesen meghatározott esetek listájában, olyan védelemre szoruló csoportok is léteznek, akikről szintén nem tesz említést a szabályzat, azonban támadás őket is érheti ezeken a felületeken. Ilyen esetekben a reakció általában lassabb, vagy teljesen elmarad. A nagyon részletes szabályozás esetén nagy hiba, amikor csak bizonyos esetekhez és személyekhez viszonyul nagy pontossággal a szabályok megalkotója. Elvégre ezáltal más közösségek hátrányosabb helyzetbe kerülhetnek ezeken a platformokon.

Ezzel szemben említettük az államok szintjén történő szabályozást is, amelynek esetgyakorlatával összefüggésben megállapítható, hogy az állami bíróságokon a gyűlöletbeszéd vizsgálata részletesebb, értelmezése pedig jóval elméletibb. Természetesen az online felületeknél nem feltétlen az a cél, hogy minden eset alapos elemzésen essen át, hiszen rengeteg az információ, a poszt, a megjegyzés, így az ilyen platformokon gyors reakciókra, nem pedig részletekbe menő kivizsgálásokra van szükség annak érdekében, hogy a közösségi rend fenntartása biztosítva legyen.

III.2. A YouTube felhasználási feltételei

A YouTube annyiban különbözik a már vizsgált közösségi oldalaktól, hogy ezen a felületen a felhasználók elsődleges célja a tartalomgyártás és a mások által feltöltött tartalom fogyasztása. A tartalomgyártás ezen a felületen leggyakoribb esetben vizuálisan, videók formájában történik. A videók alatt található kommentszekció pedig lehetőséget biztosít a felhasználóknak, hogy szabadon kifejezzék véleményüket a megtekintett tartalommal kapcsolatosan, emiatt a gyűlöletbeszéd, a gyűlöletkeltés származhat a tartalomgyártóktól és a tartalmakhoz hozzászóló felhasználóktól is. A YouTube platformján a következőket olvashatjuk a gyűlöletbeszédről:

„A gyűlöletkeltés nem engedélyezett a YouTube-on. Minden olyan tartalmat eltávolítunk, amely erőszakra buzdít vagy gyűlöletet kelt egyének vagy csoportok ellen az alábbi tulajdonságaik alapján: kor, kaszt, fogyatékosság, etnikai hovatartozás, nemi identitás és nemi kifejezés, nemzetiség, faji hovatartozás, bevándorlási státusz, vallás, nemi hovatar-

tozás, szexuális irányultság, súlyos erőszakos események áldozatai és hozzátartozóik, veterán státusz. Ha olyan tartalmat talál, amely sérti ezt a szabályzatot, jelentse azt."[30]

A hivatkozott részletet illetően pár konkrét példát is találunk az ismertetőben, amelyből érdemes lehet néhányat az alábbiakban kiemelni.

„*Örülök, hogy ez az [erőszakos esemény] megtörtént. Azt kapták, amit megérdemeltek [fentiekben felsorolt tulajdonságokkal rendelkező személyekre utalva].*"

„*[A fentiekben felsorolt tulajdonságokkal rendelkező személyek] kutyák*", *vagy* „*[a fentiekben felsorolt tulajdonságokkal rendelkező személyek] olyanok, mint az állatok.*"[31]

Láthatjuk tehát, hogy a YouTube szolgáltatója hasonlóan értelmezi a gyűlöletbeszéd fogalmát és formáit, mint az előbbiekben vizsgált platformok, azonban a példák ellenére sem bocsátkozik olyan részletes leírásokba, amilyenekkel a Facebook és Instagram esetében találkoztunk. A gyűlöletbeszéd szankcionálásáról viszont a következőképpen fogalmaz a YouTube ismertetője:

„*Ha valamilyen tartalom sérti ezt az irányelvet, akkor a tartalmat eltávolítjuk, és a tulajdonost e-mailben értesítjük. Ha ez az első alkalom, hogy megsértetted közösségi irányelveinket, erre valószínűleg felhívjuk a figyelmedet, csatornád azonban nem kap büntetést. Ha ez nem az első eset, akkor a csatornád figyelmeztetést kap. Amennyiben 90 napon belül három figyelmeztetést is kapsz, megszüntetjük a csatornádat. Csatornádat vagy fiókodat a Közösségi irányelvek vagy az Általános Szerződési Feltételek ismételt megsértése miatt megszüntethetjük. Csatornádat vagy fiókodat egyszeri súlyos visszaélés miatt is megszüntethetjük, illetve akkor is, ha a csatornát kifejezetten az irányelvek megsértése céljából hozták létre. Ha úgy ítéljük meg, hogy valamely tartalom közel áll a gyűlöletkeltéshez, akkor korlátozhatjuk az adott tartalomhoz rendelkezésre álló YouTube-szolgáltatásokat.*"[32]

Eme rendelkezések vizsgálata során megállapíthatjuk, hogy a repetitív jelleg, valamint egy bizonyos tolerancia-küszöb átlépése esetén érvénybe lépnek a cselekedet-

[30] Gyűlöletkeltésre vonatkozó irányelv. YouTube Help. https://support.google.com/youtube/answer/2801939?hl=en (2022. 04. 20.)

[31] Gyűlöletkeltésre vonatkozó irányelv. YouTube Súgó. https://support.google.com/youtube/answer/2801939?hl=hu (2022. 04. 20.)

[32] Uo.

nek megfelelő szankciók.

III.3. A felhasználási feltételek közös jellemzői

A három közösségi felület rendelkezéseinek elemzése után megállapítható, hogy ezeknek az oldalaknak a szabályozásában a gyűlöletbeszéd fogalma, formái, valamint a csoportok és személyek, akik ellen ezek irányulnak, jól meghatározottak. Ahogy már hangsúlyoztuk, a részletes szabályozásnak vannak negatívumai és pozitívumai is. Azt viszont meg kell értenünk, hogy a különböző oldalak által kiszabott szankcióknak – ahogy a fentiekben olvashattuk – nem a jogszolgáltatás a közvetlen céljuk, erre a szolgáltatóknak nem terjed ki a hatáskörük.

A szankcióknak a közösségi platformok esetében az oldalakon megjelenő tartalmak szabályozásában van jelentőségük. A közösségi oldalak szolgáltatói csupán annyit tehetnek, hogy a gyűlöletbeszéd különböző formáit törlik, az ezeket terjesztő felhasználókat pedig felfüggesztik. Ennek a folyamatnak gyorsan kell tehát megtörténnie, és pontosan ezért igyekeznek a szolgáltatók részletesen, jól meghatározni a gyűlöletbeszéd fajtáit, hogy ezeket egyből beazonosíthassák és reagáljanak, ezáltal védve a közösséget és közösségi felületük jó hírnevét.

Amennyiben viszont valaki úgy érzi, hogy súlyosan sérült emberi méltóságában, és gyűlöletbeszéd áldozata lett, bírósághoz fordulhat. Az oldal szolgáltatója minden bizonnyal a jelentés után törölni fogja majd a sértő megjegyzést, esetleg felfüggeszti annak íróját, viszont jóvátételt csak a bíróságok szolgáltathatnak. A következőkben két olyan jogesetet fogunk megvizsgálni, amelyben az online megvalósuló gyűlöletbeszédek bírósági szintre is eljutottak.

III.4. Beizaras and Levickas v. Lithuania ügy

A Beizaras and Levickas v. Lithuania ügyben[33] egy homoszexuális pár Instagramra feltöltött képéré reagálva gyűlölködő hozzászólások érkeztek. A pár úgy gondolta, hogy a litván bírósághoz fordul az eset kapcsán, azonban a bíróság úgy ítélte meg, hogy az ügynek nincs akkora súlya és komolysága, hogy eljárást lehessen indítani az elkövetők ellen. Továbbá a bíróság álláspontja szerint a gyűlölködő felhasználók felkeresése felesleges idő- és pénzpocséklás lenne. Az ügy végül az Emberi Jogok Európai Bíróságára is elju-

[33] Case of Beizaras and Levickas v. Lithuania, Application no. 41288/15.

tott, ahol megállapították, hogy a nemzeti bíróságok megsértették a pár magánélethez, jogorvoslathoz való jogát, illetve a diszkrimináció-tilalmat.

Az Emberi Jogok Európai Bírósága döntésében azzal érvelt, hogy a nemzeti bíróságok rosszul mérték fel a gyűlölködő hozzászólások súlyosságát, ugyanis egyetlen olyan megjegyzés, amely buzdít az említett képen szereplő személyek életének kioltására, kellően súlyos ahhoz, hogy az állam jogorvoslatot biztosítson ellene.

Továbbá elutasította a bíróság Litvánia azon érvelését is, miszerint az online közösségi felületeken történő megjegyzések, hozzászólások általánosságban véve nem bírnak akkora jelentőséggel, mint más írásos vagy egyéb kijelentések.

Végső soron tehát az Emberi Jogok Európai Bírósága homofób gyűlöletbeszédként határozta meg a képhez fűzött hozzászólásokat, és megjegyezte, hogy ezek ellen a nemzeti hatóságoknak kötelességük fellépni, még abban az esetben is, ha a hozzászólások íróit nehéz beazonosítani és felkutatni.[34]

III.5. Belkacem v. Belgium ügy

A Belkacem v. Belgium ügy[35] olyan szempontból érdekes és jelentős, hogy tökéletes példája annak, hogy hol húzódik meg az a bizonyos határ a gyűlöletbeszéd és a véleménynyilvánítás szabadsága között. A belga Alkotmány 25. cikke ugyan kinyilvánítja a sajtószabadságot és a cenzúra tilalmát, e jogosultság azonban nem tekinthető korlátlannak. Belgiumban a gyűlöletkeltő magatartás, illetve a holokauszt-tagadás bűncselekménynek minősül.

2012-ben egy Fuad Balkacem nevű állampolgárt kétéves börtönbüntetésre ítéltek az általa közzétett videók miatt. Ezeket a videókat a YouTube felületén osztotta meg, és arra buzdította nézőit, hogy kötelezzék el magukat különböző erőszakos bűncselekmények elkövetésére, amelyek nem muszlim emberek ellen irányulnának. Az ítéletet követően Balkacem az Emberi Jogok Európai Bíróságához fordult, viszont kérelmét elutasították. Az Emberi Jogok Európai Bírósága szerint ugyanis a gyűlöletbeszéd nem

[34] *Barzó* Tímea – *Czékmann* Zsolt – *Csák* Csilla: „Gondolatok köztere" A közösségi média személyiségvédelemmel összefüggő kihívásai és szabályozása az egyes államokban. Miskolci Egyetemi Kiadó, Miskolc 2021. 103. o.

[35] Case of Belkacem v. Belgium, Application no. 34367/14.

tartozik a szólásszabadság által nyújtott keretek közé, ebből kifolyólag pedig helyesnek véli a belga bíróságok döntését.[36]

III.6. Következtetések

A két jogeset kapcsán több tanulság is levonható. Ahogyan már többször is megfogalmaztuk, a nemzeti szabályozás meghatározásai gyakran nem kellően konkrétak, vagy nem helyesen értelmezik azokat.

Az elsőként hivatkozott ügyben a litván bíróságok az online gyűlöletbeszédnek nem tulajdonítottak nagy jelentőséget, azonban a második, belga vonatkozású jogesetben helyesnek mondható döntés született. Mindkét esetben nemzetközi intézményeket is bevontak, ennek oka pontosan abból a tényből fakad, hogy nincs egységes értelmezés a gyűlöletbeszédet illetően.

Megállapíthatjuk, hogy a határvonal megkeresése a véleménynyilvánítás szabadsága és a gyűlöletbeszéd között a nemzeti és nemzetközi joggyakorlatban sokkal bonyolultabb kérdésnek bizonyul, mint az online közösségi térben. Azonban ez okkal van így, a bíróságok tekintetében az a legfontosabb elvárás, hogy ne hibázzanak és a különböző jogszabályokkal összhangban lévő ítélet szülessen, éppen ezért a bíróságok esetében fontos több kulturális, politikai, társadalmi aspektus figyelembevétele. A közösségi oldalak szolgáltatóitól pedig általánosságban azt várja el a felhasználó, hogy valamilyen módon cenzúrázza a káros tartalmakat, így a szolgáltatók esetében sokkal fontosabb a szabályozás részletessége, és kevésbé hangsúlyos az esetek külön-külön történő vizsgálata, hogy ezáltal minél gyorsabban törölni tudják a közösséget megbotránkoztató tartalmakat.

[36] *Barzó – Czékmann – Csák*: i. m. 522. o.

Holéczy Laura Anna
joghallgató (PTE ÁJK), az ÓNSZ Civilisztika Tagozatának tagja

Várallai Luca
joghallgató (PTE ÁJK), az ÓNSZ alelnöke, Civilisztika Tagozatának Tagozatvezetője

Otthonunkban fellelhető *smart* megoldások – avagy az okoseszközök és okosmérő eszközök adatvédelmi, energiajogi vonatkozásai

I. Bevezetés

Napjainkban elképzelhetetlennek tűnik, hogy ne használjunk elektromos áramot, a közvízművek szolgáltatását, gázt vagy a távhőszolgáltatást. Hiányérzetünk támadna, ha az okostelefonunk vagy a személyi számítógépünk nem képezné a mindennapjaink részét, vagy ha az interneten nem tudnánk böngészni. Mindegyikben van egy közös tényező: a digitális technológián alapuló világ. A negyedik ipari forradalom konzekvensen magával ragadta a *Society* 5.0[1] fogalmát is, mely ugyan Japánban[2] terjedt el elsősorban, de az európai kontinens államaiban is kezdődő elemeit vélhetjük felfedezni. Életünk számos területén megjelenik a digitalizáció, melyre a jog kevésbé tud időben és produktívan reagálni, mégis vannak olyan területek, melyeket a magyar jog kezdőlegesen szabályoz. A társadalom legkisebb egységeként a család és mikrokörnyezete tapasztalja először a saját impulzusain keresztül a szociális verzionalitás e számottevő jelenségét, melyet *Society* 5.0 – nak nevezünk.[3] Hol is lehetne ennek táptalaja, mint az otthon, a háztartás? Hogyan válunk fogyasztókká, felhasználókká és akár szolgáltatókká a saját otthonunkban úgy, hogy talán nem is tudunk róla vagy nem gondolunk bele ennek következményeibe, hátulütőibe?

A XXI. században elterjedt *smart* megoldások, a digitalizáció új mérföldkövei rengeteg vívmányt hoztak magukkal, melyek fokozatosan válnak napról napra az életünk részévé. Az automatizálás és a digitális berendezések segítségével már a háztartások is

[1] *Becskeházi* Attila: Verziók evolúciója (Ipar 4.0 és Társadalom 5.0) A valóság verziói. In: Ipar 4.0 Jogi- Társadalmi – Gazdasági kihívások és válaszok (szerk. *Homicskó* Árpád Olivér). Károli Gáspár Református Egyetem Állam – és Jogtudományi Kar, Budapest 2019. 43. o.

[2] Uo.

[3] Uo.

nem csak a kor szellemének, hanem a környezetvédelmi és költséghatékonysági kritériumoknak is megfelelhetnek, ha megfelelő rendszer kiépítését veszik figyelembe.

Az otthonunkban fellelhető okoseszközök és okosmérő eszközök támogató jellege mellett rendkívül sok adatvédelmi és energiajogi kérdés merül fel. Amellett, hogy infrastrukturális biztonságot kínálnak, személyes adataink megadásakor akár magánszféránk is sérülhet, amelyhez kötődően számos jogi szabályozás is napvilágot látott.

Tanulmányunk célja a XXI. század okosotthonainkban fellelhető *smart* berendezések kapcsán felvetődő jogi dilemmák feltérképezése. Szükségesnek tartjuk a köznyelvben sok esetben szinonimaként használt „*okoseszköz*" és „*okosmérő eszköz*" fogalmak közötti distinkciótételt, mely nem csupán technológiai megoldások közötti formális elhatárolás, de meghatározó jogi relevanciával is bír.

II. Okoseszköz, vagyis okosmérő eszköz?

Az okosmérő eszköz definíciója *expressis verbis* rögzítésre került az okos mérés bevezetésével kapcsolatos központi mintaprojekt megvalósításával összefüggő szabályokról szóló 26/2016. (II. 25.) Kormányrendelet 6. pontjában, ami alapján okosmérő eszköznek tekintendő „*minden olyan villamos energia fogyasztásmérő berendezés, földgáz fogyasztásmérő berendezés, bekötési vízmérő, mellékvízmérő vagy okos mérést biztosító külön berendezéssel ellátott villamos energia fogyasztásmérő berendezés, földgáz fogyasztásmérő berendezés, bekötési vízmérő és mellékvízmérő, amely az általa mért és tárolt adatokról valós idejű információt nyújt, és ezen információk közül legalább a tényleges fogyasztásra és a fogyasztási időszakra vonatkozó regiszter adat a kijelzőjén vagy az okos mérést biztosító külön berendezés kijelzőjén elérhető a projekttag számára, biztosítja a tárolt adatok mérésvezérlési központból történő elérését, az utasítások fogadását adatkommunikációs eszköz segítségével, valamint a villamos energia tekintetében a felhasználó által a villamosenergia-hálózatba betáplált villamos energiát is figyelembe veszi*".

Az okosmérők a Nemzeti Energiastratégia energetikai kereslet-kínálat racionalizálását, így az energiahatékonyság növelését megcélzó eszközei. A *smart metering* eszközök olyan intelligens fogyasztásmérők, melyek lehetővé teszik a fogyasztók számára saját fogyasztási szokásaik megismerését, és ezen adatok ismeretében energiafogyasztásuk normalizálását. Lényeges azonban kiemelni, hogy ahhoz, hogy az intelligens mérők valódi zöld innovációt jelenthessenek, azaz a Nemzeti Energiastratégia céljaival összhangban egy „*versenyképes, fenntartható és biztonságos*" energetikai struktúraváltás

következhessen be, elengedhetetlen egy egyre nyitottabb, zöldebb gondolkodású, tudatosabb társadalom.[4]

Az okoseszközök definíciója kevéssé tisztázott a szakirodalomban, azonban meghatározása minden esetben az *Internet of Things* fogalmából kiindulva lehetséges. Az *Internet of Things* („IoT"), azaz a dolgok internete, a *terminus technicus*nak megfelelően egy *machine-to-machine* (a továbbiakban: „M2M") típusú kapcsolatot hoz létre, vagyis gépek közvetlen, automatizált, egymás közötti kommunikációját teszi lehetővé.[5] Ez tehát egy emberi beavatkozás nélküli, mesterséges intelligenciára épülő rendszert jelent, melyet okoseszközök hálózata alkot.[6] Okoseszköznek tekintendő tehát valamennyi olyan eszköz, ami internetkapcsolat által képes más okoseszközzel való adatcserére.

III. Az okoseszközök adatvédelmi kihívásai

A dinamikus technológiai fejlődés gyors reakciót és innovatív jogi megoldásokat igényel. A legjelentősebb kihívást a digitális biztonságot szavatoló, mindenre kiterjedő adatvédelmi szabályozás létrehozása jelenti. Az adatvédelmi szabályozás jogszabályi hátteréként feltétlen megemlítendő az Európai Parlament és Tanács 2016. április 27-i 2016/679 rendelete (a továbbiakban: „GDPR" vagy „*európai általános adatvédelmi rendelet*"), mely külön kiemeli, hogy „*az Európai Unió Alapjogi Chartája 8. cikkének (1) bekezdése és az Európai Unió működéséről szóló szerződés 16. cikkének (1) bekezdése rögzíti, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez*".[7] A nemzeti jogforrási hierarchia csúcsát képező Alaptörvény VI. cikk (3) bekezdése csakugyan deklarálja, hogy „*mindenkinek joga van személyes adatai védelméhez*". Az Alkotmánybíróság 15/1991 (IV.13.) AB határozata, valamint általános gyakorlata „*a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként értelmezi, hanem annak aktív oldalát is figye-*

[4] Nemzeti Energiastratégia 2030, kitekintéssel 2040-ig. Innovációs és Technológiai Minisztérium (ITM), 2020. január. https://www.enhat.mekh.hu/strategiak (2022. 04. 21.)

[5] *Eszteri* Dániel: Az új technológiák megjelenésének hatása a személyes adatok védelmére: gépi tanulás, blokklánc, internet-of-things, agyhullám-olvasás. In: Szemelvények az információs jogokról – a rendszerváltástól napjainkig (szerk. *Péterfalvi* Attila). Patrocínium Kiadó, Budapest 2021.

[6] *G. Karácsony* Gergely: Okoseszközök – Okos jog? A mesterséges intelligencia szabályozási kérdései. Dialóg Campus Kiadó, Budapest 2020. 115. o.

[7] Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) Preambulum (1) bek.

lembe véve, információs önrendelkezési jogként", azaz kiterjesztő értelmezés szerint a személyes adatok védelme az egyén saját adatairól való szabad rendelkezését is magában foglalja.[8] Az adatvédelem részletszabályait az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. (a továbbiakban: Infotv.) határozza meg. Megemlítendő ugyanakkor, hogy az Infotv. mint magyar jogszabály csak azon adatkezelésekre alkalmazandó, amelyekre a GDPR nem, bár e törvény is javarészt visszautal a GDPR-ra. Az alábbi elemzésben mindazonáltal elsődlegesen az Infotv. alapján végezzük az elemzést.

Az okoseszközök mint mesterséges intelligenciával bíró informatikai rendszerek gép-gép típusú kommunikációjuk során adatkezelést folytatnak az Infotv. 3. § 10. pontja értelmében.[9] A hazai szabályozás alapján,[10] az európai általános adatvédelmi rendelettel összhangban,[11] személyes adatként definiálható „*az érintettre vonatkozó bármely információ*". Az Infotv. a személyes adatokon belül megkülönbözteti a különleges adatok kategóriáját, ami olyan szenzitív adatokat jelöl, „*amelyek védelméhez fokozott egyéni és társadalmi érdekek kapcsolódnak*".[12] Emellett külön nevesíti a GDPR rendelkezéseivel összhangban a genetikai, a biometrikus, valamint az egészségügyi adat kategóriáját, azokat az európai általános adatvédelmi rendelet 4. cikkének 13-15. pontjaival azonosan defini-

[8] *Stefán* Ibolya: A mesterséges intelligencia adatvédelmi vonatkozásai. In: Modern Researches: Progress of the legislation of Ukraine and experience of the European Union. Baltija Publishing, Riga 2020. 38–55. o.

[9] Az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 3. § 10. „E törvény alkalmazása során adatkezelés az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése"

[10] Infotv. 3. § 2. „E törvény alkalmazása során személyes adat az érintettre vonatkozó bármely információ."

[11] Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban: GDPR) 4. cikk 1.

[12] *Krausz* Miklós: A különleges adat I. NetJog. 2018. augusztus 4. https://net-jog.hu/2018/08/04/a-kulonleges-adat-i/ (2022. 04. 22.)

álva.[13] Azonban a technológiai fejlődés a jogi szabályozás lépéstartását igényli, a revízió folyamatos lehetőségét. Ma már egyes *smart* eszközök képesek az érzelmi állapotunk pontos feltérképezésére, így fordulhat elő, hogy az okosóra felhasználója stresszel teli, feszült állapotában rezgő értesítést kap „*Vegyél mély levegőt!*" felszólítással és egy irányított tudatos-jelenlét gyakorlattal.[14] Ennek megfelelően a szakirodalomban megjelentek olyan vélemények, melyek szerint az érzelmek mint fokozottan szenzitív adatok az adatkezelés új „tárgyköreként", a fentebb ismertetett rendszeren kívüli halmazt alkotva önálló jogi szabályozást igényelnek.[15] Ezzel szemben más nézetek szerint az érzelmek a biometrikus adatok csoportján belül értelmezendők.[16]

További kihívást jelent, hogy ugyan látszólag a smart eszközök interoperabilitása, azaz együttműködési képessége[17] csupán egy zárt rendszeren belül valósul meg, azonban jelentős kiberbiztonsági kockázatok állhatnak fent az internethálózat alapú működés következtében, mivel a folyamat során akár harmadik személyek is adatokhoz juthatnak jogszerűtlenül.[18]

A külső forrásból származó veszélyeken túl további belső eredőjű rizikófaktort jelent, hogy óriás mennyiségű adat kezelésére kerül sor az okoseszközök által. Ennek oka egyrészt azok konstans bekapcsolt állapota,[19] másrészt a technológia mesterséges intelligencián alapuló sajátos jellege, melynek lényege, hogy a minél nagyobb számú adat által a mesterséges intelligencia képes fejleszteni saját magát,[20] ami egy fokozott adatigényt eredményez, de okként nevezhető meg a M2M típusú felgyorsult kommunikációs folyamat is. Ez utóbbi ugyan szükségszerű jelenség a gépek közötti kommunikáció leegyszerűsítése, így hatékonyságának növelése érdekében, ám egyúttal további potenciális veszélyt jelent az adatbiztonságra azáltal, hogy egy új, külső személy számára nem értelmezhető jelnyelvet eredményez, ami a mesterséges intelligencia működ-

[13] Inftov. 3. § 3. 3a. 3b. 3c. pontok

[14] Apple Watch Series 3. Apple. https://www.apple.com/apple-watch-series-3/ (2022. 04. 22.)

[15] *Stefán*: i. m.

[16] Uo.

[17] Interoperabilitás. Egészségtudományi Fogalomtár. https://fogalomtar.aeek.hu/index.php/Interoperabilitás (2022. 04. 21.)

[18] *G. Karácsony*: i. m. 116-118. o.

[19] Az IoT eszközök térnyerése az adatvédelem tükrében. Arsboni. 2018. január 29. https://arsboni.hu/az-iot-eszkozok-ternyerese-az-adatvedelem-tukreben/ (2022. 04. 21.)

[20] *Stefán*: i. m.

désének átláthatatlanságát idézi elő.[21] Az átláthatatlanság nem csupán megnehezítheti az esetleges későbbi jogi felelősségre vonást, de a jogszerű működést is ellehetetleníti,[22] sértve a GDPR 39. bekezdését, amely deklarálja az adatkezelés átláthatóságának követelményét, rögzítve a könnyen hozzáférhető, közérthető, világos, egyszerű nyelvezettel megfogalmazott kommunikáció elvárását.[23]

Az előzőekben említett, jelentős mértékű adatkezelés következtében könnyen felmerülhet a nem kívánt adatgyűjtés is mint biztonsági kockázat,[24] mellyel összefüggésben az adatkezelő tájékoztatási kötelezettségének megfelelő teljesítése is aggályos lehet.[25] A GDPR az adatkezelés jogszerűségének feltételeként rögzíti a jogszerű jogalap fennállását, azaz „*a személyes adatok kezelésének az érintett hozzájárulásán kell alapulnia, vagy valamely egyéb jogszerű, jogszabály által megállapított - akár e rendeletben, akár más, az e rendeletben említettek szerinti uniós vagy tagállami jogban foglalt alappal kell rendelkeznie*".[26] Az okoseszközök esetében jellemzően a jogalapot az érintett hozzájárulása jelenti,[27] ugyanakkor számos esetben azt az érintett önmagában az okoseszköz használatával adja meg úgy, hogy annak nincs tudatában.[28] Ezzel összefüggésben azonban lényeges kiemelni, hogy a GDPR rendelkezéseivel összhangban az Infotv. rögzíti az érintett előzetes tájékozódáshoz való jogát, azaz azon jogosultságát, hogy „*az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékoztatást kapjon*".[29] Ez az adatkezelői kötelezettség azonban számos esetben az okoseszköz sajátosságaiból

[21] *G. Karácsony*: i. m. 116–118. o.

[22] Uo.

[23] GDPR Preambulum (39) bek. „A személyes adatok kezelésének jogszerűnek és tisztességesnek kell lennie. A természetes személyek számára átláthatónak kell lennie, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, azokba hogy tekintenek bele vagy milyen egyéb módon kezelik, valamint azzal összefüggésben, hogy a személyes adatokat milyen mértékben kezelik vagy fogják kezelni. Az átláthatóság elve megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint hogy azt világosan és egyszerű nyelvezettel fogalmazzák meg."

[24] *Kerti* András - *Koller* Marco: Az okoseszközök applikációi által gyűjtött metaadatokkal való visszaélések kockázati szemléletmód általi, felhasználói szintű lehetséges visszaszorítása. Hadmérnök 16/4. sz. 145. o.

[25] *Stefán*: i. m.

[26] GDPR Preambulum (40) bek.

[27] *Stefán:* i. m.

[28] Uo.

[29] Infotv. 14. § a) pont

fakadó technikai akadályokba ütközik, így például az okosórák kisméretű kijelzője jelentős kihívást jelenthet a jogszerűen eljáró adatkezelők számára.[30]

Az általános adatvédelmi rendelet a személyes adatok kezelésére vonatkozó elvként rögzíti, hogy „*a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon*”.[31] Ugyanakkor nem elhanyagolható körülmény, hogy a mesterséges intelligencia technológia sajátosságaiból fakadóan képes az adatok alapján a felhasználó igényeinek kalkulációjára, pontos prognosztizálására, [32] valamint a felhasználói szokásokon túl az érdeklődési kör, akár kapcsolati rendszer feltérképezésére, ami azonban teret teremthet a visszaéléseknek.[33] A GDPR által meghatározott, a jogszerű célra vonatkozó követelményeken túl az Infotv. 4. § (1) bekezdése rögzíti, hogy „*az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának*”,[34] ami magába foglalja az adatkezelő saját belső struktúráján belüli célhoz kötött jellegét is,[35] azaz nemcsak a nem kívánt adatkezelés kiküszöbölésére szolgál ezen elv, de kiterjed annak tilalmára is, hogy az adatokat eltérő célból használja fel az adatkezelő.

Mindezeken felül információs aszimmetriát[36] idézhet elő, valamint az átláthatóság követelményét sérti az adatkezelő kilétének megállapításának aggályos jellege.[37] A GDPR 39. bekezdése rögzíti az átláthatóság követelményével összefüggésben, hogy „*ez*

[30] Az IoT eszközök térnyerése ...

[31] GDPR 5. cikk (1) bek. b) pont „A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; a 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („célhoz kötöttség”)”

[32] *Eszteri*: i. m.

[33] *Kerti – Koller*: i. m. 145-146. o.

[34] Infotv. 4. § (1) bek. „Személyes adat kizárólag egyértelműen meghatározott, jogszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok gyűjtésének és kezelésének tisztességesnek és törvényesnek kell lennie.”

[35] *Stefán*: i. m.

[36] *Vincze* János: Miért és mitől védjük a fogyasztókat? Aszimmetrikus információ és/vagy korlátozott racionalitás. Közgazdasági szemle 2010/8. sz. 725–752; Egészségügyi Fogalomtár. Információs asszimetria. https://fogalomtar.aeek.hu/index.php/Inform%C3%A1ci%C3%B3s_aszimmetria (2022.06.13.)

[37] Az IoT eszközök térnyerése ...

az elv vonatkozik különösen az érintetteknek az adatkezelő kilétéről [...] való tájékoztatására".

IV. Fogyasztói attitűd, felhasználói dilemmák, valamint a Smart Home innovációjának térnyerése

Az előzőekben ismertetett, általános jelleggel, tipikusan felmerülő adatvédelmi anomáliák ellenére, amennyiben helyes az International Data Corporation (IDC), a világ első számú információtechnológia, telekommunikációs- és fogyasztói technológiai piacokat vizsgáló[38] cégének „előrejelzése", úgy 19,6 százalékos növekedés valósulhat meg a mesterséges intelligencia piacán, melynek következtében 2022 végére 432,8 milliárd dollárra emelkedhet a piac mérete, míg 2023-ra az 500 milliárd dolláros lélektani határt is meghaladó expanzió prognosztizálható.[39] Lakossági szinten is jól megfigyelhető tendencia az okoseszközök iránti töretlen, sőt egyre fokozódó érdeklődés, amit a Nemzeti Kibervédelmi Intézet által 2020-ban lefolytatott lakossági felmérés 2022-ben publikált eredményei hűen tükröznek, hiszen a felmérésben részt vevő személyek 96 százaléka rendelkezett okostelefonnal, valamint ezen felül 15,3 százalékuk okoskarkötő felhasználó is, továbbá csaknem 19,2 százalékuk otthonában rejlik valamilyen okos háztartási eszköz is.[40] Lényeges azonban kiemelni, hogy ugyan a vizsgált mintán belül a férfiak, valamint a budapesti lakosok aránytalanul nagyobb számban töltötték ki a felmérést, így az eredmények nem tekinthetők teljes körűen átfogónak,[41] azonban korszakunk általános irányait kitűnően reprezentálják az adatok: az okosmegoldások tagadhatatlanul a mindennapjaink szerves részévé váltak.

A Zion Market Research kutatása szerint az okosotthonok globális piacának értéke 2022 végére több mint 14,5 százalékos növekedést érhet el az öt évvel korábbi adatokhoz képest, csaknem 53,45 milliárd dollárra emelkedve.[42] Az okosotthon techno-

[38] Finding new ways... IDC Summit. https://www.idc.com/eu/events/68242-idc-summit (2022. 04. 21.)

[39] Arat az AI. Computerworld. https://computerworld.hu/uzlet/idc-arat-az-ai-307041.html (2022. 04. 21.)

[40] *Palicz* Tamás – *Bonnyai* Tünde – *Bencsik* Balázs – *Pintér* Levente – *Hornyik* Zsuzsanna – *Joó* Tamás – *Bor* Olivér – *Dombrádi* Viktor: Biztonságtudatosság a kibertérben – a 2020-as országos lakossági felmérés eredményei. Belügyi Szemle 2022/2. 402. o.

[41] *Palicz* – *Bonnyai* – *Bencsik* – *Pintér* – *Hornyik* – *Joó* – *Bor* – *Dombrádi*: i. m. 414. o.

[42] Global Smart Home Market Increasing at a Good Pace to Reach USD 137.9 billion by 2026. Zion MarketResearch. 2021. október 20. https://www.zionmarketresearch.com/news/smart-ho-

lógiája lényegében egy innovatív „*épületfelügyeleti rendészeti*" megoldás,[43] mely lehetővé teszi az otthonunk automatizálását.[44] Az automatizáció nemcsak a kézi vezérlést, a környezeti hatásokhoz igazodó működést, vagy az előreprogramozott utasítások szerinti önműködő rendszert foglalja magába, de lehetővé teszi az IoT-eszközök általi távvezérlést is.[45] Az automatizáción túl az okosházak megkülönböztető sajátossága, hogy nemcsak egyes funkciók önálló automatizáltsága valósul meg, de egy központi egység által összehangolt mechanizmus is kerül kialakításra.[46]

A 2020-ban világméretűvé vált koronavírus-járvány jelentős mértékben hozzájárulhatott a Smart Home technológiák iránti érdeklődés exponenciális növekedéséhez, hiszen a szignifikánsan megnövekedett mértékű otthon töltött idővel egyenesen arányosan előtérbe került a kényelem és biztonság fokozott igénye,[47] mely jellemzők az okos otthonok innovációjának sajátjai, az energiagazdálkodás okos- és zöldmegoldásaival egyetemben.[48]

Ugyanakkor az Eurobarometer 2017-es felmérése alapján az európai lakosok csupán 61 százaléka tekint pozitívan a mesterséges intelligencia hordozta lehetőségekre.[49] A csaknem számtani középhez közeli százalékos arány hátterében az „*uncanny valley*" jelenségen[50] túl pontosan a rendezetlen, bizonytalan kérdések húzódhatnak meg – amelyeknek egy nagy halmaza adatvédelmi jellegű –, hiszen a válaszadók 88 százaléka a

me-market (2022. 04. 21.)

[43] Intelligens otthon. Tudástár. https://www.intelligensotthon-tudastar.hu/ (2022. 04. 23.)

[44] *Mandić* Dorottya: A mesterséges intelligencia alkalmazása az okosotthonokban. Biztonságtudományi Szemle 4/1. sz. 35. o.

[45] *Mandić*: i. m. 35-36. o.

[46] Intelligens otthon ...

[47] *Mandić*: i. m. 34. o.

[48] Intelligens otthon ...

[49] Mi az a mesterséges intelligencia és mire használják? Európai Parlament. https://www.europarl.europa.eu/news/hu/headlines/society/20200827STO85804/mi-az-a-mesterseges-intelligencia-es-mire-hasznaljak (2022. 04. 21.)

[50] *Eszteri*: i. m. „Emberi lényként hajlamosak vagyunk arra, hogy a „gondolkodó gépet" egy ponton túl antropomorf, az élő szervezetekre jellemző tulajdonságokkal ruházzuk fel, végső soron pedig mint – felsőbbrendűnek hitt – új létformát az emberiségre veszélyt jelentő jelenségként azonosítsuk. A filozófiában ezt a jelenséget a hátborzongató völgy (uncanny valley) fogalmával írták le először az 1970-es években. Ezek szerint, amint egyre inkább emberszerűbbek lesznek a robotok, úgy nő velük szemben a rokonszenvünk – de egy ponton túl, amikor már nagyon emberszerűek, egyszer csak bizarrnak, hátborzongatónak és veszélyesnek látjuk őket"

mesterséges intelligenciával összefüggő technológiák gondos kezelését szorgalmazta.

Ilyen adatbiztonsági kockázatot jelenthet egy Smart Home esetén, hogy az okoseszközök vezérlése a legtöbb esetben egy mobilapplikáción keresztül lehetséges, mely alkalmazás használata érdekében számos személyes adatot kényszerülünk megadni magunkról. Ezenfelül kijelenthető a mesterséges intelligencia működési mechanizmusából kiindulva, hogy valamennyi okoseszköz pontos elemzéseket készíthet akár az egyes felhasználói szokásokról,[51] mely adatok harmadik személy kezébe jutva jelentős biztonsági kockázatot jelenthetnek. Például a téli időszakban alkalmazott temperáló fűtéssel felfűtött lakás vagy a hetek óta fel nem töltött okoshűtő információja harmadik személy tudomására jutva komoly biztonsági rizikót jelenthet. Csakugyan számottevő veszélyt rejthet, amennyiben egy okos kamerarendszerhez illetéktelen nyer hozzáférést. Nem véletlen tehát, hogy az Európai Bizottság biztonsági unióra vonatkozó uniós stratégiájáról szóló 2020-ban közzétett közleménye alapján az Európai Unió összlakosságának több mint fele „*attól tart, hogy a bűnözők és csalók hozzáférhetnek az adataihoz*".[52]

Mivel a „*bűnözők gyorsan alkalmazkodnak a változásokhoz, és saját céljaikra fordítják az új technológiákat*",[53] így az adatvédelmi szempontok dinamikus integrációja, a technológiai innovációkra irányuló gyors jogalkotói megoldások korunk egyik legjelentősebb jogi kihívását jelentik.

V. Okosmérő eszközök és az okosotthonok energiajogi kérdései

Az okoseszközökhöz hasonlóan a smart metering eszközök bevezetése csakugyan alapos adatvédelmi szabályozást igényel, melynek követelményét a Nemzeti Energiastratégia is nevesíti. A smart mérők, illetve intelligens mérőeszközök számtalan előnyt jelentenek a fenntartható energetikai fejlődés szempontjából a háztartásokban, illetve a villamosenergia elosztási tevékenységét végző társaságok esetében. Lehetővé válik használatukkal és beüzemeltetésükkel az energiafelhasználás nyomon követése, az energiaszolgáltatóval való kommunikáció, illetve az egész ingatlan energetikai rendszerének feltérképezése. Az eszközök segítségével lehetőség nyílik a fogyasztási

[51] *Kerti – Koller*: i. m. 146. o.

[52] A biztonsági unióra vonatkozó uniós stratégia. A Bizottság közleménye. COM(2020) 605. 2020. július 24. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52020DC0605&from=EN#footnote14 (2022. 04. 24.)

[53] Uo.

szokások vizsgálatára is, mely globálisan jelentheti az üvegházhatás visszaszorításában való tevékeny részvételt.[54] Az okosmérő eszközök körében találunk olyan biztonságtechnikai berendezéseket, melyek egymás között is képesek összehangoltan kommunikálni. A használó ilyenkor – főleg, ha a villamosenergia aspektusát tekintjük – fogyasztóvá lép elő. A fogyasztóvédelmi és adatvédelmi kérdések ebben az esetben komplexen merülnek fel, tekintettel arra, hogy az energiaszolgáltató és a fogyasztó között létrejött „kapcsolatból" bizonyos adatok kerülnek ki a fogyasztási szokásokat illetően.

Fontos megemlíteni a European Green Deal[55] (továbbiakban: EGD) által kitűzött célt, melynek 2050-ig kell, hogy megfeleljenek a tagállamok.[56] Az éghajlat- és környezetvédelmi kihívások terén alkotott dokumentum olyan uniós szakpolitikai iránymutatásokat fogalmazott meg, mint pl. „*a fenntartható és intelligens mobilitásra való ellátás felgyorsítása*", az „*energia- és erőforrás-hatékony építés és korszerűsítés*" vagy a „*tiszta, megfizethető és biztonságos energiaellátás*". Az Európai Bizottság szerint 2050-re elérhető a klímasemlegesség,[57] melyre további stratégiát alakított ki, ám ezekhez további intézkedések szükségesek még az EGD-n kívül is. A „*Tiszta, megfizethető és biztonságos energiaellátás*" - hoz kapcsolódó fejezetben[58] az Európai Bizottság célul tűzte ki az energiarendszer dekarbonizációját, mely elengedhetetlen a további éghajlatvédelmi intézkedések körében. Az energiahatékonyság prioritásként való kezelése több problémát is megoldana, így először azt kell figyelembe venni a stratégiák között. Ehhez hozzájárul az is, hogy az intelligens infrastruktúrára való átállást szorgalmazni kell az Európai Unió területén belül, illetve egy határokon átnyúló program keretén belül kell megvalósítani. A harmonizáció érdekében a Bizottság szorgalmazta a transzeurópai energetikai

54 Okosmérés. MVM Next. https://www.mvmnext.hu/ee/egyetemes-szolgaltatas/tudnivalok/hasznos-informaciok/okosmeres (2022. 04. 20.)

55 Európai Bizottság közleménye az Európai Parlamentnek, az Európai Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. „Az európai zöld megállapodás" c. közlemény: COM (2019) 640. 2019. december 11. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:52019DC0640 (2022.06.13.)

56 Uo.: „... az EU-t olyan igazságos és virágzó társadalommá kívánja alakítani, amely modern, erőforrás-hatékony és versenyképes gazdasággal rendelkezik, ahol 2050-re megszűnik a nettó üvegházhatásúgáz-kibocsátás, és ahol a gazdaság növekedése nem erőforrásfüggő."

57 Az Európai Bizottság közleménye: Tiszta bolygót mindenkinek – Európai hosszú távú stratégiai jövőkép egy virágzó, modern, versenyképes és klímasemleges gazdaságról, COM (2018) 773. 2018. november 13. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52018DC0773 (2022.06.13.)

58 A Bizottság közleménye... i. m.

infrastruktúráról szóló rendelet[59] áttekintését, illetve az újabb technológiák és infrastruktúrák bevezetését, továbbá az intelligens hálózatok/energiahálózatok beépítését. A megoldást a Bizottság a mesterséges intelligencia nagyobb térnyerésében látja, így az *okosmérő eszközök*, illetve a *smart otthonok* elterjedése bizonyosan egy megfelelő lépést jelentene a klímapolitika elősegítésében és a Földünk megmentésében. A dokumentumban emellett kulcsfontosságúnak titulálják a digitális technológiák katalizátorként való funkcionálást a különböző ágazatok klímavédelmi törekvéseinek előmozdításában. Az 5G, a felhőalapú számítástechnika, a mesterséges intelligencia, valamint az Internet of Things gyorsító tényezőként hathatnak a szakpolitikák eredményes kimenetelében, így mindenképpen számolni kell velük a nemzetközi, regionális és a nemzeti jogban. A Bizottság többek között egy külön erre szakosodott ágazat kialakítást helyezte előtérbe, mely a digitalizáció segítségével kifejezetten az éghajlatvédelmi törekvésekre fókuszálva motorként szolgál majd a társadalomban is.

Az Európai Parlament és a Tanács 2012/27/EU Irányelve (2012. október 25.) az energiahatékonyságról, a 2009/125/EK és a 2010/30/EU irányelv módosításáról[60] (továbbiakban: 2012/27/EU Irányelv) tartalmazza a European Green Deal által is szorgalmazott okosmérő eszközök lokális szinten történő elterjesztését, mely elősegíti az Európai Unióban az energiahatékonyság megvalósulását.[61] A 2012/27/EU Irányelv részletezi, hogy az ezzel kapcsolatos szabályozásnak uniós szinten átfogóbbnak és pontosabbnak kell lennie a tagállami beüzemeltetési eljárásokat is figyelembe véve. Ennek következtében valószínűsíthető, hogy ezzel a fogyasztók igénye és hajlandósága is növekedhet ilyen eszközök beszerzésére a saját otthonukban, illetve az energiaszolgáltatók nagyüzemi szervezeti gondolkodásának interpretációja átültethető a háztartások szintjére is.[62] A tényleges fogyasztáson alapuló számlázás sokkal precízebb alternatívája is a pozitívumok között mondható ennek kapcsán, ellenben az ehhez szükséges infor-

[59] Az Európai Parlament és a Tanács 347/2013/EU rendelete a transzeurópai energiaipari infrastruktúrára vonatkozó iránymutatásokról és az 1364/2006/EK határozat hatályon kívül helyezéséről, valamint a 713/2009/EK, a 714/2009/EK és a 715/2009/EK rendelet módosításáról.

[60] Az Európai Parlament és a Tanács 2012/27/EU irányelve az enegiahatékonyságról, a 2009/125/EK és a 2010/30/EU irányelv módosításáról, valamint a 2004/8/EK és a 2006/32/EK irányelv hatályon kívül helyezéséről.

[61] *Biró* Zsófia: A fogyasztókat érintő legfontosabb technológiai újdonságok és lehetséges szabályozásuk a magyar energiaszektorban. In: A technológiai fejlődés jogi kihívásai: Kézikönyv a jogalkotás és jogalkalmazás számára (szerk. *Kis Kelemen* Bence – *Mohay* Ágoston). PTE ÁJK, Pécs 2021. 6. o.

[62] „[G]ondolkozz előbb kicsiben" elv megtalálható a 2012/27/EU Irányelvben

mációhoz való hozzáférés kérdését is tisztázni kellett.

Az okoshálózat (ún. *smart grid*) gyakorlatilag egy olyan összegyűjtő és újrafelhasználást lehetővé tevő elektromos hálózat, mely költséghatékonyan és üvegházhatás-intenzitással elektromos áramot juttat a fogyasztókhoz az infokommunikációs és egyéb vezérlést végző hálózatok közreműködésével. A modern energiatakarékossági és energiahatékonysági keretek között így a villamosenergia is újrafelhasználhatóvá válik a háztartások számára közvetetten. Meg kell említeni, hogy a rendszer úgy működik, hogy a szolgáltató bizonyos adatátvitelt végez, majd ezzel párhuzamosan a fogyasztóval is kapcsolatba kerül, így a kétirányú kommunikációval hatékonyabban lehet felmérni az energiaigényt.[63]

Az okosotthon ezzel összefüggésben, ám tágabb értelmezésben egy olyan informatikai rendszer, mely az egész háztartásban működő elektromos rendszerek közötti összehangolást és irányítást látja el. A távolsági ellenőrzést az infokommunikációs csatornákon keresztül teszi lehetővé a rendszer magja, amellyel akár a fűtőberendezések, a szórakozáselektronika, a hűtőberendezések és az árnyékolástechnika is megoldható.[64]

A már említett adatvédelmi kérdések tekintetében összefonódik a fogyasztó érdekeinek figyelembevétele, a hatékonyság növelése és a piacon lévő szereplők szokásainak feltérképezése, így az említett energiaszolgáltatók adatokhoz jutnak, cserébe a fogyasztók megfelelő szolgáltatást kapnak, hiszen ezáltal a szolgáltatók értékesíteni tudják az „árujukat". Kérdés, hogy a fogyasztói igények kielégítése érdekében felhasznált adatok mennyire sértik az Alaptörvényben is rögzített személyes adatok védelméhez való jogot a magyar szabályozás alapján.[65] Milyen relációban működhet jól ezen adatok felhasználása úgy, hogy ezáltal ne sérüljön semmilyen jog, de közben betöltse a rendeltetését az adatfelhasználás? Melyik élvez prioritást: a szolgáltatás megfelelősége vagy az adataink védelme? Ehhez kötődik a célhoz kötöttség elve, melynek információs önrendelkezési funkciójából adódik, hogy az adatkezelő csak olyan adatot használhat fel a későbbiek során, amelyre az érintett hozzájárulása vonatkozik. Értelemszerűen nem

[63] *Rostás* Péter: Digitalizáció az energetikában: Az energiaszektor közvetlen digitalizációja. DLA Piper. 2020. március 11. https://blogs.dlapiper.com/advocatus/2020/03/digitalizacio-az-energetikaban-az-energiaszektor-kozvetlen-digitalizacioja/ (2022. 04. 21.)

[64] Uo.

[65] Magyarország Alaptörvénye (2011. április 25.) VI. cikk (3) bekezdés

szükséges az elképzelt szituációban a fogyasztó villamosenergia-felhasználási igényének felméréshez olyan adat, amelynek nincsen relevanciája, amely kezeléséhez ráadásul nem is járult hozzá. Az adatkezelés minden szakaszában teljesülnie kell a célhoz kötöttség elvének, illetőleg ha célja megszűnt, magát az adatkezelést is meg kell szüntetni. A tevékenység emellett vonatkozik harmadik személy részére történő hozzáférhetővé tételre és nyilvánosságra hozatalra, így az érintett kezében van a lehetőség.[66] A fogyasztói igények kielégítése érdekében ennek ellenére olyan adatok is kikerülhetnek az érintett kezéből, amelyek a fogyasztói szerepkörében előnyös helyzetet teremthetnek, de adatvédelmi szempontból hátrányosabb pozíciót takarhatnak. Ezért is fontos megemlíteni, hogy a fogyasztónak biztosítani kell az információs önrendelkezési jogának gyakorlását.[67] Mit tehetünk a fogyasztói szerepkör védelmének érdekében amellett, hogy ez a feltétel is teljesüljön?

Az *Európa Tanács 1981. január 28-án kelt Egyezménye az egyének védelméről a személyes adatok gépi feldolgozása során*[68] (továbbiakban: Egyezmény) már tartalmazza azt a koncepciót, miszerint nem csak az állami szektor köteles betartani az Egyezmény rendelkezéseit, hanem a magánszektor is, így országhatárokon átívelő jogközelítési folyamat indult meg e tekintetben, illetve egyre szélesebb spektrumot jelent a magánjogi korrelációban. Az Egyezmény II. fejezet 5. cikkének c) pontja kimondja, hogy „*az adatoknak tárolásuk céljával arányban kell állniuk, és meg kell felelniük e célnak, azon nem terjeszkedhetnek túl*".[69] Ez megfeleltethető a célhoz kötöttség elvének, így szintén elmondható, hogy a hazai szabályozás kissé elmaradott a nemzetközi viszonylathoz képest.

VI. A Nemzeti Energiastratégia mint új energiapolitika

Az EGD-re adott reakciója a magyar szabályozásnak a Nemzeti Energiastratégia 2030, kitekintéssel 2040-ig[70] (továbbiakban: Nemzeti Energiastratégia) volt, mellyel Magyar-

[66] *Czékmann* Zsolt: Infokommunikációs jog. Dialóg Campus Kiadó, Budapest 2019. 214. o.

[67] *Fézer* Tamás: A fogyasztók adatainak és privátszférájának védelme elektronikus környezetben. In: A fogyasztók védelmének új irányai és kihívásai a XXI. században (szerk. *Szikora* Veronika – *Árva* Zsuzsanna). DE ÁJK, Debrecen 2018. 54. o.

[68] Az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről szóló 1998. évi VI. törvény

[69] Uo.

[70] Nemzeti Energiastratégia 2030, kitekintéssel 2040-ig. Innovációs és Technológiai Minisztérium (ITM), 2020 január. https://www.enhat.mekh.hu/strategiak (2022. 04. 24.)

ország energiapolitikáját határozták meg 2040-ig. A már korábban is kiadott a villamos energiáról szóló 2007. évi LXXXVI. törvény ugyan tartalmazott valamelyest hasonló célokat, ellenben a Nemzeti Energiastratégia jóval széles körűbb tájékoztatást, iránymutatást ad a jövőre nézve. Az Innovációs és Technológiai Minisztériumtól származó dokumentum legfontosabb részeit tekintjük át a következőkben.

Az energiaszektorban történő változások nem feltétlenül generálták a szabályozó környezet, az ellátásbiztonság, a költséghatékonyság és a beszerzési portfóliók felülvizsgálatát. Így a legfőbb intézkedés ezek megvalósítását jelenti, mely Magyarországon az energetika, mint stratégiai ágazaton belül működhet permanensen. Az új Nemzeti Energiastratégiát nem csak az energiahatékonysági, uniós megfelelési szempontok ihlették, hanem a magyar társadalom jólétével kapcsolatos, illetve a nemzetbiztonsági és gazdasági kérdések is szerepet játszottak.[71] A tanulmány szempontjából lényeges rész, hogy „*a családok energiafüggetlenségét a háztáji, saját célra történő megújuló energia-termelés támogatásával és az okos mérők elterjedésének elősegítésével lehet előmozdítani*".[72] Ezzel a célkitűzéssel megalapozódott az okosmérő eszközök és okos megoldások elterjedésének államilag történő ösztönzése a magyar szabályozás alapján, melynél felhívjuk a figyelmet, hogy csak az „ösztönzésre" került sor. A támogatásokkal kapcsolatban a későbbiek folyamán írunk.

A Nemzeti Energiastratégia középpontjában a fogyasztó áll, mely koncepció az egész dokumentumon tetten érhető. A fogyasztók aspektusából vizsgálandó preferenciák a következők: az alacsony rezsi, erősödő energiafüggetlenség és a nagyfokú választási szabadság.[73] Ezen tényezők megvalósulásának kiemelt szereplője a magyar családok és háztartások otthonaiban történő technológiai újításokhoz kapcsolódó támogatás az állam részéről, melynek egyik lehetséges eszköze az okosmérők bevezetése, illetve a fogyasztók energiatermelővé válásának (*prosumerré*) ösztönzése.[74] Az energiaellátás, illetve az energiafelhasználás egy új modellt alakított ki a XXI. században, amelyben a fogyasztók már képesek önellátóan is fedezni a saját energiaigényük szerint a felhasználást, mely egy rugalmas, kényelmes hozzáférést is jelent. Ennek a modellnek való

[71] Nemzeti Energiastratégia 2030, kitekintéssel 2040-ig: i. m. 9. o.
[72] Uo.
[73] Uo. 15. o.
[74] Uo.

megfelelésnek próbál eleget tenni a magyar társadalom, mely megoldást nyújthat az energiaszektor éghajlatvédelmi konklúzióihoz.[75]Ehhez azonban nagyobb hajlandóságot kell mutatni a zöldenergia terén mind az állam, mind a társadalom részéről, akár az oktatás és a média közrehatásával, mert csak így lehetséges a lakosság felvilágosítása is. Az olyan állami támogatások, mint pl. a „*Lakóépületek energiahatékonyságának és megújuló energia felhasználásának növelését célzó visszatérítendő támogatás*"[76] biztosítják a háztartások számára a bizonyos időn belül történő energetikai újítások pénzügyi hátterét.

A dokumentumban meghatározásra kerül a villamosenergia-szolgáltatás terén a fogyasztásmérők okosmérő eszközökre való kötelező kicserélése, illetve az ezen szolgáltatók, kereskedelmi és hálózati engedélyesek számára előírják, hogy ilyen okosmérő eszközzel rendelkező ügyfeleiknek kedvezőbb hálózat-kihasználást, illetve ajánlatokat biztosítsanak. Továbbá megfogalmazásra került, hogy a jogszabályi környezet is újításra szorul, így a jövőben ennek eleget kívánnak tenni.[77]

Ha egy hétköznapi magyar háztartást veszünk górcső alá, akkor az energetikai tényezőket figyelembe véve kevésnél találunk okosmérő eszközöket, inkább még a hagyományos mérő a populárisabb. A különbség hatalmas, tekintve, hogy már 10%-kal alacsonyabbá tehetjük az energiafelhasználásunkat.[78] A szimpla mérő mutatja az elfogyasztott energia mennyiségét, kvázi mutatja a mérő állását. Az okosmérő ennél jóval többet tud adni, hiszen tárolja, továbbítja az akár negyedórás adatokat is a központi hálózaton keresztül az energiaszolgáltató felé, aki kérésre, illetve időlegesen feldolgozza ezeket az adatokat, amely alapján konzekvenciát lehet levonni egy adott háztartás energetikai beállítottsága terén. Ezeknek az adatoknak nagy szerepe van az energiafelhasználás optimalizálásában, az okosmérő eszközök alkalmazásával egy átlagos magyar háztarás is hozzájárul a szén-dioxid kibocsátás redukálásához. A fogyasztási adatok kikéréshez nem kell mást tenni, mint a területileg illetékes elosztói engedélyeshez egy kérelmet kell

[75] lásd: Javaslatok, konklúziók

[76] GINOP-8.4.1/a-17 Lakóépületek energiahatékonyságának és megújuló energia felhasználásának növelését célzó hitel. https://www.palyazat.gov.hu/node/62377/revisions/102712/view# (2022. 04. 24.)

[77] Nemzeti Energiastratégia 2030, kitekintéssel 2040-ig: i. m. 17. o.

[78] Akár 10 százalékos energia-megtakarítást is hozhatnak az okosmérők. Intellimeter blog. 2013. augusztus 3. https://intellimeter.blog.hu/2013/08/03/rezsicsokkento_okos_merok_5-10_szazalekos_megtakaritast_is_hozhatnak 2022. 04. 24.)

benyújtani (pl. ELMŰ, ÉMÉSZ).[79]

VII. Javaslatok, konklúziók

Az uniós és nemzetközi jogi szabályozások figyelembevételével célszerű egy olyan nemzetgazdasági stratégiát kialakítani, mely az EGD által megfogalmazott 2050-ig elérendő céloknak megfelel, illetve elősegíti a háztartások zöldebb működését és a digitalizáció vívmányainak igénybevételével az okosabb otthonok kialakítását akár az egész magyar társadalom berkein belül. Ehhez hozzátevődik, hogy nem csak a magánszektor nagyobb társaságait vagy magukat az energiaszolgáltatókat kell mozgósítani e téren, illetve a különböző ipari ágazatokat, hanem a családokat, háztartásokat és a mikrogazdasági elemek szereplőit. A *prosumer-modell* elegendő lehet az energiahatékonysági stratégiák kialakításának első állomásaként, de ezekhez az állami és uniós támogatások lehetősége elengedhetetlen a háztartások számára.

Az okoseszközök, okosotthonok adatkezelőinek valóban jogszerű adatkezelésének biztosítása érdekében az érintettek előzetes tájékoztatásának hatékonyabbá tétele elengedhetetlen. Ehhez szükséges egy olyan az adatkezelési nyilatkozat, mely nem csupán egy beikszelt négyzet, vagy laikusként értelmezhetetlen jogi szakzsargon, hanem egy olyan tájékoztatás, mely ténylegesen biztosítja az érintett megfelelő informálását.[80] Ehhez elengedhetetlen a „*jogi szöveg hatású jelleg*" minimálisra redukálása,[81] amihez kiváló eszközt nyújthatnak az egyre nagyobb teret nyerő *legal design* megoldások. A *legal design* egy olyan új jogi és közben a laikusok által is értelmezhető, külföldön elterjedt alternatíva, mellyel a vállalkozások ügyfélközelibbé tehetik szolgáltatásukat a jogi dokumentumokkal kapcsolatban, egyszerűbbé tehetik az adatkezelési dilemmákat, csökkenthetik a pereskedési hajlamot és a jogviták kialakulását, nem mellesleg a grafikus elemekkel való ábrázolás esztétikai szempontból sem elhanyagolható a modern a megoldások körében.[82]

[79] Okosmérés. EoN. https://elmuemasz.hu/versenypiaci-szolgaltatas/tudnivalok/hasznos-informaciok/okosmeres (2022. 04. 24.)

[80] Az IoT eszközök térnyerése ...

[81] Uo.

[82] Legal Design. Data Protection Solutions. https://dataprotectionsolutions.hu/legal-design/ (2022. 04. 24.)

Horváth Dominik
joghallgató (PTE ÁJK), az Óriás Nándor Szakkollégium Közjogi Tagozatának tagja

Az országgyűlési választások digitalizációjának lehetősége Magyarországon

I. Bevezetés

Magyarország alkotmányos rendszerében a képviseleti demokrácia elvei élveznek elsőbbséget.[1] Ez talán leginkább az országgyűlési választások során érzékelhető az állampolgárok számára. Jelen kutatás azt kívánja feltárni, hogy a képviseleti demokrácia alapját képező hagyományos magyar választási rendszer áthelyezhető-e a digitális térbe. Ezen kívül megvizsgálja azt is, hogy ez milyen hatással lenne az állampolgárok szavazási szokásaira, illetve milyen politológiai, illetve szociológiai következményei lennének mindennek.

A fent érzékeltetésére a tanulmány az alábbi kérdésekre is keresi a választ: Van-e gyakorlati példa külföldön a teljes vagy akár részleges elektronikus választásra? Hogyan lehetne ezeknek a példáknak kombinált vagy akár tiszta modelljét alkalmazni hazánkban? Magyarországon lenne-e jogi háttere az elektronikus választások bevezetésére? Külföldi és magyar tapasztalatok alapján, milyen hatással lenne az elektronikus választási rendszer bevezetése a magyar társadalomra? Eltántorítja vagy inkább motiválja az állampolgárokat a választásokon való részvételre??

II. Az elektronikus választás szükségessége

A legtöbb demokratikus állam küzd a választásokon való részvételi arány folyamatos csökkenésének problémájával. Ez a csökkenő tendencia szemügyre vehető például az 1994-es, valamint 2010-es magyar országgyűlési választások részvételi arányán: 1994-ben az első fordulóban a szavazati jogosultsággal rendelkező állampolgárok 65%-a adta le a szavazatát, míg 2010-ben az országgyűlési választáson alig haladta meg a 45%-ot a választási részvétel. A hajlandóság csökkenése leginkább a fiatalabb korosztálynál figyelhető meg.[2]

---

[1] Magyarország Alaptörvénye (2011. április 25.), Alapvetés B) cikk 4. bekezdés; *Kocsis* Miklós – *Petrétei* József – *Tilk* Péter: Alkotmánytani alapok. Kodifikátor Alapítvány, Pécs 2015. 141. o.

[2] *G. Karácsony* Gergely: Az elektronikus szavazási eljárás egyes kérdései 174. o. https://dfk-online.

Ezzel szemben megfigyelhető az is, hogy napjainkban a szavazási hajlandóság fokozatosan elkezdett emelkedni. Az Európai Parlamenti választások esetében megfigyelhető, hogy 2004-ben a szavazati joggal rendelkező állampolgárok 38,63%-a adta le a szavazatát.[3] Ezt valóban a szavazási kedv csökkenése követte 2009-ben, amikor több, mint 2%-ot csökkent a résztvevők a száma a 2004-es választásokhoz képest. Ebben az évben választópolgárok 36,31%-a rögzítette a szavazatát.[4] A következő Európai Parlamenti választásnál beszélhetünk a legalacsonyabb részvételről, ugyanis 2014-ben a választójoggal rendelkező embereknek csupán 28,97%-a ment el szavazni. Ez majdnem 10%-os eltérést jelent a 2004-es választásokhoz képest.[5] A következő ciklusnál viszont a polgároknagyobb hányada vett részt a 2019-es választásokon. Ebben az évben közel 20%-al emelkedett a leadott szavaztok száma: 2019-ben a választópolgárok 43,58%-a juttatta érvényre az akaratát.[6]

Több európai ország szeretné javítani a választásokon való részvételi arányt. Az elektronikus szavazás egy olyan megoldás lehet, amely növelhetné a választási hajlandóságot, azáltal, hogy meg tudná szólítani a fiatalabb generációkat. Valószínűsíthető, hogy egy ilyen megoldás bevezetése növelné ennek a csoportnak a részvételét a különböző választásokon.[7] Ugyanakkor azzal is számolni kell, hogy egy ilyen rendszer esetleges bevezetése más társadalmi rétegek, pl. az idősek, alacsonyabb iskolai végzettséggel rendelkező személyek, kisebb településeken élő választópolgárok esetében éppen ellenté-

sze.hu/images/egyedi/bihari/karácsony.pdf (2022. 03. 04.) Fontos megjegyezni, hogy a magyar országgyűlési választások esetében is növekvő tendencia mutatkozik a választópolgárok szavazási hajlandóságában. 2014-ben például 61,73 százalék vett részt a szavazáson. 2018-ban a választásra jogosult összes választópolgár 69,73 százaléka rögzítette a szavazatát. 2022-ben minimális eltérés vehető észre az előző országgyűlési választáshoz képest, hiszen ebben az évben a szavazati joggal rendelkező polgárok 69,59 százaléka adta le a szavazatát. Ezekből az adatokból kiindulva elmondható, hogy a szavazási hajlandóság Magyarországon inkább emelkedő, de legalább stagnáló helyzetet mutat. Ld. Nemzeti Választási iroda: http://republikon.hu/media/9504/valasztasok_2014_ri.pdf (2022. 04. 20.); Nemzeti Választási Iroda https://www.valasztas.hu/ogy2018 Nemzeti Választási Iroda https://vtr.valasztas.hu/ogy2022 (2022. 04. 20.)

[3] 2009-es Európai Parlamenti választások: https://static.valasztas.hu/dyn/ep09/outroot/hu/0/emjk.htm (2022. 04. 20.)

[4] Uo.

[5] 2014-es Európai Parlamenti választások: https://static.valasztas.hu/dyn/ep14/szavossz/hu/emjk.html (2022. 04. 20.)

[6] 2019-es Európai Parlamenti választások: https://www.valasztas.hu/ep2019 (2022. 04. 20.)

[7] *Karácsony*: i. m. 174. o.

tes, választási hajlandóságot csökkentő hatást generálna, amely adott esetben a részvételi arány csökkenését eredményezheti.

Az eredményesség nagyban függ az adott ország társadalmának az internetbe vetett bizalmától. Ezt a szempontot megelőzi még a számítógépek használatának gyakorisága, valamint a számítógépek elfogadása. Fontos szempontnak mondható még a közigazgatási rendszerébe vetett bizalom. Hazánkban a digitalizálódott közigazgatás ismertnek és elterjedtnek mondható, amelyből fakadóan az állampolgárok viszonya az elektronikus rendszerekkel kapcsolatban sokkal kiegyensúlyozottabb. Sasvári Péter egy 2015-ös kutatásában kimutatta, hogy a közigazgatási rendszerek elfogadottságának mértéke nem befolyásolja a polgárok elektronikus választásának szándékát. Ebben az esetben Magyarország és Ausztria estét vizsgálta meg és vonta le ezt a következtetést.[8] A számítógépek használatával kapcsolatosan viszont kimutatták a nemek közötti egyenlőtlenséget is. Kutatások szerint női nem jobban érdeklődik az elektronikus választási rendszer kialakításával kapcsolatban, viszont nagyobb százalékban utasítja el annak használatát. Az elektronikus kereskedelem elterjedése és használata folyamatosan növeli az elektronikus ügyintézés népszerűségét is. A korosztályok közötti különbségből fakadóan elmondható az, hogy a fiatalabbak könnyebben meg tudnak bízni egy-egy elektronikus rendszerben és ezért az elektronikus szavazás is gyorsabban, valamint könnyebben elterjedhetne közöttük.[9]

III. A szavazási metódusok csoportosítása

Papír alapú szavazásról abban az esetben beszélhetünk, amikor a választójoggal rendelkező állampolgárok a nyomtatott, hagyományosnak tekinthető szavazólapon tollal rögzítik a szavazatukat.[10]

Amennyiben azonban a szavazatok leadására elektronikusan kerül sor, úgy elektronikus szavazásról beszélhetünk.[11] Az elektronikus jelleg ebben az esetben abban nyilvánul meg, hogy infokommunikációs technológia alapú rendszereket, eszközöket, háló-

[8] *Sasvári* Péter: Az e-szavazási hajlandóság empirikus vizsgálata Ausztriában és Magyarországon. In: Tudásteremtés és alkalmazás a modern társadalomban. Tudásmenedzsment Konferencia, Szeged 2015. 10. o.

[9] Uo. 5–7. o

[10] *Karácsony*: i. m. 174. o.

[11] *Sasvári*: i. m. 2. o.

zatokat stb. veszünk igénybe.[12]

Az International IDEA nemzetközi szervezet kutatócsoportja elméleti alapon csoportosította ezeket a digitális szavazási rendszereket. Alapvetően két opciót különített el a szervezet. Az első az az ellenőrzött, míg a másik a nem ellenőrzött környezetben történő szavazat leadás. A különbség abból fakad, hogy míg az ellenőrzött környezetben az ezzel megbízott tisztségviselők kontroll alatt tudják tartani az elektronikus szavazás menetét, addig a másik esetben ezt az ellenőrzést nem tudják garantálni.[13]

Az fenti mellett egyéb csoportosítási szempontokkal is találkozhatunk. Lehet beszélni papíralapú szavazásról, valamint gépi szavazásról is (on-line és off-line). A papír alapú szavazás alatt a klasszikus értelemben vett eljárást értjük, amikor a választók nyomtatott szavazólapra rögzítik a szavazatukat. A másik kategória a gépi alapú szavazás, amely azt jelenti, hogy a választópolgárok valamilyen szavazógép segítségével fejezhetik ki a választási akaratukat. A gépi, azaz elektronikus szavazás további két csoportra bontható. Az első csoportba azok a választási rendszerek tartoznak, amelyben az elektronikus eszköz nincsen csatlakoztatva a világhálóhoz. Ebbe a csoportba sorolható például az urnát helyettesítő érintők jelzős számítógép.[14] Ezzel szemben a másik csoporthoz tartozó szavazógépek csatlakoztatva vannak valamilyen hálózathoz – ide tartoznak például a szerver, valamint a kliens gépek. Abban az esetben beszélhetünk internetes szavazásról, amikor a szavazáshoz lebonyolításához tartozó eszközök internetes hálózathoz vannak csatlakoztatva.[15]

Az elektronikus szavazás egyik módja az, amikor egy DRE (*Direct-Recording Electronic*) eszközt alkalmaznak. Az említett eszköz követlenül rögzíti a leadott szavazatokat: az eszköz egy kijelzőn jeleníti meg a szavazólapot és a választópolgár az érintőképernyő vagy ó gombok segítségével tudja leadni szavazatát. Az eszköz a szoftvere segítségével helyben fel is dolgozza a leadott szavazatokat, szükség esetén pedig készít

[12] *Cserny* Ákos – *Nemeslaki* András: Az e-szavazás lehetőségei és korlátai Magyarországon: Kutatási irányok és fejlesztési javaslatok az e-demokrácia kiterjesztésére. In: Választási dilemmák: Tanulmányok az új választási eljárási törvény nóvumai és első megmérettetése tárgyában (szerk. *Cserny* Ákos). Nemzeti Közszolgálati Egyetem, Budapest 2015. 238. o.

[13] *Petrovics* Roberto: Az i-választás lehetőségei Magyarországon az észt modell tükrében Scriptura 2019/2. sz. 1–2. o.

[14] *Sasvári*: i. m. 2. o.

[15] *Karácsony*: i. m. 174–175. o. Sasvári: i. m. 2–3. o.

egy nyomtatványt is. Ezt követően a hordozható memóriáját elviszik a szavazatösszesítés és véglegesítésé helyszínére, ahol pontosan tudják elemezni a leadott szavazatokat.[16]

Ezt a módszert azonban sok esetben túlságosan manipulálhatónak találják, ezért még sehol nem volt próbálkozás országos szinten bevezetni. Egyelőre önkormányzati, valamint tartományi szinteken alkalmazzák egyes országokban, mindenesetre a választópolgárok körében kifejezetten nagy népszerűségnek örvend.[17]

Van egy további lehetőség is: mégpedig az, amikor a szavazatukat leadni kívánó polgárok otthoni internet-kapcsolat segítségével fejezhetik ki választói akaratukat. Ez az opció viszont magában hordoz kockázatos elemeket: hackerek számára például megkönnyíti az említett rendszerek befolyásolását.[18]

IV. Külföldi példák

Európán belül már több ország is elkezdte tesztelni a digitális szavazás különféle típusait. *Franciaországban* már 2003-ban megkezdték az internetes választások tesztelését.[19]

Az *Egyesült Királyság* 2000-ben kezdte tesztelni a digitális választások lehetőségeit. Több szavazókörzetben is tesztelték már az interneten vagy pedig telefonon keresztül leadható szavazatok hatékonyságát. Viszont a teszt során több kérdés is felmerült a kialakított rendszernek a megbízhatóságával kapcsolatban. 2003-ban kb. 1,5 millió választópolgár adta le a szavazatát interneten, telefonon vagy pedig SMS-en keresztül. Megállapították ekkor, hogy nem lesz elegendő egy csatorna biztosítása, hanem többet szükséges igénybe venni egy ilyen nagy volumenű használat során.[20]

Ausztriában a Bécsi Gazdasági és Üzleti Adminisztráció Egyetem közreműködésével három e-szavazási tesztet is elvégeztek. 2006-ban zajlott az egyik ilyen teszt, amit párhuzamosan indítottak az éppen aktuális elnökválasztással, úgy, hogy a leadott szavazatok természetesen semmilyen kihatással nem voltak hagyományos választási eljárás menetében zajló választásra.

[16] *Sasvári*: i. m. 3. o.
[17] Uo.
[18] Uo.
[19] Uo. 4. o.
[20] *Karácsony*: i. m. 176. o., Sasvári: i. m. 4. o.

Észtország kifejezetten előrehaladott állapotban van a választás digitalizálásával kapcsolatban. Az országban 2007 óta elektronikus országgyűlési szavazásokat tartanak. Ezt megelőzte egy 2005 januárjában lebonyolított főpróbája a rendszernek. 2009-ben az Európai Unió engedélyezte az észteknél az Európai Parlamenti szavazások internetes rendszeren történő megvalósítását. Ez jelezheti, hogy az általuk létrehozott digitális rendszer megfelelően teljesíti a megbízhatóság, valamint a biztonság követelményeit.[21]

Svájc abszolút különleges helyzetben van, tekintve, hogy az országban évente többször is kinyilatkoztatják a választópolgárok az akaratukat. Az 1990-es évektől náluk már elterjedt a postai szavazás, amely jelentősen kényelmesebbé tette a választásokon való részvételt. A legszélesebb körű szavazási kísérletnek a Genfi Internetes Szavazási Rendszert lehet tekinteni. Az a kártya a központi eleme ennek a rendszernek, amelyet minden választás előtt kézhez kapnak a választópolgárok. Ez a kártya szükséges mind a személyes, mind a levél, mind pedig az interneten keresztül történő szavazáshoz. Személyes szavazás esetén a kártyát magával kell vinnie a polgárnak, míg levélszavazás esetén a szavazattal együtt a borítékban el kell küldeni. Az internetes szavazásnál a kártyán található kóddal tudja leadni a szavazatát az akaratát kinyilvánító állampolgár. Egy személyes azonosító kód is található a kártyán, ami a lekaparható felület eltávolítása után lesz látható. A lekaparást követően a kártya nem használható fel sem a személyes, sem pedig a levélszavazat leadását illetően. A kártyán szereplő 16 szájegyből álló kód, a lekaparás után látható azonosító kód, valamint a születési idő és hely megadásával tudja azonosítani magát a választópolgár az internetes szavazás felületén. Az azonosítás csak az után történik meg, hogy a szavazatról visszaigazolást küld a rendszer a szavazópolgárnak.[22]

Németországban jelenleg kétféle opciót tartanak megfelelőnek az elektronikus választás esetét tekintve. Az egyik megoldásnak az elektronikus szavazógépeket tartják, míg a másik megoldásnak a digitális tollat. A digitális toll lényege az, hogy a választó a szavazatát speciális szavazólapra, speciális tollal adja le. Ennek a szavazási metódusnak a lényege, hogy a tollon található rögzítő eszköz, ami egy kamera, felveszi a leadott szavazatot és a szavazópolgár, amikor leadja a papírt és a tollat a papír a hagyományos megoldások alapján lesz kezelve, míg a tollat egy beolvasó eszközbe helyezik és az elekt-

[21] *Petrovics*: i. m. 1–3. o., Sasvári: i. m. 4. o.

[22] *Karácsony*: i. m. 176. o.

ronikus szavazatot is összeszámolják. A két szavazási rendszer egymás mellett párhuzamosan működik. Németország ennek a választási formának nagy úttörője. 1999-ben több egyetemen, valamint állami és magán tanácsok választásait is elektronikus választási rendszer segítségével vitték véghez.[23]

Belgium területén már 1994-ben megjelentek az elektronikus szavazógépek első változatai. Az elektronikus szavazógépek használatához a választópolgárok egy mágneses kártyát kapnak, amely alapján a szavazógép megjeleníti a szavazólapot. Ezt követően tudja leadni a szavazatát a választópolgár, amelynek eredményét a mágneses kártya rögzíti. Ezt a kártyát juttatják a hagyományos szavazó urnába. Ebben az esetben a szavazatok összeszámolásának az ideje rövidül meg jelentősen a mágneses kártyák használatából fakadóan. 2007-ben például az elektronizált lehetőségnek köszönhetően öt órával hamarabb összeszámolták a szavazatokat, mint a hagyományos, papír alapon leadott szavazatokat.[24]

Az *Amerikai Egyesült Államokban* a 2016-os elnökválasztáson már csak Kolorádóban, Oregonban és Washingtonban lehetett kizárólag levélszavazattal rögzíteni a szavazati döntéseket. Az összes többi államban már működött az elektronikus szavazás.[25]

V. Választási alapelvek érvényesülése

A demokratikus választási alapelvekkel össze kell vetni az elektronikus szavazás megvalósulásának lehetőségét és azt, hogy az alapelveknek milyen mértékben tudna megfelelni az elektronikus választás egy-egy megoldása.

A *választás általánossága* azt jelenti, hogy mindenki, aki jogosult a választásra, az részt vehet rajta, illetve nem zárható ki senki sem, aki részt vehetne a szavazáson. Ez az alapelv a választójog demokratizmusának garanciája. A választásra jogosultak alanyi körét a lehető legszélesebben határozza meg. A választójoggal rendelkező állampolgárok nyilvántartását a Nemzeti Választási Iroda vezeti egy elektronikus nyilvántartásban.[26] Ennél a szempontnál szükséges megvizsgálni azt, hogy nem okozna-e aránytalanul nagy

[23] *Karácsony*: i. m. 176. o. Sasvári: i. m. 4. o.

[24] *Karácsony*: i. m. 175–176. o.

[25] *Kocsis* Gergő: Elektronikus választási rendszerek az Egyesült Államokban. Arsboni. 2017. május 15. https://arsboni.hu/elektronikus-valasztasi-rendszerek-az-egyesult-allamokban/ (2022. 04. 18.)

[26] *Petrétei* József: Magyarország alkotmányjoga I. Kodifikátor Alapítvány, Pécs 2016. 226–227. o.

nehézséget bizonyos társadalmi csoportoknak az elektronikus szavazás. A papír alapon történő választás nem kifejezetten képes alkalmazkodni a speciális bánásmódot igénylő szavazati joggal rendelkező állampolgárokhoz. Az elektronikus szavazás esetében megvalósuló szavazógépi megoldás esetében nincsen számottevő eltérés a papír alapú szavazás esetéhez képest. Az interneten, azaz távolból is megvalósítható szavazás esetébe elmondható, hogy a mozgásukban korlátozott személyek számára sokkal szélesebb lehetőséget tud nyújtani a szavazatuk rögzítésére. Mindazonáltal szükséges szempont az is, hogy az interneten keresztül történő szavazáshoz szükséges két külső forrás, amellyel nem minden ember rendelkezhet, illetve az ezekkel való rendelkezésre nem kötelezhető egy választópolgár sem. Ezek az internethozzáférés és a szavazat rögzítésére alkalmas eszköz. Ezek biztosítását az állam is tudná garantálni a helyszíni szavazógépekhez hasonlóan. Ezzel a megoldással megoldódna az a diszkriminatív szempont, miszerint nem mindenki rendelkezik internethozzáféréssel és egy olyan eszközzel, amit például egy kijelölt helyen a szavazás időtartama alatt tud használni.[27] A következő szempont lehet, hogy milyen mértékben számít diszkriminációnak az, hogy egyes választópolgárok a saját eszközüket használva tetszés szerinti időben, helyszíntől függetlenül adhatják le a szavazatukat, míg azok az állampolgárok, akik szavazatukat eszköz és internet kapcsolat hiányában egy megadott helyszínen tudják csak leadni.

A *választás egyenlőségének* alapelve értelmében minden választásra jogosult választópolgár azonos számú és azonos értékű szavazattal rendelkezik. Illetve egyenlő jogokkal vehet részt a választásban. Ennek az alapelvnek a választásra jogosultak körében kell érvényesülnie. Ezen túlmenően a választójog egyenlőségének alapelvéből levezethető a jelöltek és a jelölő szervezetek esélyegyenlőségének követelménye is.[28] Az elektronikus választás esetében szükséges biztosítani azt, hogy a szavazati joggal rendelkező állampolgár internetes, azaz távoli szavazás esetén is tudja magát azonosítani és csak egyszer szavazhasson. Több országnak is van megoldása ezeknek a szempontoknak a megfelelő kezeléséhez.[29] Releváns szempont, hogy ezeket digitálisan szükséges megvalósítani és a technológia jelenleg folyamatosan fejlődik. A blokklánc technológiában nagy lehetőségek rejlenek, amelyeket az elektronikus választás során alkalmazni lehet-

[27] *Karácsony*: i. m. 177.o

[28] *Petrétei*: i. m. 228–229. o.

[29] *Karácsony*: i. m. 176.o

ne.[30] Lentebb még esik erről a technológiáról is említés

A *választás titkosságának* elve kimondja, hogy minden választópolgár a saját választói döntését mások megítélésétől mentesen hozhatja meg. Valamint szavazata nyilvánosságra kerülés nélkül meghozható. Az Alkotmánybíróság véleménye szerint az alapelv azt a követelményt támasztja, hogy az államnak mindent meg kell tennie, hogy a szavazó állampolgárok által leadott szavazatok tartalma mások számára ne legyen megállapítható, illetve megismerhető. Ez egy feltétlen érvényesülést kívánó követelmény.[31]

A *választás szabadsága* szerint minden választójoggal rendelkező szavazó a választójogával szabadon, azaz kényszer, vagy más meg nem engedett külső befolyás nélkül élhet. Ez az alapelv rögzíti a választópolgár önkéntes részvételét is.[32]

A titkosság esetében releváns szempont, hogy milyen módon van biztosítva az, hogy a polgár szavazatának tartalmát ne ismerje meg harmadik személy, és a szavazatokat összegyűjtők se tudják megállapítani az állampolgárok szavazatáról, hogy pontosan kihez melyik szavazat tartozik. A szavazófülke egyszerű, de megfelelő megoldásnak bizonyult eddig a szavazatok titkosságának megőrzését illetően. Az elektronikus szavazás esetében nagyobb a valószínűsége a külső behatásnak, akár a társadalmi, akár családi nyomásnak. A Velencei Bizottság álláspontja alapján a levélszavazatokban rejlő kockázatokhoz képest a családi szavazásban nem rejlik több kockázat.[33] Ennek ellenére fontos szempont, hogy a szavaztok rögzítésére szolgáló eszközök kinek a tulajdonát képezik. Ez olyan szempont lehet, amelyen keresztül nagyon könnyen befolyásolhatóvá válhatnak a családtagok. Érdekes, hogy egy ilyen esetben a közügyek védelme élvez prioritást a magánélettel szemben és nem pedig fordítva. Ennél az alapelvnél megállapítható az, hogy a szavazófülke magánya biztosítja megfelelőbben a szavazópolgárok számára a szavazat rögzítésének lehetőségét. Amint kihelyezzük ellenőrizetlen helyszínre a szavazást, je-

[30] Bővebben lásd: Albin *Benny* – Aparna Ashok *Kumar* – Abdul *Basit* – Betina *Cherian* – Amol *Kharat*: Blockchain based E-voting System. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3648870 (2022. 03. 04.); R. Ramya – Nischal Ramesh – Mithrashree Sekar – G. Pushpak: E-ballot system based on blockchain technology. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3884812 (2022. 03. 04.)

[31] *Petrétei:* i. m. 230. o.

[32] *Petrétei:* i. m. 231 o.

[33] Draft report on the compatibility of remote voting and electronic voting with the demands of the documents of the council of europe. European Commission for Democracy Through Law. CDL-EL (2003) 16. 2003. november 28.

lentősen megnövekszik annak a kockázata, hogy nem érvényesülnek megfelelően, vagy tisztán az alapvető választási elvek. Ezeknek a kiküszöbölésére nyújthat megoldást az, hogyha a szavazó többször is le tudja adni a szavazatát és minden esetben csak az utolsó, azaz a végső szavazata lenne érvényes. Ez jelentősen megnehezítené a befolyásoló szándék érvényesülését, valamint a választópolgár illetéktelen ellenőrzését.[34]

A *szavazás közvetlensége* kimondja, hogy a választók és a választottak között nem érvényesülhet befolyás, azaz mindenki személyesen adhatja le a szavazatát, mások közbeiktatása nélkül. A törvényhozónak kötelessége olyan szabályokat hoznia, hogy ez az alapelv is érvényesülni tudjon. Eddig erre a szavazófülke magánya jelentette a megoldást. Itt az elektronikus választás megvalósulása esetében sérülhet ez az alapelv is. Sokkal kevésbé ellenőrizhető, hogy valóban a szavazati jogosultsággal rendelkező személy adja-e le a szavazatát vagy pedig az, akinek hozzáférése van az adott eszközhöz.[35]

VI. A 2021-es előválasztás

Magyarországon 2021-ben a szövetséget kötött ellenzéki pártok „előválasztást" tartottak[36], amelynek az volt a célja, hogy egy közös miniszterelnök jelöltet tudjanak kiállítani a kormánypárti miniszterelnök jelölt ellen. Ez az előválasztás két fordulóból állt. Az első fordulóban még öt jelölt mérkőzött meg egymással, az utolsóban pedig már csak kettő.[37]

Ezen a választáson a választópolgároknak hagyományos, illetve elektronikus módon is volt lehetőségük szavazni. Az online szavazással kapcsolatosan közzétett adatkezelési tájékoztatóban több szempontot ismertetnek, valamint egy táblázatba rendezve láthatjuk az adatkezelés célját, a kezelt személyes adatokat, az adatkezelés jogalapjainak és az adatkezelés időtartamának meghatározását. Célok között megfogalmazásra került az azonosítás szükségessége, az adott választókerületben történő szavazási jogosultság ellenőrzése, a 18. év alatti szavazók esetében szülői hozzájárulás megadása az előválasztáson való részvételhez szükséges adatok felhasználása, valamint a kapcsolattartás a szavazatot leadó választópolgárral az országgyűlési választásig. Ezeknek az adatkezelési

[34] *Karácsony*: i. m. 176. o.

[35] *Petrétei*: i. m. 229. o.

[36] Termesztésen az Alaptörvény vagy választási törvény szempontjából ez nem minősült választásnak. Ez egy pártkezdeményezés volt, amit nem az állam szervezett, illetve bonyolított le. A kutatás szempontjából a technológiai megvalósulás miatt fontos ezt is elemezni.

[37] Egy visszalépésből fakadóan az előválasztás három jelöltből két jelölt között dőlt el.

tevékenységeknek adott egy keretet a tájékoztató.[38]

A választás általánossága az előválasztás során érvényesült, hiszen minden szavazati joggal rendelkező állampolgár számára nyitott volt a lehetőség, hogy érvényesítse a szavazati jogosultságát, sőt olyanok is szavazhattak, akik a szavazás időpontjában nem, de a 2022-es országgyűlési választáson már választójoggal rendelkeztek. A választás egyenlősége is érvényesült, mert minden választásra jogosult megegyező számú és megegyező értékű szavazattal rendelkezett. A választópolgárok egyenlő jogokkal vehettek részt az előválasztás során. A szavazás közvetlensége, mit alapelv nem érvényesült, hiszen az alapelvben megfogalmazta a törvényhozó, hogy mindenki személyesen rögzítheti a szavazatát. Az előválasztás során erre is volt lehetőség, de az interneten keresztül rögzített szavazatok esetében hiányzott a személyesség. A szavazás titkossága szintén megvalósult, viszont itt is fontos külön megemlíteni azokat, akik interneten keresztül adták le a szavazatukat. Az internetes megoldás esetében elengedhetetlen az, hogy a szavazók bízzanak a szavazás hátteréül szolgáló informatikai rendszerben. A választás szabadsága esetében releváns tényező, hogy a szavazófülke hiányában voksoló állampolgároknál a rendszer nem tudta ellenőrizni, hogy milyen környezetben, esetleg több ember jelenlétében történt-e a szavazás. Ilyen esetben nem zárható ki a külső befolyásolásnak a ténye. Ebből fakadóan ez az alapelv kifejezetten sérülékenynek mutatkozik.[39]

Az előválasztás során a hagyományos az elektronikus szavazati mód mellett hagyományosan is szavazhattak a választópolgárok.[40] Ehhez első körben el kellett fogadni az adatvédelmi tájékoztatót. Ezt követően minimális adatmennyiséget kellett megadniuk a szavazni vágyó polgároknak. Az adatok megadását követően egy valós idejű kép és hangátviteles rendszerhez csatlakoztatták a szavazót, ahol valós időben ellenőrizték le a szavazó adatait. Ez csupán 1-2 percet vett igénybe, majd ezután kapcsoltak egy operátort, aki jelen esetben egy önkéntesekből álló csoport volt. A hitelesítést és azonosítást követően megjelent a szavazólap, amely egy abszolút letisztult és egyszerű felületnek volt tekinthető. Ezen az ablakon tudta az előválasztásban résztvevő polgár rögzíteni a

[38] Adatkezelési tájékoztató. Előválasztás 2021. https://elovalasztas2021.hu/wp-content/uploads/2021/09/adatkezelesi-szemelyes-210908.pdf (2022. 02. 27.)

[39] *Petrétei*: i. m. 226-231

[40] *Balázsi* Levente: Rekorddal ért véget az előválasztás, a második fordulóban még többen szavaztak. Index. 2021. október 17. https://index.hu/belfold/2021/10/17/ellenzeki-elovalasztas-reszveteli-adatok-szavazas-rekord-miniszterelnok-jelolt/amp (2022. 04. 28.)

szavazatát, majd tudta azt eljuttatni a szavazat számlálókhoz. Az utolsó mozzanatában a szavazásnak elméletileg már teljes mértékben érvényesülnie kellett az anonimitásnak.[41]

VII. Javasolt rendszer

Véleményem szerint a blokklánc alapú elektronikus választási rendszer bizonyul a leginkább alkalmasnak, hiszen a jelentősége abban rejlik, hogy a hagyományos választási rendszerek működtetésének érdekében felhasznált anyagi kiadások jelentős hányada megspórolható lenne.

A javasolt rendszer négy részre osztható. Megkülönböztetjük az adatgyűjtést, a szavazók személyazonosságának ellenőrzését, a megszerzett új adatok blokkokhoz kötését és végül az eredmények közzétételét.

Az elektronikus választások több társadalomban bizonytalanságot ébresztenek, amely fakadhat társadalmi vagy szociológiai bizonytalanságból, vagy pedig technológiai bizalmatlanságból is. A társadalmi és szociológiai bizalmatlanság ellenszere az idő és a népszerűség lehet, míg a technológiai kérdések megválaszolását a blokklánc technológia rejtheti magában.

A blokklánc technológia a *Bitcoin* kriptovaluta gerincét képezi és egy teljesen új korszakot indított el az interneten és az internetes szolgáltatásokban.[42]

A blokklánc egy olyan adathalmaz, amelyben az adatok egy „szétszórt főkönyvben" szerepelnek, csak hozzáfűzhető és emiatt soha nem törölhető. A főkönyv teljesen módosíthatatlan, valamint állandó. Minden blokk egy hash-ből áll, amely függvény függvénye az előző blokknak és minden blokk ilyen módon láncolva van, ezzel erősítve a módosíthatatlan állapot elérését.[43]

A blokkláncok között két típust különböztethetünk meg, az első típusban egy nyilvános blokklánccal találkozhatunk, amelybe bárki írhat vagy olvashat a világ bármely területéről. A másik típus ezzel szemben egy zártabb, egy privát blokklánc, amely megszabja, hogy ki tekintheti meg, vagy éppen ki kapcsolódhat a blokklánchoz. Ehhez

[41] Hogyan lehet szavazni? Előválasztás 2021. https://elovalasztas2021.hu/hogyan-lehet-szavazni/ (2022.05.02.)

[42] *Benny – Kumar – Basit – Cherian – Kharat*: i. m. 1. o.

[43] *Ramya – Ramesh – Sekar – Pushpak*: i. m. 2. o.

a hozzáférést csupán bizonyos csomópontok számára szükséges engedélyezni, amelyek az engedélyezést követően kapcsolódni tudnak a blokklánchoz.[44]

A technikai specifikációk lehetővé teszik, hogy a blokklánc technológiát alkalmazni lehessen az elektronikus választások rendszerében is. Ennek a blokklánc alapú rendszernek az első lépése a regisztráció. Ezt követően a regisztrált választó egy egyedi *hash* címet kap, amelyen keresztül egyszer tud szavazni.[45]

A szavazó állampolgár jelenleg a lakcímének megfelelő szavazókörben, azon belül is a szavazó helyiségben vagy a mozgóurnával szavazhat. A szavazóhelyiségekben reggel hattól este hét óráig lehet szavazni. A szavazónak az azonosítása a szavazóhelyiségben történik meg alapvetően, ahol a kinyomtatott szavazóköri névjegyzékben látják a szavazati joggal rendelkezők névsorát. A szavazást követően a leadott szavazatokat továbbítani kell a megszámolásuk helyére.[46]

Az elektronikus szavazórendszer két alrendszerre osztható. Az egyik a regisztrációs rendszer, míg a másik a szavazó rendszer. Ez a rendszer valóban jelentheti az elektronikus szavazás nyitottabb, átláthatóbb és függetlenebb mivoltját. A nyilvános ellenőrizhetőség is megoldható lehetne, valamint a rendszert meg lehetne úgy alkotni, hogy ne lehessen manipulálni.[47]

Egy ilyen rendszerrel összefüggésben két fő probléma vár megoldásra. Az egyik szempont a platform integritásából, a választási rendszer biztonságából és a választás során biztosítandó adatvédelemből tevődik össze. Illetve ide tartozik még az a szempont is, hogy a valós idejű választásokat folyamatosan követni, valamint ellenőrizni lehessen. A szavazatok leadását követő folyamatok, mint például a szavazatok begyűjtése, elosztása és megszámlálása tartoznak a második szempont körébe. Ezek a folyamatok a technológiai adottságoknak köszönhetően teljes mértékben automatizálhatók. Ezáltal kivonható az emberi erőforrás igénye a szavazási rendnek ebből a fázisából.[48]

A blokklánc technológia egyik legnagyobb előnye, hogy nincs lehetősége külső

[44] Uo.
[45] *Benny – Kumar – Basit – Cherian – Kharat*: i. m. 3. o.
[46] *Petrétei*: i. m. 253-256. o.
[47] *Benny – Kumar – Basit – Cherian – Kharat*: i. m. 3–4. o.
[48] *Ramya – Ramesh – Sekar – Pushpak*: i. m. 3–4. o.

erőnek befolyásolni, törölni vagy akár megváltoztatni a rendszerbe betáplált szavazatokat. Ezáltal csökken az esélye az eredmény befolyásolhatóságának, ami az elektronikus választás elterjedésének egyik kulcsa lehet.

A blokklánc technológiának a három fő tulajdonsága kellőképpen megnyugtató lehet a társadalmak számára, ilyen tulajdonságnak számít a törölhetetlenség, amely megakadályozza az adatok bármilyen módosításának lehetőségét. Az ellenőrizhetőség, aminek az alapját képezi, hogy a blokklánc technológiából fakadóan az összes adat a decentralizált rendszer összes csomópontja, földrajzi és egyéb akadályoktól teljesen függetlenül, akár a fő csomópont sérülése esetén is lekérhető. A következő hasznos tulajdonsága a rendszernek az elosztott konszenzus, amely lényegét tekintve egy protokoll, amely döntéseket hoz, hogy melyik felhasználónak vagy rendszergazdának van engedélye új műveleteket véghezvinni.[49]

A választások során kétféle csomópontból állhatnának. Az egyik a választókerületi csomópont lenne, amely minden választókerületet vagy körzetet lefedne. Ezek a csomópontok egy szoftverszolgáltatóból állnának, amely a „*boot node*"-al dolgozik és ellenőrzi az intelligens szerződést. Az okos szerződések a szavazás megerősítésével és a választókerületi csomópontok ellenőrzésével továbbküldésre kerülnek és így adódnak hozzá a blokklánchoz. Egy alcsomópontnak értékelhető a rendszer indításáért felelős csomópont, amely az összes többinek az összeköttetésért felel, a választókerületi pontok kommunikációjának segítésén kívül.[50]

Intelligens szerződések segítségével hoznak létre az adminisztrátorok szavazólapokat. Meghatározzák az egyes kerületek és választókörzetek jelöltlistáját. A választópolgárok regisztrációját követően az adminisztrátoroknak létre kell hozniuk egy olyan listát, amelyen azok szerepelnek, akik elfogadják a szabályokat. A szavazni kívánó polgár hitelesítésében a kormány szolgáltatása szükséges. Ezt követően minden egyes személy adatai ellenőrzésre kerülnek, majd a leadott szavazatok kapnak egy egyedi azonosító címkét a biztonságos tárolás miatt. Az utolsó fázisban az intelligens szerződések segítségével ellenőrzik az automatikusan összeszámlált szavazatokat. Végül kihirdetik az eredményeket.[51]

[49] Uo.
[50] Uo.
[51] Uo.

Az elektronikus választás, amelynek alapjául a blokklánc technológia, valamint az okos szerződések szolgálnak sokkal inkább számít hatékonyabb és biztonságosabb rendszernek, mint a jelenlegi. Ezt támasztják alá a rendszernek a következő előnyei is. A blokklánc technológia megfékezi, hogy bárki hozzáférhessen a leadott szavazatokhoz, vagy más adatokhoz. A rendszer kizárja a plusz szavazatok hozzáadását, törlését vagy módosítását. A választópolgárok számára biztosított az átláthatóság, amelynek köszönhetően ellenőrizhetik a leadott szavazatokat. A rendszer több csomópontból áll, és ha bármelyik pontot frissítik, a módosított adatok azonnal megjelennek az összes többi ponton is és ezáltal kizárható a szavazó befolyásolása. Az okosszerződések alkalmazhatóságából fakadóan hatalmas humán erőforrás mennyiség megtakaríthatóvá válni a rendszer bevezetésével. A választópolgárok bármikor, bárhonnan le tudják adni a szavazatukat. Egyrészt ez kényelem, másrészt pedig a szavazási hajlandóság befolyásolhatóságának jelentős kockázatát visszaveti. A szavazatszámlálás esetében szintén az egyik fontos szempont a humán erőforrás nélkülözhetősége, míg a másik az, hogy a számolás alkalmával megjelenő szabálytalanságok esélye is redukálódik. Végül meg kell említeni a költséghatékonyságot is, amelynek köszönhetően a megtakarított forrásokat egyéb fejlesztésekre lehet fordítani.[52]

VIII. Ellenérvek az e-szavazással szemben

Az elektronikus szavazással kapcsolatosan megkülönböztethetünk technológiával és társadalmi-szociológiával kapcsolatos ellenérveket.

Az azonosítás a technológián belül az első olyan akadály, amit érdemes fenntartásokkal kezelni. Egy szavazó azonosításakor kétlépcsős folyamatot kell elvégezni. A hitelesítés az első lépcső, amikor megvizsgáljuk, hogy a vizsgált alany valóban létezik-e, valamint rendelkezik-e a szavazás rögzítéséhez és érvényesítéséhez szükséges adatokkal. Ez a folyamat egyszerűbb, hiszen a választói névjegyzékkel szükséges csupán összevetni a szavazatukat rögzíteni kívánó választópolgárokat. Az azonosítás tartozik a második faktorba, amikor megállapíthatóvá válik, hogy az érintett személy valóban az, akinek állítja magát. Technikailag még nem forrott ki a pontos digitális azonosítás megoldása, viszont itt szükséges megemlíteni a levélszavazatok kérdéskörét is, amelyet az országok már régóta elfogadottan alkalmaznak, pedig abban az esetben is az azonosítás

[52] *Ramya* – Ramesh – Sekar – *Pushpak*: i. m. 3–4. o.

hasonló hiányosságait mutatja. Bár az előválasztás, valamint az ügyvédek esetében megvalósuló azonosítás megkezdte ennek a problémakörnek a megoldását.[53] A levélszavazatoknak az alapvető funkciója, hogy a választójog gyakorlásával minél több választópolgár élni tudjon. Ebből fakadóan arányban áll az esetleges sérelem veszélyével. Elmondható, hogy az elektronikus szavazás is alkalmazható eljárás lehetne, hogyha arányban állna a szavazásnak egyéb körülményeivel.[54]

A levélszavazatok esetében találkozhattunk már csalás gyanújával. A levélszavazatok a 2022-es Országgyűlési Választás idején is sok kérdést vetettek fel, hiszen egyes híradások szerint több esetben is felmerült, hogy történtek visszaélések az említett szavazási formával.[55]

A rendszer működésének ellenőrizhetősége is kérdéses az elektronikus megvalósulás esetén, ugyanis a szavazatok leadása, továbbítása, tárolása, összesítése mind számítógépes programok útján történnek, amelyből logikusan következik, hogy az ellenőrizhetőség is kifejezetten bonyolult. Ebben az esetben a szavazatok manipulálásának a veszélye áll fenn.

A Német Szövetségi Alkotmánybíróság kimondta, hogy az elektronikus választás csak akkor lehet összhangban a német alkotmánnyal, hogyha annak minden lépése ellenőrizhető. Ennek megvalósulására megoldás lehet, hogyha a felhasznált szoftverek forráskódjait bárki által elérhetővé teszik és így minden érdeklődő számára áttekinthető

[53] *Farkas* Fanni – *Lovas* Lilla: Távazonosítás, távelőttem és elektronikus ellenjegyzés – melyik mit jelent és mire jó? Jogászvilág. 2021. március 23. https://jogaszvilag.hu/cegvilag/tavazonositas-tavelottem-es-elektronikus-ellenjegyzes-melyik-mit-jelent-es-mire-jo/ (2022. 03. 18.); *Nótin* Tamás: Interneten is lehet szavazni az előválasztáson, indul az előregisztráció. Index. 2021. szeptember 13. https://index.hu/belfold/2021/09/13/indul-az-eloregisztracio-az-elovalasztas-online-szavazasara/ (2022. 03. 16.)

[54] Karácsony: i. m. 180-182. o.

[55] Borítékolható a csalás a levélszavazatokkal. Rések vannak a magyar választási rendszerben. Euronews. 2022. március 30. https://hu.euronews.com/2022/03/30/boritekolhato-a-csalas-a-levelszavazatokkal-resek-vannak-a-magyar-valasztasi-rendszerben (2022. 04. 21.); Kidobott levélszavazatok egy marosvásárhelyi szemétlerakónál. Euronews. 2022. március 31. https://hu.euronews.com/2022/03/31/kidobott-levelszavazatok-egy-marosvasarhelyi-szemetlerakonal (2022. 04. 21.); *Siklós* András: Feljelentést tettek a kidobott levélszavazatok ügyében. Index. 2022. március 31. https://index.hu/belfold/2022/03/31/ellenzek-valasztasi-csalas-hatarontuli-szavazolap/ (2022. 04. 21.); *Farkas* György: László Róbert: A levélszavazás legitimitása megkérdőjeleződik. 24.hu 2022. április 1. https://24.hu/belfold/2022/04/01/laszlo-robert-levelszavazat-valasztas-2022-csalas-ervenytelen/ (2022. 04. 21.)

és véleményezhetővé válna.[56]

Társadalmi ellenérvnek minősül például a digitális megosztottság, amely abban nyilvánul meg, hogy a digitális készülékek kezelése a társadalom egyes csoportjainak számára nehézséget jelenthet. Illetve itt említhető meg a már említett szempont is, ami az internetkapcsolattal, valamint egy szavazat rögzítésére alkalmas eszköznek a birtoklásának társadalmi akadályaiban nyilvánul meg.[57]

IX. Konklúzió

A blokklánc technológia vegyítése az okos szerződésekkel egy ideális elektronikus választási rendszer alapjául szolgálhat. Az azonosítás marad a digitális szavazási rendszernek az egyetlen kérdőjeles része, de arra megfelelő megoldást – vagy legalábbis megfontolandó kiindulási alapot – nyújthat a már hazánkban is megvalósított előválasztás során alkalmazott azonosítási eljárás.

Az elektronikus választás bevezetése még sok megválaszolatlan kérdést tartogat. Ezek a kérdések kockázatot rejtenek, amelyeknek a feltárása nem feltétlenül áll arányban a digitális rendszer bevezetéséből származó haszonnal.

A társadalmi és szociológiai megnyugvás talán elérhető lenne, amennyiben párhuzamosan elindulnának az elektronikus választások a hagyományos választás mellett, valamint az átlagos állampolgár több választás esetében tudná elektronikus formában az akaratát érvényesíteni, valamint helyet kapna az oktatásban is. Az emberek bizalmát csak így szerezhetné meg egy ilyen rendszer.

Problémát jelent azonban, hogy technikailag nem kivitelezhető az elektronikus 100%-os pontossággal rendelkező azonosítás. Figyelembe kell venni továbbá a német alkotmánybíróság rendelkezett fent említett, a transzparenciára és ellenőrizhetőségre vonatkozó elvárásait.

Azt sem szabad elfelejteni, hogy a hagyományos szavazás a választójoggal rendelkező ál-

[56] A hackertámadásokra való tekintettel azonban nem biztos, hogy ez lenne a legjobb megoldás. Ez csupán az alkotmányosságnak való megfelelés egyik módszere, nem pedig az elektronikus választás megvalósításának leghatékonyabb megoldása.

[57] *Karácsony*: i. m. 177-178. o. *Sasvári*: i. m. 6-9. o.

lampolgárok számára egy tradicionális jelentőséggel bíró ünnepi aktust is jelent[58], tehát szubjektív, „érzelmi" indokok is szólhatnak e forma megtartása mellett.

Alapvetően több európai országban szükség lenne egy közvéleménykutatásra, amely az elektronikus választással kapcsolatos kérdésekre keresne válaszokat. Ebből kikövetkeztethető lenne, hogy mekkora szavazó bázist vonzana, illetve veszítene az elektronikus formában megvalósuló választás.

A szavazási hajlandóság növekszik. Meg kell tehát vizsgálni, hogy érdemes-e átállni az elektronikus választás rendszerére pusztán a XXI. század digitalizációs nyomása miatt.

[58] *Karácsony*: i. m. 182. o.

Józsa Ede
szakkollégista, Collegium Iuridicum

A pénz fogalma a modern számítástechnikai vívmányok fényében

I. Bevezetés

A modern világ új technológiák sokaságát hozza létre. Ezek megértése kulcsfontosságú, főleg, ha olyan alapvető fogalmakról alkotott képünket érintik, mint a pénz.

Egyre többet hallunk a *kriptovalutá*król – és az árak hatalmas volatilitásáról –, továbbá az előállításukról, azaz a bányászásról. Ezek elsősorban és alapvetően közgazdaságtani és mérnöki problémákat vetnek fel, de a kriptovaluták társadalmakra gyakorolt hatásaira tekintettel az ezt övező kérdések a jogászok figyelmét sem kerülhetik el. A kriptovaluták és az alapjukat képező technológiai megoldás(ok) társadalomra gyakorolt hatásait mi sem példázza jobban, mint az, hogy ha a környezetünkben kimondjuk, hogy *Bitcoin*, *Ethereum* vagy *blokklánc* (és sorolhatnánk), gyakorlatilag mindenki elismerően bólogat, pedig igazából a legtöbben meglehetősen hiányos tudással rendelkeznek arról, hogy miről van szó valójában. Véleményem szerint a *kriptovaluták* fogalmával, felhasználásával, illetve szabályozásával kapcsolatosan tájékoztatásra, edukációra van szükség, és be kell látnunk, hogy e feladat nem csak a jövő generációit terhelő kötelezettség. A téma aktualitása tehát vitathatatlan.

Amikor a *kriptovaluták* szabályozásáról beszélünk, alapvetően ellentmondásba kerülünk, hiszen ez szembemegy e technológia lényegével, így fennállna annak a veszélye, hogy éppen az esszenciája veszne el azáltal, ha megvalósulna valamilyen központi ellenőrzés. A paradoxon jelenséget, miszerint szabályozni kellene a szabályozhatatlant, egységes és átfogó, minden nemzet által közösen alkotott és összhangban lévő felülvizsgálattal lehet megoldani, ezáltal kiküszöbölve az egymásnak ellentmondó nemzeti szabályozásokat. Meglátásom szerint tehát ellenőrző szerv hiányában nem tartható kordában ez a rendszer, amire mielőbb egy működőképes megoldást kell megalkotni, hiszen a *kriptovaluták* hamarosan a mindennapi életünk részévé fognak válni.

A dolgozat célja a kriptovaluták legismertebb szereplője, a Bitcoin működésén keresztül bemutatni, hogy ezek a blokklánc technológiára épülő hálózatok miért

jelenhetnek meg a jövőben megfelelő alternatívaként a napjainkban elterjedt (fiat) pénzek helyett, és tölthetik be digitális pénzként a pénzeszköz szerepét.

II. A pénz klasszikus értelemben vett fogalma

Elsősorban a pénz fogalmi körének tisztázásával kell kezdenünk, hiszen csak ezután vizsgálhatjuk, hogy alkalmas-e a *Bitcoin*, valamint az egyéb kriptovaluták sokasága beilleszkedni e fogalomkörbe. Bár amikor a pénzre gondolunk, mindannyian ugyanarra a jelenségre reflektálunk, ez voltaképpen három hagyományos formában jelenik meg az alapvető jellemzői és a pénzügyi rendszerben betöltött szerepe szerint: *készpénz*, *jegybanki számlapénz*, valamint *kereskedelmi banki számlapénz*.[1]

A készpénz a jegybankok által kibocsátott pénz, amely az adott bankkal szembeni követelést testesíti meg, így a készpénz egyben jegybankpénz is. A jegybanki számlapénz szintén jegybankpénznek számít, viszont ezt már csak a kereskedelmi központi bankok használják egymás között, és mint ezen intézmények digitális megtakarítása jelenik meg.[2] A felhasználása a bankok egymás közötti ügyleteinél valósul meg, ennek segítségével számolnak el egymás között, ha két jogalany külön helyen bankol. Tehát a jegybanki számlapénz nem érhető el magánszemélyek, illetve vállalkozások számára. A kereskedelmi banki számlapénz[3] szintén digitális formában megjelenő pénz, amelyet a kereskedelmi bankok hoznak létre a hitelezési folyamat lebonyolításakor.[4] Ez nem követelés formájában jelenik meg a jegybankkal szemben, viszont a kereskedelmi bankok névértéken beválthatják jegybanki számlapénzre.

[1] *András* Bence: A pénz a tárcádban nem más, mint valaki adóssága. Portfolio. 2019. március 13. https://www.portfolio.hu/prof/20190313/a-penz-a-tarcadban-nem-mas-mint-valakiadossaga-315077 (2022.05.27.); *Szabó* Gergely – *Kollarik* András: Az MNB elmagyarázza mi is az a digitális jegypénz. Portfolio. 2017. november 5. https://www.portfolio.hu/uzlet/20171105/az-mnb-elmagyarazza-mi-isaz-a-digitalis-jegybankpenz-266855 (2022. 04. 30.)

[2] Digitális pénzek. Infojegyzet. Országgyűlés Hivatala 2021/43. https://www.parlament.hu/documents/10181/39233854/Infojegyzet_2021_43_digitalis_penzek.pdf (2022. 04. 30.)

[3] A kereskedelmi banki számlapénz átlagosan egy ország pénzének 90%-át teszi ki

[4] A hitelezési folyamat részletesebb bemutatásáért lásd: A hitelek szerepe a pénzteremtésben. Infojegyzet. Országgyűlés Hivatala 2020/88. https://www.parlament.hu/documents/10181/4464848/Infojegyzet_2020_88_hitelek.pdf/9bb611ee-f6be-7257-d1c2-5d17ec046456?t=1607679745716 (2022. 04. 30.)

Amikor a pénz fogalmáról beszélünk, különbséget kell tennünk közgazdaságtani,[5] valamint jogi[6] értelmezés között. Azonban mivel nem rendelkezünk tételes jogi meghatározással, ami a pénz fogalmát behatárolná, ezt a hétköznapi, üzleti, valamint közgazdasági gyakorlatban használt kifejezés tükrében érdemes értelmeznünk. Pénz alatt nem értünk mást, mint azokat a javakat, amelyek adott helyen és időben a pénz gazdasági, valamint jogi természetű funkcióinak eleget tesznek. Mivel a múltban számos eszközt használtak pénzként, a fogalom meghatározása leginkább ennek funkciói[7] révén valósítható meg: értékőrző, értékmérő és *fizetőeszköz*.[8]

Ami a fizetést[9] illeti, annak módozatát általában[10] a diszpozitív jellegű szabályozásnak köszönhetően, valamint a szerződési szabadság elve[11] alapján a felek szabadon határozhatják meg, így jogosultak a pénznem, pénzjószág meghatározására is. Ugyanakkor a jog világában pénz alatt elsősorban a pénznemeket kell érteni, nem pedig a pénzre szóló követeléseket, amilyen a bankszámlapénz.

A pénz elsősorban társadalmi, gazdasági jelenség, amelyet a jól bevált gyakorlat hozott létre, tehát önmagában a jog nem képes egy vagyontárgyat pénzzé tenni. Egy vagyontárgy pénzzé akkor válhat, ha betölti annak funkcióit, esetleg jobb alternatívaként, mint elődje, a jog rendelkezése önmagában nem elegendő ehhez a folyamathoz.

---

[5] *Szóka* Károly: A helyi pénz és társadalmi vonatkozásai. Act Sci Soc 2013/1. sz. 59-66 o.

6 A jog területén a pénz számos formában jelenik meg: pénz, pénzösszegek, összegek, készpénz, ár. Ennek ellenére, bár rendelkezünk számos meghatározással, ezek nem egyenlőek egy egységes meghatározás meglétével. Bővebben lásd: Radu I. *Motica* – Lucian *Bercea*. Banii in codul civil roman. https://drept.ucv.ro/RSJ/images/articole/2006/RSJ1/0104MoticaBercea.pdf (2022. 04. 28.)

[7] *Bánfi* Ziád: A bitcoin-jelenség háttere – a bitcoinról pénzelméleti szempontból. Budapesti Corvinus Egyetem–Nemzetközi Bankárképző Központ Zrt. BADI – Posztgraduális Bankmenedzsment Program. 4. o.

[8] *Világi* Balázs: A pénz digitalizációja új nézőpontból. EconomaniaBlog. https://economaniablog.hu/2021/01/25/a-penz-digitalizacioja-uj-nezopontbol/ (2022. 04. 30.)

[9] Polgári jogi terminológiával élve szavatosabb a teljesítés, ami a szűkebb értelemben vett pénzfizetést is magában foglalja.

[10] A fizetés tekintetében a 2015. április 2-i 70/2015. sz. törvény és 193/2002 számú rendelet a modern fizetési rendszerek bevezetéséről korlátozó intézkedéseket tartalmaz.

[11] A román Polgári törvénykönyvről szóló 2009. évi 287. törvény (a továbbiakban: Rptk.) 1169. cikk

III. Az elektronikus[12] pénz és fajtái

III.1. Az elektronikus pénz szűkebb és tágabb értelemben

Romániában az 1998. március 5-i 58. számú törvény (a banki tevékenységről) határozza meg az elektronikus pénz fogalmát: „*a kibocsátóval szembeni követelést képviselő monetáris érték, amely halmozottan megfelel a következő feltételeknek: a) elektronikus adathordozón tárolják; b) olyan pénzeszközök átvételéért cserébe bocsátják ki, amelyek értéke nem lehet kisebb a kibocsátott pénzértéknél; c) azt a kibocsátón kívül más szervezetek is elfogadják fizetőeszközként*”[13].

Valójában a pénz hagyományos fogalmának bemutatásakor tárgyalt jegybanki és kereskedelmi banki számlapénzek is tekinthetőek úgy, mint csak elektronikus formában megjelenő pénzek,[14] amelyek a digitális formában való létezés szempontjából különböztethetők meg a készpénztől, amely fizikai formában létezik.[15] Ennek ellenére, amikor az elektronikus pénz fogalmáról beszélünk, ez szűkebb értelemben nem foglalja magába a jegybanki és kereskedelmi banki számlapénzek fogalmát.

Ezzel ellentétben a Nemzetközi Fizetések Bank (BIS) értelmezése szerint[16] a tágabb értelemben vett elektronikus pénz fogalmába beletartozik „*minden olyan érték, amelyet elektronikusan tárolnak egy olyan eszközön, mint egy számítógép merevlemeze vagy egy chipkártya, így a tágabb értelemben vett elektronikus pénz fogalmi tartományába tartozhatnak digitális pénznemek is*”.[17] Ugyanakkor amennyiben a szűkebb értelemben vett elektronikus pénz fogalmát tartjuk szem előtt, ebben az esetben csak az tekinthető elektronikus pénznek, „*amit az egyes országok jogrendszere kifejezetten elektronikus pénznek minősít, és így legtöbbször az adott ország törvényes pénznemében denominált, valamint névértékén beváltható jegybankpénzre vagy kereskedelmi banki pénzre, illetve készpénzre is visszaváltható*”.[18]

---

[12] Az elektronikus kifejezést a digitális szó szinonimájaként kell értelmezni.

[13] 1998. március 5-i 58. sz. törvény a banki tevékenységről 3. cikk 13. pont

[14] A digitális pénz, vagyis a kizárólagosan elektronikus formában létező, nem kézzelfogható pénz fogalma nem újdonság ld. https://www.investopedia.com/terms/d/digital-money.asp (2022. 04. 30.)

[15] *Bánfi*: i. m. 5. o.

[16] Digital Currencies. Bank for International Settlements. https://www.bis.org/cpmi/publ/d137.pdf (2022. 04. 30.)

[17] *Bánfi*, i. m. 5. o.

[18] Digital Currencies ...

Továbbiakban a BIS értelmezése szerinti csoportosítást fogjuk felhasználni, alkalmazva az általa megfogalmazott tág értelmezést, így a digitális pénznemek – szintén mint a tágabb értelemben vett elektronikus pénz – fogalmának és altípusainak bemutatásával folytatjuk az elemzést.

III.2. A digitális pénznemek és virtuális pénznemek

Fontos kiemelni, hogy a digitális pénzek tekintetében nem rendelkezünk egységes terminológiával nemzetközi viszonylatban és a hazai források tekintetében. Bár mint láttuk, az előbb említett BIS jelentés mindvégig a „digitális pénznemek" kifejezést használja, ezt fenntartással teszi, és kijelenti, hogy nem kíván állást foglalni arról, hogy tartalmi szempontból mi is tekinthető digitális pénznek és a szóhasználat indoklásaként a következő tényt hozza fel: ezen eszközök kétséget kizáróan digitális formában jelennek meg.

A Nemzetközi Valutaalap[19] (IMF) szintén a „digitális pénznemek" kifejezést használja kiindulási pontként, viszont az általa közzétett anyag[20] olvasásakor érzékelhető ugyanaz az óvatosság, mint az előbb tárgyalt BIS által adott terminológia használatakor. Bár a szóhasználat tekintetében szimmetriát láthatunk, ez nem mondható el tartalmi szempontból, hiszen míg a BIS által adott meghatározásban csak tágabb értelemben jelenik meg a törvényes fizetőeszközben denominált elektronikus pénz az elektronikus pénzek körében, addig az IMF ezeket minden fenntartás nélkül ide sorolja.[21]

Az IMF meghatározása[22] szerint a digitális pénznem egy digitális (elektronikus) formában megjelenő értékkel egyenlő, amely lehet törvényes fizetőeszközben megnevezett, vagy más, eltérő elszámolási egységben denominált – azonban ilyen esetben már virtuális pénznemekről beszélhetünk. A virtuális pénznem lehet konvertibilis és nem

[19] A Nemzetközi Valutaalap 1945-ben jött létre, létrehozója az Egyesült Nemzetek Szervezete (ENSZ), székhelye pedig Washington. Mint a nemzetközi monetáris rendszer központi intézménye, főbb céljai: a nemzetközi pénzügyi együttműködés és az árfolyam stabilitás elősegítése, a gazdasági növekedés fokozása és a magas szintű foglalkoztatás megteremtése, illetve, hogy átmeneti pénzügyi segítséget nyújtson fizetési mérleg problémákkal küzdő tagországainak. https://www.mnb.hu/a-jegybank/informaciok-a-jegybankrol/nemzetkozi-kapcsolatok/anemzetkozi-valutaalap-imf (2022. 05. 01.)

[20] Virtual Currencies and Beyond: Initial Cosniderations. IMF. (2016) 8. o. https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf (2022. 05. 01.)

[21] Vö. IMF (2016), 8. o. és BIS (2015), 6. o.

[22] IMF (2016), 8. o.

konvertibilis. A konvertibilis virtuális pénznem tulajdonsága, hogy ez beváltható valós pénzre, és ezáltal termékekre vagy szolgáltatásokra költhető. Ezzel ellentétben a nem konvertibilis pénznem „*csak a megfelelő virtuális világon belül használható fel*" .[23] Ez utóbbira tökéletes példa az online játékokban megjelenő játékpénzek sokasága.

Az Európai Központi Bank[24] (ECB) és az Európai Bankhatóság[25] (EBA) álláspontja megegyezik az eddig bemutatott meghatározásokkal. Ennek értelmében a virtuális pénznem „*a nem szabályozott, digitális pénz egy fajtája, amelyet a fejlesztői bocsátanak ki és tartanak ellenőrzésük alatt, és egy meghatározott virtuális közösség tagjai használnak és fogadnak el egymás között*",[48] illetve „*valamely digitális formában megjelenő, elektronikus úton továbbított, tárolt és kereskedett értéket jelöl, amelyet nem egy központi bank vagy más hatóság bocsát ki, és amely nem áll feltétlenül közvetlen kapcsolatban a hagyományos fizetőeszközzel sem, egyes természetes vagy jogi személyek ugyanakkor csereeszközként elfogadják*".[26]

Hasonlóképpen – akárcsak a BIS esetében – az ECB egy későbbi elemzésében szintén a terminológia pontosítására törekszik és véleménye szerint szintén a „*virtuális pénznem*" kifejezés a széles körben elterjedt. Ugyanakkor a fogalom gyakori használata ellenére az ECB kihangsúlyozza, hogy ezen eszközöket sem közgazdasági, sem pedig jogi értelmezésben nem tekinti a szó szoros értelmében pénznek.[27] A Romániában hatályos jogszabály szerint az elektronikus pénz meghatározása a következőképpen hangzik: „*elektronikusan, akár mágneses úton tárolt, a kibocsátóval szembeni követelést megteste-*

[23] *Bánfi*, i. m. 6. o.

[24] Az ECB központi bankként működik, azon országok központi bankja, amelyek átvették az eurót. Fő feladata az árstabilitás fenntartása, amelyet az, alacsony, stabil és kiszámítható infláció biztosításával" célozzák megvalósítani. https://www.ecb.europa.eu/ecb/html/index.hu.html (2022. 05. 01.)

[25] „Az Európai Bankhatóság (EBA) egy független uniós hatóság, amely azon munkálkodik, hogy az európai bankszektor egészében biztosítsa a prudenciális szabályozás és felügyelet hatékony és következetes szintjét. Általános célkitűzései a pénzügyi stabilitás fenntartása az EU-ban, valamint a bankszektor integritásának, hatékonyságának és szabályos működésének biztosítása" https://www.eba.europa.eu/languages/home_hu (2022. 05. 01.)

[26] EBA Opinion on 'virtual currencies'. EBA (2014) 11. o. https://www.eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1 (2022. 05. 01.)

[27] ECB (2015), 4. o. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (2022. 05. 01.)

sítő pénzérték, amelyet pénzeszközök átvételekor bocsátanak ki fizetési műveletek teljesítése céljából, és amelyet az elektronikus pénz kibocsátójától eltérő személy fogad el".[28]

III.3. A kriptovaluta fogalma

A *kriptovaluta* egy digitális eszköz, egy kódsor, ami a megbízhatósága miatt fizetőeszközként – decentralizált fizetőeszközként – is használható[29]. Az értéket nem a mögötte lévő fedezet, hanem a közmegállapodás generálja[30]. A *kriptovaluták* alapja a globalizáció és a digitalizáció. Az egyik legnagyobb előnyük – itt az előny gazdasági, technológiai, nem pedig jogi előnyt jelent –, hogy nem kell hozzájuk központi hatalom, tehát állami felügyelet nélkül, bankrendszertől függetlenül működnek. Ennek köszönhetően lehetetlenné válik a manipuláció és az infláció gerjesztése, továbbá a rendszer a *blokkláncnak* (*blockchain*), illetve az *osztott főkönyvi technológiának* (*distributed ledger technology*) köszönhetően rendkívül megbízható[31]. A tranzakciók alacsony ára, valamint a felsorolt előnyök mellett említést kell tennünk a *kriptovaluták* gazdasági és technológiai hátrányáról is. Maga a rendszer fenntartása nagyon költséges, energiaigénye meghaladja egy kisebb ország teljes energiaszükségletét[32]. Ezen túlmenően – bár sokat lehet nyerni ezen eszközök adásvételén – általánosan elmondható, hogy a központi kontroll hiányában nagy árfolyam emelkedések és esések következhetnek be. Úgy vélem, hogy a *kriptovaluták* esetében egyelőre nem kell félni az összeomlástól, a technológia még gyerekcipőben jár, így – tanulva a történelemből – van időnk egy válságot megelőző szabályozás kialakítására.

A jog és a *kriptovaluták* összefüggésében felmerülő fő kérdés az a szabályozáshoz, pontosabban a szabályozás hiányához fűződik[33]. Azt tapasztalhatjuk, hogy a nehézkesen, lassan reagáló kormányzati struktúrák (jogalkotás, kormány) egyelőre tartanak a

[28] 2011. évi 127. törvény 4. cikk (1) bekezdés f) pont.

[29] *Kázsmér* Dániel: A kriptovaluták jogi szabályozása. Jurátus. 2018. május 8. https://juratus.elte.hu/a-kriptovalutak-jogi-szabalyozasa/ (2022. 05. 20.)

[30] *Varsányi* Károly: Mi adja a bitcoin értékét? FintechZone. 2017. december 27. https://fintechzone.hu/mi-adja-a-bitcoin-erteket/ (2022. 05. 20.)

[31] Mi az a bitcoin bányászat? PCGuru. 2017. július 6. https://www.pcguru.hu/hirek/hardver-mi-az-a-bitcoin-banyaszat/41938 (2022. 05. 20.)

[32] Saifedean *Ammous*: The Bitcoin Standard – The Decentralized Alternative to Central Banking. Wiley, New York 2020. 183. o.

[33] A kriptovaluta szabályozás jövője. Jogászvilág. 2017. október 25. https://jogaszvilag.hu/cegvilag/a-kriptovaluta-szabalyozas-jovoje/ (2022. 05. 20.)

jogi eszközökkel történő megragadásától, így szabályozásuk még a fejlettebb országokban is bizonytalan, egyelőre csak sötétben tapogatózásnak minősíthető.

Ha jellemeznünk kellene a digitális pénzek elöljáróját, a *Bitcoint*, az eladhatóság, hitelesség és szuverenitás kifejezések érzékeltethetik talán legjobban igazi értékét[34]. A *Bitcoin* az első valódi megoldásnak látszik a történelem során számtalanszor problémás, a mindennapokban jelen lévő pénz fogalmára.

Elmondhatjuk, hogy a *Bitcoin* az elmúlt másfél évtized alatt gyakorlatilag hiba nélkül működött, és amennyiben ez a jövőben is így marad, kijelenthetjük, hogy a pénz kérdésére olyan választ kaptunk, amely az egyének akaratát tükrözi, immunis az infláció jelenségére, valamint nagyszerűen vesz részt a gazdasági életben: „*tér, idő és arányosítás szempontjából kiválóan eladható*".[35] Meglátásom szerint a pénz revolúcióját tapasztalhatjuk, amelyre a jövőben úgy fogunk visszatekinteni, mint a múltban történt előrelépések egyikére, akár a kagylókat, sót, nemesfémet, különböző váltókat lecserélő készpénz, majd bankszámlapénz megjelenésekor. Jellemző, hogy egy adott kor technológia fejlettsége befolyást gyakorol a monetáris rendszerre[36]. Így hozott létre a kohászat magasabb rendű pénzformákat a kagylóknál, illetve tengeri gyöngyöknél, valamint a rendszeres pénzveretés eszerint fejlesztette tovább a korábban használt, amely a jogászok éberségét és következetességét is megkívánja.

A történelem igazolta, hogy azok a nemzetek, társadalmak, amelyek „kemény" pénzügyi rendszer mellett voksoltak, nagyobb stabilitást és jobb megélhetést értek el. Ilyen volt Caesar Római Birodalma, Konstantin Bizánci Birodalma, vagy a jelenkori Svájc, amely az aranystandard utolsó bástyájaként szerepelt a történelemben[37]. Ezzel ellentétben azok, akik a hiteltelen vagy technológiai szempontból alárendelt pénzformák mellett döntöttek, például a kínaiak az ezüst preferálásakor vagy az afrikai kereskedők az üveggyöngyök használatánál, súlyos árat fizettek döntésükért. A választás lehetősége ezúttal minket illet, és érdemes elgondolkodni, hogy a jövőben egy futurisztikus Római Birodalom, vagy egy sors sújtotta Afrika népéhez szeretnénk tartozni, hiszen a jelenlegi pénzformák tükrében a *Bitcoin* legalább olyan komoly alternatívaként jelenik meg, mint

[34] *Ammous*: i. m. 183. o.
[35] Uo.
[36] Uo. 184. o.
[37] Uo.

az említett példák.

IV. A kriptoérme (*crypto token*) és a White Paper fogalma

Szükséges különbséget tennünk a *kriptovaluta* (*cryptocurrency*), valamint a *kriptoérme* (*crypto token*) fogalma között. Igazából új *kriptovaluta* kibocsátásáról csak nagyon kis százalékban beszélhetünk, hiszen akkor mondhatunk egy *kriptovalutát* újnak, ha eltérő blokklánc technológiára épül. Az esetek többségében nem történik ilyen technológia alapú érdemi fejlesztés, így a legtöbbször új kriptoeszköz létrehozásakor *kriptoérmé*kről beszélhetünk, nem *kriptovalutá*król. Ezek a *kriptoérmék* döntő többségben a következő, alap *kriptovaluták* blokklánc technológiájára épülnek, mint *token*ek: *bitcoin*, *ether*, *ripple*, *litecoin*, *neon*, *cardano*.[38]

Alapvetően négy fajta[39] *kriptoérmét* különíthetünk el, amelyek más-más tulajdonosi jogokat biztosítanak. A legismertebb ezek közül a *fizetési érme* (*payment token*), amely fizetési funkciók ellátására alkalmas. A *használati kriptoérme* (*utility token*) hozzáférést biztosít a blokklánc alapú szolgáltatáshoz, olykor kedvezményeket biztosít. A harmadik és egyben az értékpapírral leginkább párhuzamba állítható *kriptoérme*, a *pénzügyi eszköz típusú* (*asset token*), amely tulajdonosi vagy hitelezői pozíciót jelöl. Ez amennyiben tényleges értékpapírként nyilvános kibocsátásra kerül, részvényesi vagy kötvényes pozícióként is funkcionál. A *pénzügyi eszköz típusú érme* két újabb alegységre osztható, az *előfinanszírozást* és az *elővásárlási jogot* biztosító *kriptoérmékre* (*pre-financing, pre-sale token*). Az előbbi tulajdonosa egy még fejlesztés alatt álló projektben szerez jogokat, ez a technológia fejlesztésének kezdetleges szakaszában elérhető, amikor még a kísérleti stádium sem vette kezdetét. Ezáltal a kibocsátó kötelezi magát, hogy meghatározott időpontban a megegyezett feltételek szerint a hitelező tulajdonába juttatja az adott mennyiségű *kriptoérmét*. Eközben a *pre-sale token* elővásárlási jogot biztosít kibocsátási áron, vagy olykor az alatt, a jövőben eltervezett jegyzéskor.[40] A dolgok

[38] *Bujtár* Zsolt: A kriptovaluta ökoszisztéma szabályozási kihívásai. In: A puro pura defluit aqva. Ünnepi tanulmányok Nochta Tibor professzor 60. születésnapja tiszteletére (szerk. *Benke* József). PTE ÁJK, Pécs 2018. 65. o.

[39] A négyes elhatárolást az ICOrating nevű amszterdami ICO minősítő társaság további kétfajta kriptoérmével bővítette: szavazó, valamint jutalom érme. A szavazó (*vote token*) kriptoérme szavazati jogot biztosít tulajdonosa számára a projekt fejlesztése során, a jutalom érme (*reward token*) elővásárlási jogot vagy egyéb előnyt biztosít a projekt ICO-ja során.

[40] *Bujtár*: i. m. 66. o.

akkor válnak érdekessé, amikor a négy típusú *token* tulajdonságait egyetlen magának tudhatja. A fent bemutatott *kriptoérme* fajták bárhogyan kombinálhatók, így *hibrid kriptoérmék* kibocsátására is van lehetőség. Ennek megfelelően szintén négy, *kriptoérme* kibocsátástípust különböztethetünk meg: fizetési, használati, a vagyoni eszköz és a hibrid érme típusú kibocsátást.[41]

A következő fogalom, amelynek tisztázása kulcsfontosságú, ha a kriptopénzek kibocsátásáról beszélünk, a *White Paper*. Amint már jeleztük, a kriptovaluták tekintetében nem beszélhetünk a szó szoros értelmében kibocsátóról, így a megjelenésre váró technológia érdemi leírása e dokumentum keretében megtekinthető. A *White Paper* elsősorban egy informális eszköz, amely marketingcélokat betöltő dokumentumok összeségét jelenti. A feladata, hogy egy adott technológia, szolgáltatás vagy termék részletes bemutatásával elnyerje a fogyasztó tetszését. Ezen dokumentum használata bevett gyakorlat az üzleti vállalkozások körében, elősegíti ezek együttműködését (*Business-to-business* – B2B) is. A *White Paper* dokumentumokat három típusra oszthatjuk fel: a *háttéranyagot szolgáltató* (*background*), a *felsorolásokat tartalmazó* (*numbered list*), valamint a *problémát feltáró megoldást nyújtó* (*problem solution*) *white paperek*.[42]A *háttéranyagot szolgáltató white paper* a legfontosabb működési jellemzőkre koncentrál, a *felsorolásokat tartalmazó* dokumentum a megfelelő használati utasításokat és ezzel kapcsolatos tippeket tartalmaz és a harmadik, a *problémát feltáró megoldást nyújtó* kategória új megoldással áll elő egy még meg nem oldott probléma tekintetében.[43] Ezek a dokumentumok nem terjedelmesebbek 2500 szónál, és betölthetik a gazdasági és üzleti szervezetek között létező szabályozási, valamint politikai célú érdekek írásba vetett összefoglalását.[44]

Ezen *white paper* típusok bemutatása azért volt szükségszerű, mert a *kriptovaluták* kibocsátói, megfelelő szabályozás hiányában ezt a vállalati, és egyben kommunikációs szokást alkalmazzák. Egyes esetekben ezek a *white paperek* akár szoftverelemeket, programozási tételeket is tartalmaznak. Általában egy probléma megjelölésével kezdő-

[41] Uo.

[42] *Bujtár*: i. m. 69. o.

[43] Adam *Hayes*: Whitepaper. Investopedia. https://www.investopedia.com/terms/w/whitepaper.asp (2022. 04. 23.)

[44] Ilyen például: a Fintech szektor szabályozására vonatkozó nemzetközi összehasonlítás: The Complex Regulatory Landscape for FinTech. Az Uncertain Future for Small and Medium-Sized Enterprise Lending. World Economic Forum. https://www3.weforum.org/docs/WEF_The_Complex_Regulatory_Landscape_for_FinTech_290816.pdf (2022.06.13.)

dik a dokumentum, amelyre a bemutatott projekt igyekszik megoldásként szolgálni. Így az adott piaci szegmens szakemberei átfogó képet kapnak a projekt mibenlétéről, ami a befektetés irányába sodorja őket, vagy éppen ellenkezőleg. Meg kell jegyezni, hogy a *white paperek* tartalma olykor csak megfelelő szaktudással rendelkezők számára értelmezhető.

V. A Bitcoin mint digitális készpénz

A digitális éra szülöttjeként, a *Bitcoin* innovatív megoldás a pénzzel kapcsolatos, előzőekben vázolt problémára. Hogy mennyire jelentős a *digitális készpénz*, akkor érthetjük meg, ha először a múlt fizetési módozatait vizsgáljuk: a készpénzes fizetést, valamint a közvetített fizetést.

A Román Polgári Törvénykönyv (Rptk.) a következő előírásokat tartalmazza a fizetésre vonatkozóan: „*a fizetés pénzösszeg átutalásában vagy adott esetben bármely más, a kötelezettség tárgyát képező szolgáltatás teljesítésében áll*”.[45]A történelemben az államok örökkévaló próbálkozásaként jelenik meg, hogy nemzeti valutájukat, olykor más valutákat, mint *törvényes fizetőeszközt* fogadjanak el jogalkotás révén. Ezek a jogszabályok meghatározzák azon vagyontárgyakat, amelyek átadásával az adósságok, tartozások törleszthetőek. A *törvényes fizetőeszköz* meglétéből a következő jogok és kötelezettségek származnak: az adós kötelezettsége, hogy tartozását az adott fizetőeszközzel teljesítse, valamint a hitelező szintén ezen eszközzel való kifizetésre jogosult.

A magánjogi viszonyokban a felek a diszpozitív jellegű szabályok tekintetében szabadon megválaszthatják szerződéses kapcsolataikon belül a teljesítés feltételeit és vele együtt a pénznemet is.[46] Tehát a *törvényes fizetőeszköz* alkalmazására akkor kerül sor, amennyiben a szerződő felek nem rendelkeztek a törlesztés pénzneméről. Általában a törlesztést ugyanabban a pénznemben kell leróni, amelyben azt meghatározták, különösen igaz ez a rövid határidővel rendelkező teljesítésekre, valamint amelyek nem érintenek külföldi ügyleteket.

Ugyanakkor megfigyelhető, hogy a fizetések számottevő részében sem az adós, sem pedig a hitelező nem köteles készpénzben rendezni a jogügyletet. A *bankszámlap-*

[45] Rptk. 1469. cikk (2) bek.

[46] Magyarországon a Polgári Törvénykönyvről szóló 2013. évi V. törvény 6:59. § Vö. Romániában az Rptk. 1169. cikk.

énz használatának előnyei háttérbe szorították a *készpénz* felhasználását, és amint láthatjuk, a 2013. évi V. törvény (a Polgári Törvénykönyvről – Ptk.) rendelkezése[47] kimondja, hogy azt jogilag is fizetőeszközként kell kezelni. Mivel a *bankszámlapénz* – akárcsak a *készpénz* – pénznek számít, eltérő rendelkezés hiányában, az adós választása, hogy melyik formában tesz eleget a fizetési kötelezettségének. Amennyiben a megállapodás előírta a *készpénzben* való törlesztést, a hitelező visszautasíthatja a fizetést, más esetben kénytelen elfogadni az adós kezdeményezését.

Ahogy azt *Grosschmid* Béni megfogalmazta: a *bankszámlapénz* nem csupán „*az önkéntes készforgalomban tényleg folyó pénz*", hanem egyben „*a hitelezőre rátukmálható fizető eszköz*".[48] Mivel a hitelező nem utasíthatja vissza a *bankszámlapénzzel* történő fizetést – és tudjuk, hogy ez a *törvényes fizetőeszközök* legfontosabb tulajdonságaként szokott megjelenni –, felmerül a kérdés, hogy a bankszámlapénz nem kezelhető-e immár *törvényes fizetőeszközként* is. Az elmondottakhoz még annyit fűznék hozzá, hogy véleményem szerint a *bankszámlapénz törvényes fizetőeszközként* való elfogadásának kérdése mellett érdemes a kérdéskört immár a *digitális pénzekre* is kiterjeszteni, hiszen a valóság azt mutatja, hogy egyre szélesebb körben pénzként, olykor különleges példaként (El Salvador), akár nemzeti pénzként jelenik meg. Tehát a *készpénzzel* való fizetés, akárcsak a közvetett módon történő fizetés, törvényes eszközként szolgál a tartozások kielégítéséhez. A *készpénzzel* történő fizetés személyesen, az adós és a hitelező között jön létre, azonnali és végleges jogügyletként szolgál, amely materiális formában megjelenő jószág feletti tulajdonos személyének leváltását jelenti. Az ilyen fizetések hátránya a fizikai jelenlét követelménye, amely igencsak hátrányos napjaink szerteágazó, olykor határokon átnyúló kereskedelmi világában.

A közvetített fizetésnél a két jogügyletben szereplő fél mellett megjelenik egy harmadik, végrehajtási feladatokat ellátó, megbízható fél. Ide sorolhatók a csekkel, bank- és hitelkártyával, átutalással, PayPal-lal stb. történő fizetések. A harmadik személy felel a pénzügyi tranzakció sikerességéért, így a személyes jelenlét szükségtelenné válik, ami egyben a pénz fizikai valóságban történő mozgatását is megkerüli. Hátrányként például a harmadik fél sebezhetősége, tranzakciós költségek, időbeli eltolódás jelenik meg. Amint láthatjuk, mindkét módozat rendelkezik előnyökkel és hátrányokkal, ezért a piaci

[47] Ptk. 6:42. §

[48] *Grosschmid* Béni: Fejezetek kötelmi jogunk köréből. Grill, Budapest 1933. 499. o.

szereplők általában kombinálva használják őket. Az elektronikus pénzügyi műveleteket a közvetett fizetési rendszer kizárólagos feladatkörként kezelte mindaddig, amíg a *Bitcoin* meg nem jelent. Ami megkülönbözteti a *Bitcoint* más *digitális tárgyaktól*, az az, hogy rendszerint a digitális világban létező tárgyak természetüktől fakadóan nem korlátozott mennyiségűek. A végtelen számra lehetőséget adó generálás volt az ok, amiért lehetetlen volt új pénznemet létrehozni a digitális térben.

Ugyanakkor minden elektronikus fizetési művelethez egy közvetítő félre volt szükség, aki a dupla költést kiküszöböli. Ezek alól az első kivételt a *Bitcoin* képezte, amely lehetővé tette a *digitális fizetést* közvetítő nélkül, valamint az első olyan *digitális tárgyként* jelenik meg, amely korlátozott számú. Ezen tulajdonságainak köszönhetően kijelenthetjük, hogy a *Bitcoin* nem más, mint az első példája a *digitális pénznek*. A harmadik fél segítségével történő üzletelésnél maradva érdemes ennek hátrányait is kiemelni. Először is, egy ilyen személy biztonsági kockázatként jelenik meg.[49] Ennek oka, hogy az esetleges tolvajok (hackerek) új támadási felületet kapnak, ezáltal a rendszer számos informatikai bűncselekménynek[50] van kitéve, de ezenkívül a műszaki jellegű problémák száma is hatványozódik.

Továbbá, a politikai befolyás is színteret kap, a számlák lekövetése vagy megfigyelése lehetségessé válik az eljárási normák betartásával, a különleges felügyeleti vagy vizsgálati módszerek segítségével.[51] Amíg nem volt lehetőség a harmadik fél megkerülésére, a kormányzati szervek befolyást gyakorolhattak bármikor, bármely művelet tekintetében, az állami biztonság vagy az ellene elkövetett terrorizmus, illetve pénzmosás veszélyének lehetőségére hivatkozva. Ezek mellett, a közvetített fizetés velejárója a csalás problémája, amely a tranzakciós költségek növekedésével jár a kívánt biztonság megteremtése céljából, ez pedig késlelteti az elszámolás menetrendjét.

Gyakorlatilag a megbízható fél „*elveszi a nagy részét a tulajdonosi jognak*” ,[52] amivel a saját pénzünk felett rendelkezhetnénk, ezáltal a likviditás jórészt sérül. Ez a tény a pénz egyik alapvető tulajdonságát sérti, miszerint annak helyettesíthetőnek és likvidnek

[49] Nick *Szabo*: Trusted Third Parties Are Security Holes. Nakamotoinstitute. 2011. https://nakamotoinstitute.org/trusted-third-parties/ (2022. 04. 14.)

[50] Román Büntető Törvénykönyv. 249–252. cikk

[51] Román Büntetőeljárási Törvénykönyv: 152–153. cikk

[52] *Ammous*: i. m. 186. o.

kell lennie. A helyettesíthetőség azt jelenti, hogy minden pénzegység azonos értékkel rendelkezik más egységekkel, a likviditás pedig a gyors eladhatóság tulajdonságát jelöli. A pénz feletti szuverenitás érdekében ezen két tulajdonságnak egyidejűleg teljesülnie kell.

A készpénz esetében, bár az eddig említett hátrányok nem jelennek meg, számos egyéb problémába ütközhetünk. Ezek az ügyletek elveszítették praktikus mivoltukat, mivel a modern kereskedelem nagy távolságok átszelésére alkalmas megoldásra vágyik. Hiába, hogy az elektronikus bankolás az egyének jogainak súlyos korlátozásához vezet, nem igazán van más választásuk a piaci szereplőknek, mint elfogadni a rendszer működésének szabályait. Rontott a helyzeten az arany elhagyása után, amikor az állam – tovább csökkentve az emberek önrendelkezési jogosultságait – a *fiatpénzekre* való átállás mellett voksolt, amelyek mennyisége teljes mértékben a jegybankokra van bízva. Ezáltal, lassan, de biztosan szemtanúi lehetünk a vagyon inflációjának.

Satoshi Nakamoto[53] alkotása nem más, mint egy teljes mértékben *peer-to-peer* alapon működő *elektronikus pénz*, amelyhez nem szükséges harmadik személy bevonása az ügylet lebonyolítása kedvéért, egy olyan pénz, amelynek mennyiségi változása nincs kitéve semmilyen önkényes akaratnak[54]. A *peer-to-peer* nem más, mint egy olyan hálózati struktúra, amely felhasználóinak egyenjogokat biztosít, és ugyanolyan kötelezettségeket szab[55]. Ezeket a szabályokat senki sem tudja megváltoztatni, és nem létezik központi koordinátor. A *node*-ok[56] működtetői nem tudják egyoldalú akaratukat érvényesíteni és más tagokat ezek elfogadására kényszeríteni, ezek privilégiumai sérthetetlenek maradnak[57]. Ilyen ismert hálózat a BitTorrent, ami lényegében egy fájlmegosztó proto-

[53] Adam *Hayes*: Who is Satoshi Nakamoto? Investopedia. 2022. május 17. https://www.investopedia.com/terms/s/satoshi-nakamoto.asp (2022. 05. 20.)

[54] *Ammous*: i. m. 187. o.

[55] Mi az a P2P azaz a peer-to-peer technológia? CoinMixed. 2019. január 8. https://coinmixed.eu/mi-az-a-p2p-a-peer-to-peer-technologia/ (2022. 05. 20.)

[56] „*Node*-nak (*csomópont*) a kriptovilágban azokat az eszközöket hívjuk, amelyek lényegében lehetővé teszik a *blokklánc hálózat* működését. Bármilyen aktív elektronikus eszköz lehet *node*, beleértve a számítógépeket, a telefonokat vagy akár a nyomtatókat, amennyiben azok internethez csatlakoznak, ezáltal rendelkeznek IP-címmel. A *node* szerepe, hogy támogassa a hálózatot azáltal, hogy tárolja a *blokklánc* másolatát és néhány esetben tranzakciókat dolgoz fel. Minden *kriptopénznek* saját *node*-jai vannak." Forrás: Mi az a node? CoinCash. https://hu.coincash.eu/kripto-szotar/n/node (2022.06.13.)

[57] *Ammous*: i. m. 208. o.

koll. A különbség, hogy a központosított rendszerekben az adatok egy közös, központi szerver segítségével elérhetők, miközben a BitTorrent felhasználói közvetlenül jutnak hozzá egymás fájljaihoz. Miután valaki egy teljes fájl letöltője lesz, annak megosztójává válik. Ez számos problémára megoldás, hiszen egy ilyen rendszer hatalmas adatmennyiség megosztására alkalmas anélkül, hogy különösebb infrastrukturális befektetésre legyen szükség, és a ,,sebezhető pont", vagyis a harmadik személy problémája is feledésbe merül. Az összes fájl, amely a hálózat részét képezi, *kriptográfiai hasheléssel*[58] védett, amely által ellenőrizhető, hogy a terjesztő módosította azokat vagy sem.

A *Bitcoin* rendszere hasonló a BitTorrentével[59], csak míg az utóbbinál felhasználói filmeket, dalokat vagy könyveket osztanak meg, addig a *Bitcoin* használói a *megosztott főkönyvön* osztoznak, amely tartalmazza a valaha végrehajtott összes tranzakciót. Tehát a *Bitcoin* azonos jellemzőkkel bír, mint a *készpénz*[60] (közvetítőnélküliség, végérvényes ügylet) és ugyanakkor senki által nem manipulálható mennyiséggel rendelkezik, így ellenáll az infláció jelenségének. Mindez megvalósítása technológiai eszközök révén elérhető, mint például a már bemutatott *peer-to-peer* hálózat, *hashelés*, digitális aláírások és *proof-of-work*[61] (PoW).

A harmadik fél hiánya eddig bizalomhiányhoz vezetett, hiszen senki nem töltötte be a közvetítő szerepet. Nakamoto innovációja ezt úgy oldja meg, hogy a *Bitcoin* központi elveként az ellenőrizhetőséget jeleníti meg[62], amely a bizalom meglétét teljesen irrelevánssá teszi. Ez úgy történik, hogy minden tranzakció a *főkönyvbe* kerül. Bármely ügylet végrehajtásakor, a hálózat akármelyik tagja ellenőrző szerepbe bújhat, és meg-

[58] Egy olyan folyamatot jelent, amely visszafordíthatatlanul egy tetszőleges adatfolyamot képes megadott méretre tömöríteni (ez az egység a *hash*) és adatbázisba rögzíteni. A *hash* kulcsszerepet játszik a *Bitcoin* működésében, ez szükséges az elektronikis aláírásokhoz, a *proof-of-workhoz*, a tranzakcióazonosításokhoz, *Bitcoin* címekhez stb. Gyakorlatilag egy adatrészlet azonosítását teszi lehetővé, a teljes adat felfedése nélkül.

[59] What are the similarities that Bitcoin and Torrent Share? Quora. https://www.quora.com/What-are-the-similarities-that-Bitcoin-and-Torrent-share (2022. 05. 20.)

[60] *Ammous*: i. m. 187. o.

[61] „A *proof of work* egy folyamat, amely során a bányászok (ők azok, akik a bonyolult *kriptográfiai feladatokat* megoldják, ezáltal validálják a tranzakciókat és új *blokkokat* hoznak létre a blokkláncon) jutalmat kapnak az algoritmustól. Az algoritmus szerint, csak azok tudnak új *blokkot* létrehozni, akik elegendő számítási kapacitással rendelkeznek. Példa *kriptovalutákra*, amelyek ezt a protokollt használják: *Bitcoin*, *Ethereum*, *Litecoin*, *Monero stb.* Forrás: *German* Péter: Mi is az a proof of stake és a proof of work? CryptoFalka. https://cryptofalka.hu/proof-of-work-proof-of-stake/ (2022.06.13.)

[62] *Ammous*: i. m. 187. o.

vizsgálhatja, hogy a küldő valójában rendelkezett e megfelelő egyenleggel a tranzakció lebonyolításához. Eközben a *node*-ok (*hálózati csomópontok*) versenyeznek, hogy minél hamarabb a műveletből származó új *blokkokat* frissíteni tudják.[63] Egy ilyen *blokk* létrehozásáért a *node* számítási teljesítményét matematikai műveletekre fordítja, amelyek végeredménye bárki által ellenőrizhetővé válik. Ez a PoW rendszer, amelyben a *blokk* megalkotása csak az összes hálózati tag engedélyével és a helyes megfejtéssel lehetséges.[64] Amennyiben egy *node* helyes megoldással áll elő, ez láthatóvá válik, és a többiek szavaznak az érvényességéről.[65] Ezután a *blokk* elfogadása azonnal egy újabb *blokk* létrejöttét jelenti, amely *láncolatként* kapcsolódik az előzőhöz (ezért megváltozhatatlan), amelyben az új tranzakciók lesznek tárolva a következő PoW folyamat végbemeneteléig. Az ilyen érvényes *blokk* jutalommal jár, ezt nevezzük *block reward*-nak, ami nem más, mint a hálózatba kerülő új *Bitcoin*, valamint tranzakciós költségek összessége. Ezeket a tranzakciós költségeket minden esetben a küldő fél fizeti[66]. A Román Polgári Törvénykönyv ezzel ellentétben más, bár akaratpótló jellegű szabályozást tartalmaz az ügyletek költségére vonatkozóan: „*ellenkező kikötés hiányában, az ár kifizetésének költségei a vevőt terhelik*".[67] Az előbb bemutatott folyamatot hívják *bányászatnak*, és ennek megfelelően a *node*-okat gyakran *bányászoknak*. A bányászok jussát a *block reward* képezi, amely a PoW során felhasznált költségeiket hivatott fedezni. Míg napjainkban a központi bankok által, az újonnan forgalomba került pénzt hitelezésre és az állam működésére fordítják, a *Bitcoin* rendszere csak azokat jutalmazza, akik a *főkönyv* frissítésében segítenek. A *Bitcoin* azért mutat előnyt a *fiatpénzekkel* szemben, mert amíg utóbbiak bármikor sokszorosíthatók, a *Bitcoin* úgy lett programozva, hogy 10 percenként keletkezhessen új *blokk*, amelyekért a jutalom először 50, majd minden négy év elteltével az előzőnek a fele volt, tehát 25, majd 12.5 és jelenleg 6.25, viszont a folyamat tovább folytatódik.[68]

---

[63] Átlagosan 10 percenként kerül sor erre, a helyes megoldással rendelkező *node* ún. *block reward*-ba részesül. Forrás: Mining and Consensus. O'Reilly. https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch08.html (2022.06.13.)

[64] Andrew *Tar*: Proof of Work Explained. CoinTelegraph. 2018. január 17. https://cointelegraph.com/explained/proof-of-work-explained (2022. 05. 20.)

[65] *Ammous*: i. m. 188. o.

[66] Uo.

[67] Román Polgári Törvénykönyv 1666. cikk (3) bekezdés

[68] Ezt nevezzük angolul *block reward halving*nak, az aktuális adatokat pedig a következő oldalon lehet követni: Bitcoin Block Reward Halving Countdown https://www.bitcoinblockhalf.com/ (2022. 04. 15.)

A közjog és a *kriptopénzek* közötti legjelentősebb ellentétes impulzus a pénzkibocsátással kapcsolatban jelenik meg, hiszen ez mindig az állami szuverenitás meghatározó eleme volt, ám a *kriptovaluták* megjelenésével olyan fizetőeszköz került a piacra, amelynek nincs meghatározott, politikai értelemben legitim kibocsátója.

A bankjegyek kibocsátásának monopóliumát törvény rögzíti és szentesíti, amely az ország *törvényes fizetőeszközét* is meghatározza.[69] A *kriptovaluta mint törvényes fizetőeszköz* vonatkozásában jelenleg egyetlen példát hozhatunk, El Salvador esetét, ahol a kormány a jelenleg ismert *kriptovaluták* közül a *Bitcoin*t ismeri el a klasszikus értelemben vett pénzként.

A fizetés eszköze a múltban elképzelhetetlen volt bankszámlák segítségével, hiszen még nem volt az emberek birtokában a kellő informatikai tudás ilyen műveletek lebonyolításához és egyáltalán rendszerek létrehozásához. Napjainkban ezt már természetes dolognak tartjuk, és a mindennapjaink részét képezik ezek az eszközök. A használat gyakorisága igazolja ezeknek a fizetési rendszereknek a hasznosságát, véleményem szerint egy hasonló fejlődési áttörésnek lehetünk szemtanúi, hiszen a *kriptopénzek* hatékonyabb alternatívával állnak elő, mint eddig akármilyen fizetési rendszer. Az előre programozott rendszer[70]nek köszönhetően a jövendőbeli *Bitcoinok* mennyiségét senki nem tudja befolyásolni[71]. Ezt nevezzük *nehézségi kiegyenlítésnek*[72] (*difficulty adjustment*), aminek hatása, hogy minél több tulajdonos lesz, annál értékesebbé válik a *Bitcoin*, valamint ezáltal a ,,*bányászok*" munkabére is nő. Azt gondolhatnánk, hogy a jövedelmezőbb bányászás velejárójaként történő, több bányász megjelenésének következménye a termelés növekedéséhez, és ezáltal inflációhoz vezetne. Igaz, a több bányász jobb számítási teljesítményt jelent, de ennek ellensúlyaként jelennek meg a bonyolultabb ma-

[69] Románia hivatalos pénzneme a lej: Románia Alkotmánya 137. cikk (2) bekezdés, míg Magyarországon a forint tölti be ezt a funkciót: Magyarország Alaptörvénye K) cikk: „Magyarország hivatalos pénzneme a forint". Mindkét ország meghatározza a törvényes fizetőeszközét, illetve jogszabályban rögzíti a bankjegy és érme kibocsátásra felhatalmazott intézményét. Magyarországon a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 4. § (2) bek., Romániában a 2004. június 28. 312. sz. törvény 2. cikk (2) bekezdés a Román Nemzeti Bank alapokmányáról.

[70] 90% of all Bitcoins Mined. When will All Bitcoin Enter Circulation?. NDTV. 2021. december 21. https://www.ndtv.com/business/bitcoin-mining-news-whats-the-future-of-bitcoin-now-that-90-of-all-bitcoins-have-been-mined-2660878 (2022. 05. 20.)

[71] *Ammous*: i. m. 188. o.

[72] Network Difficulty. Blockchain. https://www.blockchain.com/charts/difficulty (2022. 05. 20.)

tematikai problémák[73], amelyek fenntartva az erőegyenlőség szintjét, ugyancsak átlagosan 10 percet kívánnak az új blokkok létrehozására[74]. Ez a módszer biztosítja, hogy a *Bitcoin* időtálló, inflációra immunis pénzként vegyen részt a gazdasági életben – akárcsak a múltban az arany–, nem pedig egy végtelen sokszorosításra alkalmas, gyenge, hiteltelen pénzként. Az *alapkészlet-töblettermelési*[75] *ráta* ezáltal védett, amely egyik fő előnyeként jelenik meg, a *fiatpénzekkel* szemben[76]. A *Bitcoin* áremelkedése nem vezethet a mutató eltorzulásához, a következmény ez esetben a bányászathoz szükséges energiaköltségében fog megjelenni,[77] aminek következménye a hálózat biztonságának fejlődése. Ahogyan Saifedean *Ammous* fogalmazott: „*a Bitcoin a valaha volt legerősebb pénz, mert értéknövekedése nem eredményez mennyiségi növekedést, kizárólag a rendszert teszi biztonságosabbá és ellenállóbbá a támadásokkal szemben*".[78] Az eddig felsorolt jellemzők különböztetik meg a *Bitcoint* az egyéb pénzként szolgált/szolgáló eszközöktől, mint amilyenek a tengeri kagylók, ezüst, réz, arany, állami valuta és egyebek voltak a történelem során. Ezek esetében az árfolyam növekedése elkerülhetetlenül a termelés mennyiségének növekedését vonta maga után. A többlettermelés nehézségének megléte volt az ok, amiért az arany vált a legtöbb civilizáció fizetőeszközévé. A *Bitcoin* még szigorúbb előállítást alkalmaz, a *nehézségi kiegyenlítés* rendszerének köszönhetően. Így adott esetben az arany reagálása az áremelkedésre szintén többlettermeléshez vezetne, amit a *Bitcoin* esetében lehetetlen lenne megvalósítani. A *Bitcoin* PoW rendszerében fellelhető aránytalanság: a tranzakciók ellenőrizhetőségének költsége és a blokkok megalkotásának ára közötti különbség az ok, ami miatt igazán biztonságosnak mondható a hálózat. Az új *blokkok* mindig több energiába (értsd: áramfogyasztás és számítási kapacitás) kerülnek, a létrejövő műveletek ellenőrizhetősége semmibe sem kerül. Így a hamis ügyletek bevezetésének lehetősége értelmetlen, hiszen a költséges PoW megoldásokat a *node*-ok szinte ingyen utasítanák vissza. Viszont amennyiben valaki mégis próbát tenne

[73] Liam *Kemp*: What are the math problems in bitcoin mining? Coinformant. 2022. június 10. https://coinformant.com.au/what-are-the-math-problems-in-bitcoin-mining (2022. 05. 20.)

[74] *Ammous*: i. m. 189. o.

[75] Indikátor, amely jelzi a forgalomba levő mennyiséget a piacra kerülő új mennyiség függvényében, amely az értékállóság fő mutatójaként is szolgál. Forrás: Árpási Zoltán: PlanB és a legjobb matematikai modell a bitcoin ár becslésére. CryptoFalka. https://cryptofalka.hu/bitcoin-stock-to-flow-planb-s2f/ (2022.06.13.)

[76] *Ammous*: i. m. 189. o.

[77] Hiszen bonyolultabb matematikai megoldások lesznek szükségesek.

[78] *Ammous*: i. m. 189. o.

a rendszer kijátszására, az ilyen a bányász jutalmát szankcióként visszavonja a rendszer.[79] A jutalmak (*coin*ok) – amelyek csupán digitálisan léteznek – nem mások, mint az adatbázis tételei, a jogügyletben résztvevő felek közötti tulajdonosi jog hitelesített módosulásainak összessége. A birtoklás nem név alapú, hanem az *elektromos pénztárcák* címei alapján követhető. Ezzel ellentétben a román szabályozás szerint a birtoklás személyhez kötött, amely különböző jogokat és kötelezettségeket teremt: „*a birtoklás a tulajdonjoggal kapcsolatos előjogok tényleges gyakorlása azáltal, hogy az a személy, aki tulajdonosa a dolognak, tulajdonosként viselkedik*".[80] Az *elektromos pénztárcákat*, amelyek mellesleg nyilvánosak, tulajdonosaik *privát kulcsok*[81] révén őrzik meg. Egy ilyen kulcs megszerzése a fizikai lopás következményeit vonhatja maga után. Ahogy azt a Román Büntető Törvénykönyv tartalmazza: „*az ingóságok más személy birtokából vagy őrizetéből annak beleegyezése nélkül, jogtalan eltulajdonítás céljából történő elvétele hat hónaptól három évig terjedő szabadságvesztéssel vagy pénzbüntetéssel büntetendő*".[82] A joggyakorlat álláspontja szerint a lopás tárgyát képezhetik úgy testetlen, mint fizikai formában megjelenő tárgyak egyaránt.[83]

Ralph *Merkle* találta fel a *Merkle-fa adat struktúra rendszert*,[84] amely adatrendezési feladatot lát el a *Bitcoin* hálózatában is. Ő a következőképpen jellemezte a *Bitcoint*: „A *Bitcoin egy új életforma. Az interneten él és lélegzik. Azért él, mert képes az embereknek fizetni, hogy életben tartsák. Azért él, mert hasznos szolgáltatást végez, amiért az emberek hajlandóak fizetni. Azért él, mert bárki bárhol futtathatja a kódja másolatát. Azért él, mert az összes másolat folyamatosan kommunikál egymással. Azért él, mert bármely szabályszegő másolatot azonnal kiselejtez, gyorsan és mérlegelés nélkül. Azért él, mert radikálisan transzparens: bárki láthatja kódját, és hogy mit csinál. Megváltoztathatatlan. Vitathatat-*

[79] *Ammous*: i. m. 190. o.

[80] Rptk. 916. cikk (1) bek.

[81] A birtoklás privát kulcs nélkül lehetetlen. Ennek őrzése kulcsfontosságú, hiszen ha valaki megszerzi, az hozzájuthat a *Bitcoin*unkhoz, ami olyan, mint a fizikai lopás. Az ilyen kulcsok védelme nem egyszerű, viszont elengedhetetlen a biztonság fenntartása szempontjából. Forrás: Miért fontos a privát kulcs, és mire is való igazából? Kriptoworld. https://www.kriptoworld.hu/miert-fontos-a-privat-kulcs-es-mire-is-valo-igazabol/ (2022.06.13.)

[82] Rbtk. 228. cikk (1) bek.

[83] A Legfőbb Semmitő és Ítélőszék 55/A/2016 határozata.

[84] Mi az a merkle-fa? Coincash. 2019. november 5. https://hu.coincash.eu/kripto-szotar/m/merkle-fa (2022. 05. 11.)

lan. Manipulálhatatlan. Lefizethetetlen. Megállíthatatlan. Megakaszthatatlan."[85]

VI. Következtetések

Amint láthattuk, a *kriptovaluták* megjelenése a jogalkotó számára igencsak bonyolult feladatot állít. Nem egyszerű olyan gyakorlat kialakítása, amely innovációra, a *blokklánc technológiájára* kell épüljön, ugyanakkor elengedhetetlen fontosságú, mivel nagy mértékben befolyásolni fogja a gazdasági élet minden szegmensét. A *kriptopénz* a pénzről alkotott fogalmunkat akarja átírni, egy olyan jelenség megváltoztatására hivatott, amely a mindennapjaink részét képezi, ezért szükségesnek találom a jogalkotó részéről egy megfelelő, átfogó, ugyanakkor a technológia lényegét szem előtt tartó szabályozás kialakítását. Megállapítható, hogy a *kriptopénzek* számos tekintetben szembemennek a bevett gyakorlattal, legyen szó a pénzkibocsátás monopóliumáról, a jog által biztosított kényszerítő erők alkalmazásáról, adózásról és más jogintézményekről. Számos példát hozhatunk, amelyben a k*riptovaluták* tulajdonosai a jog kiskapuin keresztül érinthetetlenné válnak, például az elővásárlási joggal, végrehajtási procedúrákkal, eljárási normákkal vagy anyagi jogi jellegű jogszabályokkal összefüggésben. A *kriptovaluták* kibocsátására a tőkepiac szabálykerete talán megfelelő megoldás lenne, viszont amint láttuk, az államok egyelőre a fogalom körülhatárolásánál tartanak.

A *készpénz és bankszámlapénz* közti magánjogi eltérések véleményem szerint alkalmazandók a *kriptopénzek* – mint teljes mértékben immateriális formában megjelenő, a gazdasági életben megfelelő alternatívaként jelentkező eszköz – tekintetében egyaránt. Mivel mély technológiai tudást igényel ezen pénzeszköz megértése, úgy gondolom, hogy a kriptovilággal kapcsolatosan folyamatos képzésre, informálásra van szükség.

[85] Ralph *Merkle*: DAOs, Democracy and Governance. Cryonics Magazine 2016/4. sz. 28-40. o.

Kovács Bence Zsolt
szakkollégista, Collegium Iuridicum

Nagy Gellért
szakkollégista, Collegium Iuridicum

A félvezetők topográfiájának védelme

I. Bevezető

Jelen dolgozat célja a félvezetők górcső alá vétele jogi szempontból és ezen belül legfőképpen a félvezetők topográfiája nemzetközi jogi védelmének elemzése. Annak érdekében, hogy megértsük a téma fontosságát egy technikai bevezetőben magyarázatra szorul, hogy mi is egy félvezető, ezek az anyagok hogyan működnek és miért alkotják a 21. századi, bináris kor alapját. E rövid bevezetőt követően szólunk a félvezetők topográfiája védelmének a jogi fejlődéstörténetéről, majd ezek után a dolgozat gerincét képező legfőbb, a félvezetők topográfiájának az oltalmát szolgáló, nemzeti és nemzetközi normák ismertetésese, elemzése következik.

A téma relevanciáját az Európai Unióban az is adja, hogy nem titkolt cél az EU azon törekvése, hogy digitalizációban vegye fel a versenyt a világ többi gazdasági nagyhatalmával. Ehhez elengedhetetlen a félvezetők gyártási képessége. Az elérendő célt tükrözi az a friss, 2022. februári, a Bizottság által előterjesztett jogszabályjavaslat, amely a digitális szuverenitás elérése, a félvezetők hiányának megszüntetése és Európa technológiai vezető szerepének megerősítése érdekében került kidolgozásra.[1] Ez az úgy nevezett chipekről szóló európai jogszabály már 2021 szeptemberében beharangozásra került,[2] választ adva a SARS-CoV-2 nevű koronavírus járvány által okozott, a nemzetközi kereskedelmi ellátási láncok akadályoztatásával járó, félvezető hiányra az EU belső, közös piacán. A jogszabály legfőképp a digitális válságkezelésre és a külső függőség megszüntetésére hivatott majd, de emellett a zöld átállás megvalósítását is

[1] A hivatalos sajtóközlemény az alábbi linken érhető el: https://ec.europa.eu/commission/presscorner/detail/hu/ip_22_729 (2022. 04. 09.)

[2] European Chips Act: Communication, Regulation, Joint Undertaking and Recommendation. Európai Bizottság. https://digital-strategy.ec.europa.eu/hu/node/10707 (2022. 04. 09.)

elő kívánja mozdítani.[3] A záró gondolatokban javaslatot fogalmazunk meg, hogy hogyan lehetne ezt a chiphiány által okozott gazdasági problémát a jog – *ergo* új szabályozási rendszer – eszközével megoldani.

A továbbiakban a félvezetők meghatározásáról, fizikai felépítéséről és fontosságáról kívánunk röviden szólni.

II. A félvezetőkről általánosan

Az információ korában élünk. Ennek a bináris világnak az alapjait először az elektroncső (gázzal töltött vagy vákuum cső, egy anóddal, egy katóddal és köztük egy ráccsal) majd a tranzisztor jelentette. Előbbiek rengeteg energiát fogyasztottak és kimondottan gyakran égtek ki.[4] Az elektrotechnikai forradalom lehetővé tette a tranzisztorok gyártásának gépesítését, ezek széles körű elterjedését és ezzel együtt egyre kisméretűebbé válását. A tranzisztorok más anyagokkal szennyezett félvezetőkből készülnek.[5] Talán jól kiemeli ezek fontosságát, hogy csak egy ember kapott valaha kétszer is fizikából Nobel díjat, John Bardeen, mind a két esetben másokkal megosztva, először 1956-ban,[6] másodszorra 1972-ben.[7] Az elsőt a félvezetőkön végzett kísérletek és a „tranzisztor hatás" felfedezésének köszönhetően.

A félvezető anyagok meghatározásánál mellőzve a fizika-tankönyvekben található definíciót, egy félvezető nem más, mint az az anyag, amely bizonyos körülmények között szigetel és bizonyos körülmények között vezeti az áramot. Más szóval, a félvezetők esetén az elektronok képesek energiaszint váltásra, de csak különleges, egyedi körülmények között. Ilyen esetben az anyag vezetővé válik. Ilyen félvezető anyag például a szilícium, amelyet olyan gyakran használtak félvezetőként, hogy a híres, innovációs központként ismert, Kaliforniában található völgyet is erről az anyagról nevezték el.[8]

---

[3] A teljes indoklásért lásd a Bizottság Ajánlását. https://ec.europa.eu/newsroom/dae/redirection/document/83103 (2022. 06. 12.)

[4] *Bozó* Balázs: Az elektroncsövek működése. Elektroncső. http://www.elektroncso.hu/cikkek/csovek.php (2022. 04. 09.)

[5] *Rékai* János: Adalékok a tranzisztor előtörténetéhez. Fizikai szemle 2010/6. sz.

[6] The Nobel Prize in Physics 1956. https://www.nobelprize.org/prizes/physics/1956/summary/ (2022. 04.09.)

[7] The Nobel Prize in Physics 1972. https://www.nobelprize.org/prizes/physics/1972/summary/ (2022. 04. 09.)

[8] Félvezetők. BME. https://web.archive.org/web/20101123000116/http://www.fke.bme.hu/

A félvezetőkből felépített tranzisztorok és az ezek által alkotott logikai kapuk és áramkörök sokasága képezi a mikrochip alapját.[9] Az áramkörök pedig elektromos impulzusokkal dolgoznak. A következőkben a szilícium félvezető képességéről lesz szó.

A szilícium egy félvezető, amely önmagában nem vezeti az áramot, viszont mivel a külső elektron héján 4 elektron található – ez határozza meg az anyag számos kémiai tulajdonságát –, az azon a héjon maximális 8-ból, éppen ezért valószínű, a körülötte levő más 4 szilícium atomokkal kovalens kötések fognak keletkezni, egy kristályrács kialakítása és a külső elektronok megosztása végett. Ha ezt a kristályt foszforatommal (külső elektron héján 5 elektron található) vagy bórral (külső elektron héján 3 elektron található) szennyezzük, akkor egy elektron vagy felszabadul és mozgóképessé válik a kristályszerkezetben (negatív, N-típusú félvezetőt kapunk) vagy növeljük az anyag vezető képességét azzal, hogy növeltük a mobilis elektronok számát (pozitív, P-típusú félvezetőt kapunk). Egy N-típusú és egy P-típusú félvezetőt egymás mellé rakva egy diódát kapunk, amely igen hasznos, hiszen ez a váltó áramot egyen árammá képes alakítani.[10] Ami a dolgozat vizsgálódási tárgyát képezi, az egy egymás melletti N-típusú majd P-típusú és megint egy N-típusú félvezető, amely kiadja a legegyszerűbb és a legtöbbet használt NPN-típusú tranzisztort. A középső P-típusú félvezetőbe, ha pozitív feszültséget vezetünk, akkor az NPN-típusú tranzisztor vezeti az áramot, ezzel kiteljesítve az áramkört. Így ez kvázi egy kapcsolóként működik, pontosan úgy, mint az elektroncső, két eredményt (a bináris korban ez a 1 és a 0) képes kiadni.[11]

Félvezetőket ugyanakkor áram fejlesztésére is fel lehet használni. Többek között egy NP-típusú félvezető a napelem legfontosabb összetevője. Ezzel a fenntarthatóság és a megújuló energiaforrások kiaknázásában is igen fontos szerep jut a félvezetőknek.[12]

---

oktatas/meresek/4.pdf (2022. 04. 09.)

[9] Chris *Woodford*: Transistors. Explainthatstuff. https://www.explainthatstuff.com/howtransistorswork.html (2022. 04. 09.) Közeli felvételekért egy mikrochipről, annak felépítéséért, lásd: https://www.nisenet.org/catalog/media/zoom_microchip_video (2022. 04. 09.)

[10] Félvezetők ...

[11] További információkért lásd: *Woodford*: i. m. vagy Superconductor Information for the Beginner. http://superconductors.org/INdex.htm (2022. 04. 09.)

[12] Az NP-típusú félvezető alapú napelem működéséért lásd: How a Solar Cell Works. ACS. https://www.acs.org/content/acs/en/education/resources/highschool/chemmatters/past-issues/archive-2013-2014/how-a-solar-cell-works.html (2022. 04. 09.) és Semiconductors and Silican Solar Cells. http://butane.chem.uiuc.edu/pshapley/Environmental/L9/2.html (2022. 04. 09.)

Amit a félvezetők topográfiájának védelméről elöljáróban tudni érdemes, az az, hogy „az információs közkincstől elhatároló kétfokozatú küszöbkritériumokat szerzői jogias formában megtaláljuk a topográfiák tekintetében is. Akkor részesülhet oltalomban a mikroelektronikai félvezető termék topográfiája, ha eredeti. A topográfia pedig akkor eredeti, ha saját szellemi alkotómunka eredménye. A topográfia tehát nem lehet az információs közkincs része, nem lehet kivonás, csak saját szellemi alkotómunka révén való hozzáadás. A második küszöbkritérium arra vonatkozik, hogy ez a hozzáadás egy minimális kreativitás révén elegendő mértékben különbözik-e az információs közkincstől, meghaladja-e a konvencionálist, a közhelyet, mivel megalkotása idején nem szokásos az iparban és így az oltalommal együtt járó tilalom nem korlátoz-e másokat érdemtelenül."[13]

III. A félvezetők topográfiája védelmének fejlődéstörténete

Az iparjogvédelem területét szabályozó első nemzetközi egyezmény elfogadására már 1883-ban sor került, az akkor még nóvumnak számító Párizsi Uniós Egyezmény aláírásával.[14] E kezdeti szabályozás ugyanakkor még, érthető módon, nem tartalmazott a félvezetők topográfiájának védelméről szóló rendelkezéseket. Több mint száz év elteltével, 1989 május 26-án, azonban egy washingtoni diplomáciai konferencia keretében, a résztvevő államok képviselői aláírták az integrált áramkörök alapvető jogvédelmi elveit lefektető úgynevezett Washingtoni Szerződést (Integrált Áramkörökre vonatkozó Szellemi Tulajdon Oltalmáról szóló Egyezmény, angol nyelven: *Washington Treaty on Intellectual Property in respect of integrated Circuits*, a továbbiakban: IPIC Egyezmény).[15] E szerződés legjelentősebb előírása, amely folytán ratifikálása komoly akadályokba ütközött, hogy a félvezetők topográfiájának védelmét 8 éves időintervallumban korlátozza, továbbá ezen topográfiák jóhiszemű utánzása esetén nem ad lehetőséget kártérítés követelésére.[16]

A félvezetők topográfiájának védelméről rendelkező, mindmáig legfontosabb nemzetközi egyezmény a Kereskedelmi Világszervezet égisze alatt került elfogadásra.

[13] *Bovroszky* Jenő: Az enyém, a tied és a miénk a szellemi tulajdonban Áttekintés a közkincs és a szellemi magántulajdon egyes összefüggéseiről az Internet tükrében. In: Ünnepi dolgozatok Gyertyánfy Péter tiszteletére. (szerk. *Faludi* Gábor) ELTE ÁJK Polgári Jogi Tanszék, Budapest 2008.

[14] Paris Convention for the protection of industrial property of March 20, 1883.

[15] Treaty on Intellectual Property in Respect of Integrated Circuits Adopted at Washington, on May 26, 1989.

[16] Bujorel *Florea*: Protecția juridică a topografiilor produselor semiconductoare. Revista Română de Drept Privat 2008/4. sz.

A Kereskedelmi Világszervezet (*World Trade Organization*, a továbbiakban: WTO) 1994-ben a Marrakesh-i Egyezménnyel jött létre, amelynek 1. C) számú melléklete a „Megállapodás a szellemi tulajdonjogok kereskedelmi vonatkozásairól" címet viseli. A Megállapodásra a magyar szakirodalomban TRIPS-megállapodásként szoktak hivatkozni, amely elnevezés a melléklet hivatalos, angol megnevezéséből ered: *Agreement on Trade-Related Aspects of Intellectual Property*.[17]

„A TRIPS-megállapodás rendelkezései a szellemi tulajdon kereskedelmi vonatkozású nemzetközi fejlesztésére, a jogérvényesítésre és a vitarendezés szabályozására irányulnak."[18] A TRIPS-megállapodás a szellemi tulajdon kereskedelmi vonzatairól rendelkezik, és annak elfogadása a WTO csatlakozás egyik alapfeltételévé vált.[19] A TRIPS-megállapodás az első olyan nemzetközi kereskedelmi megegyezésnek tekinthető, amely egyszerre határozza meg a többoldalú szellemi tulajdonra vonatkozó szabályokat, és egy olyan minimális nemzeti keretszabályozást teremt, amely szükséges a szellemi tulajdonjog érvényesítéséhez.[20]

E megállapodás 6. Szakasza négy cikkben rendelkezik az integrált áramkörök topográfiájának védelméről (35-38. cikkek), kitérve többek között a védelem céljára, a védelem időtartamára és a megállapodás vizsgált rendelkezéseinek az integrált áramkörök alapvető jogvédelmi elveit lefektető, már említett IPIC Egyezmény előírásaival való kapcsolatára.

Az 1980-as években az akkor közösségi, mai szóhasználattal uniós jogalkotó is felismerte a félvezetők topográfiájának védelmét elengedhetetlenné tevő tényezők meglétét. Ennek eredményeként, 1986. december 16-án a Tanács elfogadta a 87/54/

[17] Az Általános Vám- és Kereskedelmi Egyezmény (GATT) keretében kialakított, a Kereskedelmi Világszervezetet létrehozó Marrakesh-i Egyezmény és mellékleteinek kihirdetéséről szóló 1998. évi IX. törvény (a továbbiakban: WTO megállapodás) 1. C) Melléklet

[18] *Vallasek* Magdolna – *Kokoly* Zsolt – *Kis* Réka: Román szerzői jog. Forum Iuris Könyvkiadó, Budapest – Kolozsvár 2019. 33. o.

[19] Uo.

[20] Semiconductors & the World Trade Organization. How Global Trade Rules Have Spurred Semiconductor Growth & Innovation, Semiconductor Industry Association, 2020. https://www.semiconductors.org/wp-content/uploads/2020/11/The-WTO-and-the-Semiconductor-Industry-Nov-2020_2.pdf?fbclid=IwAR1kzJScun6kYqw_-AXYvd1A4-0zGOguB_TdqJuHY-07qr2D62q-MUl30AAI (2022. 04. 08.) 2. o.

EGK irányelvet a félvezetők topográfiájának oltalmáról[21] (a továbbiakban: Irányelv). Az Irányelv indoklásában a jogalkotó kiemelte, hogy a félvezető termékek számos iparág tekintetében egyre fontosabb szerepet töltenek be, jelentőségük alapvető az akkori európai közösség fejlődése szempontjából. Továbbá, a félvezetők topográfiájának kialakítása, a felhasznált (úgy emberi, mint pénzügyi) erőforrások tekintetében, jelentősebb terhet rónak a fejlesztőre, mint a topográfiák többszörözésének költségei. Ebből az okból kifolyólag, a közösségi jogalkotó úgy ítélte meg, hogy a tagállamok szabályozásai nem biztosítanak megfelelő védelmet a félvezetők topográfiájának kifejlesztését illetően, ezért szükséges egy átfogó, közösségi szintű szabályozás.[22]

Magyarországon, az iparjogvédelem terén az 1992-ben bevezetésre kerülő szabályozás, amely a mikroelektronikai félvezető termékek topográfiája oltalmáról szóló 1991. évi XXXIX. törvénynek köszönhetően valósult meg, első volt a félvezetők topográfiája oltalmáról szóló jogszabályok sorában. E törvény szinergikusan, „modern jogalkotásként feldolgozza az ún. Washingtoni Egyezmény és az Európai Közösség félvezető termékek topográfiájáról szóló irányelvének rendelkezéseit, ill. direktívájának szabályait."[23]

Végül, de nem utolsó sorban, a félvezetők topográfiájának védelme tekintetében érdemes kiemelni, hogy az egyes államok az elmúlt évtizedek során jelentős számú jogszabályt fogadtak el e tárgykörben. Románia esetében például, már az 1995. évi 16-os számú integrált áramkörök topográfiájának védelméről szóló törvény lefektette a szabályozás keretét, amelyet ugyanakkor csak a 2005. évi 337. számú módosító törvény hozott összhangba a már említett, félvezetők topográfiájának oltalmáról szóló 87/54/EGK irányelvvel.[24]

IV. A félvezetők topográfiájának védelme nemzeti és nemzetközi normákon keresztül

A továbbiakban a nemzetközi iparjogvédelmi szabályok közül a Kereskedelmi Világszer-

[21] A Tanács Irányelve (1986. december 16.) a félvezető termékek topográfiájának oltalmáról. 87/54/EGK. (a továbbiakban 87/54/EGK irányelv)

[22] A közösségi jogalkotó indoklását azzal zárja, hogy az Irányelvben megfogalmazottak tagállami alkalmazása iránt „sürgős szükség mutatkozik", ezzel is hangsúlyozva a szabályozás iránt megnövekedett igényt. Ld. Irányelv.

[23] *Tattay* Levente: A szellemi alkotások teljes körű újraszabályozása Magyarországon. Iustum Aequum Salutare 2009/2. sz. 152. o.

[24] *Bujorel: i. m.*

vezet égisze alatt elfogadott TRIPS-megállapodás és az Európai Unión belül hatályos a Tanács 87/54/EGK irányelvének tükrében kerül vizsgálatra a félvezetők topográfiája. Az Amerikai Egyesült Államok félvezetők elhelyezését védő jogszabályt ismertetjük a nemzeti jogszabályok közül, mivel ennek a befolyása a legnagyobb a nemzeti szabályozások közül világszerte.

IV.1. A félvezetők topográfiájának védelme a TRIPS-megállapodás tükrében

Ahogyan azt már az előzőekben vázoltuk, a Kereskedelmi Világszervezet TRIPS-megállapodása, a II. rész 6. fejezetében, négy cikket szentel a vizsgált témakörnek. E 6. fejezet a félvezető áramkörök térbeli elrendezése (topográfiája) címet viseli.[25]

A megállapodás 35. cikke rendelkezik a TRIPS-megállapodás előírásainak IPIC Egyezménnyel való kapcsolatáról. E cikk rendelkezéseinek értelmében a tagok egyetértenek abban, hogy az integrált áramkörök topográfiáját oltalomban kell részesíteni. Mindezen védelmet oly módon kell megteremteni, hogy az összhangban legyen az IPIC Egyezmény 2-7. cikkével (kivéve a 6. cikk 3. bekezdését), 12. cikkével, illetve a 16. cikk 3. bekezdésével.

A 36. cikk a védelem hatályát adja meg, kiemelve, hogy azt a 37. cikk 1. bekezdése rendelkezéseinek fenntartásával kell értelmezni. A 36. cikk előírásainak fényében, a tagok jogellenesnek tekintik a jogosult engedélye nélküli mindazon cselekményeket, amelyek egy oltalmazott topográfia, az oltalmazott topográfiát megtestesítő félvezető áramkör, vagy e félvezető áramkört megtestesítő, a topográfiát továbbra is tartalmazó termékek importálására, forgalmazására vagy egyéb kereskedelmi célú terjesztésére irányulnak. Észrevehető, hogy a vizsgált rendelkezések hatálya kellően részletes és tág, ily módon lefedi a félvezetők topográfiájának védelme kapcsán felmerülő jogsérelmek körét.

A megállapodás 37. cikke ugyanakkor taxatíve felsorolja mindazon eseteket, amelyek a jogosult engedélyéhez nem kötött cselekményeknek minősülnek, ily módon pedig a tagok nem tekintik jogszerűtlen cselekedeteknek. Nem tekinthető jogszerűtlen magatartásnak tehát, a jogosulatlanul sokszorosított topográfiát megtestesítő félvezető áramkör vagy egy ilyen félvezető áramkört tartalmazó bármely termék importálása,

[25] WTO megállapodás II. rész 6. fejezet

forgalmazása vagy terjesztése abban az esetben, ha az adott cselekményt végrehajtó (vagy megrendelő) személy nem tudta vagy nem kellett tudnia, a félvezető áramkör beszerzésének pillanatában, hogy az jogtalanul sokszorosított topográfiát tartalmaz. Továbbá, a 31. cikk a)-k) pontjaival összhangban, és az abba foglaltak betartása mellett, nem tekinthető jogszerűtlen cselekedetnek a kormány által vagy a kormány által feljogosított harmadik fél által történő hasznosítás sem.

Az oltalmi időre vonatkozó előírások keretét a TRIPS-megállapodás 38. cikke adja meg. E rendelkezés alapján két eltérő esetet különíthetünk el:

Azokban tagállamokban, ahol az oltalom feltételei között a lajstromozás is szerepel, az oltalmi idő a lajstromozás iránti bejelentés benyújtásának napjától vagy a világon bárhol történő első kereskedelmi hasznosítástól számított 10 évig tart;

Azokban a tagállamokban azonban, ahol a lajstromozás nem egyike az oltalom feltételeinek, a félvezetők elhelyezkedésének oltalmát a világon bárhol történő első kereskedelmi hasznosítástól számított legalább 10 évig kell biztosítani.

E két helyzet mellett, a 38. cikk 3. bekezdése kiemeli, hogy a tagállamok minden esetben rendelkezhetnek oly módon, hogy az oltalom a topográfia létrehozásától számított 15 év elteltével megszűnjön.

Figyelembe véve a félvezetők kiemelt piaci szerepét, az elmúlt években érzékelhető problémákat és negatív tendenciákat, valamint a félvezetők felhasználási területein tapasztalható gyors innovációkat és fejlesztéseket a TRIPS-megállapodás által előírt 10 évesoltalmi idő arányosnak tekinthető a védeni kívánt szellemi tulajdonjoggal.

Ugyan, a TRIPS-megállapodás már több mint 25 éves múltra tekint vissza, mégis oly pontos keretet ad a félvezetők topográfiája nemzetközi védelmének, amely mindmáig megkerülhetetlen a vizsgált tárgykörben felmerülő kérdések megválaszolásakor.

IV.2. A félvezető termékek topográfiájának oltalma a Tanács 87/54/EGK irányelvében

Az akkori közösségi jogalkotó, felismerve a gazdasági fejlődés irányát, annak gyorsaságát, viszonylag korán, 1986. december 16-án elfogadta a félvezető termékek topográfiájának oltalmáról rendelkező Irányelvét. A Tanács nem titkolt céljai között szerepelt, ahogyan azt az Irányelv preambulumában is hangsúlyozza, hogy a számos iparágban kiemelt szerepet betöltő félvezetők topográfiájának védelmét olyan magas szintre emelje,

amely elősegíti az Európai Közösség ipari fejlődését.

Az Irányelv fogalommeghatározása szerint félvezető terméknek tekintendő, és ezáltal oltalomban részesül, minden olyan termék, amely „félvezető anyagréteget tartalmazó anyagból áll; és egy vagy több vezető, szigetelő vagy félvezető anyagból álló, előre meghatározott térbeli mintával összhangban elrendezett rétegekkel rendelkezik; és kizárólag vagy más funkciókkal együtt elektronikus funkciók végrehajtására szolgál".[26] Szintén az Irányelv értelmezésében félvezető termék topográfiájának számít minden olyan, összefüggő képek bármely módon rögzített vagy kódolt sorozata, amely e félvezetők rétegeinek térbeli elrendezését, felületének mintáját vagy a minta egy részét ábrázolja.[27]

Az Irányelv 2. cikke értelmében a tagállamoknak oltalmazniuk kell a félvezető termékek topográfiáját minden olyan esetben, ha az eleget tesz a megadott feltételeknek, amelyek alapján az adott topográfia megalkotója saját szellemi alkotómunkájának tudható be és nem szokásos a félvezető iparban.

Az Irányelv rendelkezéseinek alapján, főszabály szerint a félvezető termékek topográfiájának oltalma az adott topográfia szerzőjét illeti meg. E szabály alól ugyanakkor, számos kivételt is felsorol a vizsgált Irányelv. Ily módon, a 3. cikk (2) bekezdése tükrében például abban az esetben, ha a szerző a topográfiát munkaviszony keretében alkotta meg, az oltalom a munkáltatót illeti meg és mindazon esetekben, amikor egyéb szerződéses jogviszony keretében került megalkotásra a topográfia, az oltalom a megbízót illeti meg.

Minden esetben, a 3. cikk (3) bekezdése szerint az oltalomra azon személyek jogosultak, akik a tagállamok valamelyikének állampolgárai, vagy akiknek szokásos tartózkodási helye a tagállamok valamelyikében van (illetve gazdasági társaságok vagy más jogi személyek esetében jogosult oltalomra a társaság, ha telephelye valamely tagállamban található). Ugyanakkor, ha a rendelkezések szerinti más oltalom nem áll fenn, a vizsgált cikk (4) bekezdése értelmében, az oltalom megillet minden olyan személyt, aki a topográfiát először az Unió valamely tagállamában hasznosítja, vagy e hasznosításra a topográfia jogosultjától engedélyt kapott.

[26] 87/54/EGK irányelv, 1. Fejezet, 1. cikk (1) bekezdés a) pont
[27] 87/54/EGK irányelv, 1. Fejezet, 1. cikk (1) bekezdés b) pont

Az Irányelv által biztosított oltalom tartalmáról az 5. cikk rendelkezik, amely előírja, hogy az oltalom alapján engedélyezhető, vagy adott esetben megtiltható a védett topográfia többszörözése, a topográfiáknak, illetve az azok alapján gyártott félvezető termékeknek a kereskedelmi célú hasznosítása vagy behozatala. Ugyanakkor, az oltalom nem terjed ki a topográfiák elemzésére, értékelésére, oktatási célt szolgáló többszörözésére, illetve ezirányú tagállami szabályozás esetén a magáncélú többszörözésre sem.

A TRIPS-megállapodáshoz hasonlóan az Irányelv is különbséget tesz az oltalom kezdetét tekintve, a lajstromozással, illetve az anélkül keletkező oltalmak között. Az Irányelv 7. cikke alapján, abban az esetben, ha az oltalom lajstromozással keletkezik, a védelem kezdetének időpontja lehet a lajstromozás iránti kérelem szabályszerű benyújtásának napja vagy az adott topográfia első kereskedelmi célú hasznosításának napja. Ellenkező esetben, az oltalom kezdetének a topográfia bármely országban történő első kereskedelmi célú használatának napját, vagy a topográfia első rögzítésének és kódolásának napját tekintjük.

Az Irányelv, szintén a TRIPS-megállapodáshoz hasonlóan, az oltalmi időt az első kereskedelmi célú hasznosítás naptári évének végétől számított tíz évben korlátozza. Továbbá, előírja, hogy minden olyan esetben, amikor az első rögzítés vagy kódolás napjától számított 15 éven belül nem került sor a topográfia kereskedelmi célú hasznosítására a keletkezett oltalom megszűnik.[28]

IV.3. A félvezető termékek topográfiájának oltalma az Amerikai Egyesült Államok *Semiconductor Chip Protection Actjének* értelmében

Az Amerikai Egyesült Államokban valósult meg elsőnek az integrált áramkörök, és ezzel a félvezető termékek topográfiájának a védelme a *Semiconductor Chip Protection* Act révén 1984-ben.[29] Ezt megelőzően nem feltétlenül volt törvénytelen azonos topográfiájú, konkurens chipet előállítani. Ez az amerikai chipgyártók (legfőképpen az Intel) részéről megfogalmazott panaszhoz vezetett, amelynek köszönhetően elfogadták a *chip piracy* elleni jogszabályt. Ennek a jogalkotói aktusnak betudhatóan indult el világszerte az a folyamat, amely keretében hasonló, a félvezető termékek topográfiájának a védelme iránti nemzeti és nemzetközi jogszabályokat fogadtak el(Japán volt az első aki követte a példát,

[28] 87/54/EGK irányelv, 2. Fejezet, 7. cikk (3) és (4) bekezdés

[29] Semiconductors ...

majd az előbbiekben már tárgyalt uniós szabályozása következett).

A maga nemében a jogszabály *sui generis* jelleggel bír, mivel sem a *copyright* (szerzői jogi), sem a *patent* (szabadalmi)[30] törvény rendelkezései nem vonatkoznak rá, hiszen a félvezetők topográfiái nem lettek volna védhetőek a szerzői jog körében. Az integrált áramköröknek egy speciális, egyéni szabályozást hozott létre a törvény, amely ötvözi az előbb említett két jogszabály rendelkezéseit.[31] Ehhez hozzá kell tenni azt, hogy az USA jogrendszere *common law* rendszer lévén, a *Semiconductor Chip Protection* Act alapján lefektetett esetjog nagyban meghatározza a jogszabály alkalmazásának számos aspektusát.[32]

„Az oltalom tárgya az amerikai szokás szerint nagyon konkrétan van meghatározva: a maszkmű (*maskworks*) azaz az integrált áramkörök (*integratedcircuits*) elrendezési mintájának a *mikrochip*-be való átvitelére szolgáló eszköz."[33] Ezt eklatánsan bizonyítja, hogy már az első cikkelye a törvénynek meghatározza ezeket a fogalmakat.[34] A maszkmű fogalma mára kiüresedett, de a jogszabály a mai napig tartalmazza.[35]Ezzel ellentétben az EU-ban az oltalom tárgya maga a topográfia, mint az előző részből kiderült.

A védelem a bejegyzéstől számított 10 évig áll fenn, amely „kezdődhet az első forgalomba hozatal, a bejelentés vagy a topográfia első rögzítésének vagy kódolásának napja közül a korábbival."[36] Ez egy olyan megoldás, amely a közérdeket is figyelem előtt tartotta (hogy később közkincsként majd bárki szabadon fel tudja használni a topográfiai újításokat), ugyanakkor ezt az időintervallumot elegendőnek tartotta a jogalkotó arra, hogy közben innováció menjen végbe az iparágban. E megoldás talán még a kutatást is serkenti. Ugyanakkor a 10 év mai léptékkel nézve már túl hosszú időtartam, a technológiai újítások sokkal gyorsabban követik egymást ebben a gazdasági szektorban, ezért

[30] A szellemi tulajdonjog védelmében ezt hibrid paradigmának nevezi Bovroszky Jenő. A funkcionális irányultságú topográfiákat ebbe a kategóriába sorolja. Részletekért lásd: *Bovroszky*: i. m. 15. o.

[31] Uo. 46–47. o.

[32] Uo.

[33] Uo.

[34] 17 U.S. Code § 901 - Definitions (a) (1)

[35] Thomas *Hoeren* – Francesca *Guadagno* – Sacha *Wunsch-Vincent*: Breakthrough Technologies – Semiconductors, Innovation and Intellectual Property. WIPO Economic Research Working Paper 2015/27 sz. 28. o.

[36] *Bovroszky*: i. m. 55. o.

kijelenthető, hogy a szabályozás jelentősen előnyben részesíti az időintervallum szempontjából az újítót.

Érdekességnek számít továbbá, hogy „az oltalom nem terjed ki a topográfia alapját és egyben közkincset képező elvre, eljárásra és rendszerre, sem a félvezető termékben tárolt információra. Ennek következményeként, a szoftverekre vonatkozó szerzői joghoz hasonlóan megengedett a független kifejlesztés (*independent creation*) és – meghatározott korlátokkal – a mérnöki visszafejtés (*reverse engineering*)."[37]Az illegális másolás (maszkmű megsértése) szokásos tesztje a szerzői jogi törvény *substantial similarity* (lényegi hasonlóság) tesztje. Megjegyzendő ugyanakkor, hogy bár ez egyértelműen szerepel az amerikai jogszabályban, a topográfiajog általános elve alapján lehetőség van a mérnöki visszafejtésre bármilyen szankció nélkül.[38]

V. Záró gondolatok

Megismételve a dolgozat alaptézisét, a félvezetők áramkörökben való hasznosítása tette lehetővé azt a technológiai forradalmat, amelynek köszönhetjük az internetet, számítógépeket, mobiltelefont és sok más elektronikus eszközt. A 21. század emberének éppen ezért a félvezetők léte vagy nem léte meghatározza a mindennapjait, kapcsolattartás egyszerűsítését említve csak a sok végbe ment változásból. A dolgozatban láttatni próbáltuk, hogy ennek a kimondott jelentőségű területnek hogyan történik a védelme világszerte, milyen fontos nemzeti és nemzetközi normák szabályozzák a félvezetők topográfiájának védelmét.

A SARS-CoV-2 járvány által okozott globális chiphiány megmutatta mennyire vannak összekötve a világ országai kereskedelmük által, mennyire függnek egymástól a technológiai ipar nagyjai. Ezt a válságot csak erősíti az a tény, hogy a chiptermelés 75 százaléka Kelet-Ázsiában folyik és a legfejlettebb chipek 90 százaléka Tajvanon készül[39] (a *Taiwan Semiconductor Manufacturing Company* valamivel több mint 52 százalékos piaci részesedést ért el a félvezető gyártás földkörüli piacán).[40] Ezért fontos olyan techno-

[37] Uo. 47. o.

[38] Uo.

[39] Julian E. *Barnes*: How the Computer Chip Shortage Could Incite a U.S. Conflict With China. New York Times. 2022. január 26. https://www.nytimes.com/2022/01/26/us/politics/computer-chip-shortage-taiwan.html (2022. 04. 08.)

[40] Leading semiconductor foundaries revenue share worldwide from 2019 to 2021, by quar-

lógiák kifejlesztése, amelyekkel az Európai Unió is rendelkezni fog gyártási kapacitással. A chipgyártásban a decentralizáció csak előnyös lehet.

Ugyanakkor felbukkantak új kihívások is a láthatáron. Rock törvénye vagy Moore második törvénye, amelyet Arthur Rockról vagy Gordon Moore-ról neveztek el, azt mondja ki, hogy egy félvezető chipet gyártó üzem költsége a technológiai fejlesztésekkel és a chipek méretének egyre nagyobb csökkenésével, négyévente megduplázódik.[41] Ez eddig igaznak bizonyult és komoly akadályokat gördít a jövőbeli innováció elé. Ugyanakkor, ami talán aggasztóbb, azok a fizikai korlátok a mikrochipek esetén, amelyek egyre inkább materializálódnak. Az ún. alagúthatásnak betudhatóan nem lehet a tranzisztorok méretét a végteleségig csökkenteni, mivel egy idő után nem lesznek képesek arra, hogy megbízhatóan váltásnak a két állapotuk között.[42]

Mindezen felmerült nehézségeket és kihívásokat a jog erejével enyhíteni lehetne, hiszen a félvezetők topográfiájának védelméről rendelkező hatályos jogszabályokat számos helyen adaptálni kellene a kor kihívásaihoz. Példának okáért a nemzetközi és nemzeti szellemi tulajdonjog védelméről szóló normák nagy része a félvezetők elhelyezkedésének oltalmai periódusát 10, illetve 15 évben határozzák meg. Az előbb említett normák ugyanakkor nem számítanak újkeletűnek, az akkori – a mainál sokkal lassabb – technológiai fejlődéshez voltak mérve. A technológiai szektorban az innováció viszont egyre csak gyorsult. Ezért szükségszerűnek találnánk ennek a periódusnak a csökkentését, mivel a régi szabályozás csak visszafogja a fejlődésnek a mai potenciálját és a félvezetők sokszorosítását is nagymértékben hátráltatja.

ter. Statista. https://www.statista.com/statistics/867223/worldwide-semiconductor-foundries-by-market-share/ (2022. 04. 08.)

[41] Bob *Schaller*: The Origin, Nature and implications of "Moore's Law". Microsoft Research. https://web.archive.org/web/20081113014641/http://research.microsoft.com/~gray/Moore_Law.html (2022. 04. 08.)

[42] Raul J. *Martin-Palma*: Quantum tunnelling in low-dimensional semiconductors mediated by virtual photons. AIP Advances 2020/1. sz.

Nagy Gellért
joghallgató, Collegium Iuridicum

Online vitarendezés az 524/2013/EU rendelet tükrében

I. Fejlődéstörténeti előzmények, illetve az online vitarendezési platform célja

Az alternatív vitarendezési eljárások közösségi szintű létrehozása és szabályozása már a XX. század utolsó évtizedeiben megjelent a közbeszédben. Alternatív vitarendezési eljárások alatt mindazon, a jogviták peres eljáráson kívüli rendezésére szolgáló módszereket értjük, amelyek „*jellemzően gyorsabbak, olcsóbbak és egyszerűbben igénybe vehetőek, mint a peres eljárások [...] önkéntesek, bizalmasak és független harmadik személy bevonásával járhatnak*".[1]

Ezen alternatív vitarendezési eljárások Európai Közösségen belülimegteremtése volt az egyik legfőbb ok, amiért 1987-ben az Európai Bizottság egy szakértői csoportot hozott létre, Marcel Storme professzor vezetéséve annak érdekében, hogy egy európai eljárásjogi kerettörvénykönyv kidolgozásával elősegítsék a jogharmonizációt az eljárásjog területén is. A szakértői csoport tanulmányában kiemelte, hogy a békéltetés, ugyan a tagállami szabályozásokban nagyon eltérően és változó módon jelenik meg, egy alternatív, gyors, egyszerű, könnyen, mindenki számára elérhető és kevéssé költséges eljárás megteremtése nagy mértékben hozzájárulna a tagállami bíróságok túlterheltségének csökkentéséhez, illetve az igazságszolgáltatás minőségének javításához.[2] Ezt követően 1993-ban egy európai bizottsági zöld könyv vetette fel az egységesített, közösségi szinten szabályozott vitarendezési eljárások igényét, amelynek megteremtését néhány ajánlással is sürgették a közösség intézményei (például a 98/257/EK vagy a 2001/310/EK ajánlásokkal).[3]

Megfigyelhető, hogy 2005 és 2011 között az unió jogalkotó elsősorban az egyes

[1] *Malik* Éva: Pillanatkép az alternatív polgári vitarendezésről. Jura 2017/1. sz. 293. o.

[2] Ghinoiu *Decebal Adrian*: Metode alternative de soluționare a litigiilor în sistemul dreptului comunitar. Revista Română de Drept Privat 2010/4. sz.

[3] *Simon* Rita: A fogyasztói viták alternatív vitarendezése Európában – ötlet-verseny és fórum shopping a nemzeti szabályozás és implementációs kötelezettség tükrében? Iustum Aequum Salutare 2016/2. sz. 65. o.

fontosabb gazdasági szektorok tekintetében fogadott el alternatív vitarendezési normákat, mint például az energiaszektor (2009/72/EU és 2009/73/EU irányelvek).[4] Ezt követően, 2011-ben az Európai Parlament kiadott egy határozatot, amelyben az alternatív vitarendezési módszerek szélesebb körű alkalmazására hívja fel a figyelmet. E határozat, nem pusztán a fogyasztók és kereskedők között létrejövő, de a két vagy több kereskedő között fennálló jogviszonyok kapcsán felmerülő viták alternatív rendezésének előnyeit is kiemeli.[5]

Az alternatív vitarendezési eljárások szükségessége az online térben lebonyolított vásárlások egyre gyakoribbá válásával még inkább felerősödött. Szükségessé vált, mint ahogyan azt a vizsgált rendelet is leszögezi indoklásában, hogy mind a fogyasztók, mind a kereskedők minél nagyobb bizalommal legyenek a belső piac digitális dimenziója iránt, és ki tudják használni az általa nyújtott előnyöket, lehetőségeket. Továbbá, elengedhetetlenné vált, hogy mind a kereskedők, mind a fogyasztók biztonsága, jogainak védelme még inkább teret kapjon.

Az online vásárlások esetében felmerülő jogviták klasszikus úton történő rendezésének lassúsága talán a legjelentősebb nehézség, amellyel a fogyasztók és a kereskedők találkozhatnak az ily módon lebonyolított jogügyletek esetében.[6] Ugyanakkor, az online vásárlások körében felmerülő jogviták jelentős része kisebb összegű követelések kapcsán merül fel, amelyek esetében a klasszikus bírói eljárások már aránytalanul költségesek és hosszadalmasak lennének.[7]

E folyamatok eredményeként első lépésben[8] az Európai Parlament és a Tanács 2013. május 21-én kiadta a fogyasztói jogviták alternatív rendezéséről szóló 2013/11/EU

[4] Rebecca *Berto*: Alternative Dispute Resolution in the Digital Sector. International Journal on Online Dispute Resolution 2020/2. sz. 106. o.

[5] Uo.

[6] *Goicovici* Juanita: Noile procedure de soluționare alternativă a litigiilor dintre comercianți și consumatori. Studia Iurisprudentia 2015/4. sz.

[7] *Simon*: i. m. 64. o.

[8] Az Európai Unió aktusai mellett fontos kiemelni az ENSZ Nemzetközi Kereskedelmi Jogi Bizottságának (UNCITRAL) online vitamegoldó eljárás kérdése kapcsán tett lépéseit. A Bizottság 2010-ben tűzte napirendjére az online vitamegoldó eljárás problémáját, és elhatározta, hogy mintaszabályokat (Rules) tartalmazó nemzetközi jogi dokumentumokat dolgoz ki. A mintaszabályok kidolgozását azonban lelassították bizonyos, a munkacsoporton belüli nézeteltérések. Lásd: *Milassin* László: Fogyasztóvédelem és az online vitamegoldó eljárás. Iustum Aequum Salutare 2014/2. sz. 95. o.

irányelvet (fogyasztói alternatív vitarendezési irányelv), amely az adásvételi vagy szolgáltatási szerződésekkel kapcsolatos jogviták rendezésére kínál megoldásokat.

Szintén 2013. május 21-én a Parlament és a Tanács kiadta az 524/2013/EU számú fogyasztói jogviták online rendezéséről szóló rendeletet (fogyasztói online vitarendezési rendelet). Az irányelv és a rendelet, bár a gyakorlati alkalmazásban jelentős mértékben összefonódik, hatályuk tekintetében eltérnek egymástól. Míg az irányelv hatálya mind az online, mind a hagyományos ügyletek kapcsán felmerülő jogvitákra kiterjed, addig a rendelet előírásai, amint arra az alábbiakban részletesebben is kitérünk, kizárólag az online adásvételi vagy szolgáltatási szerződésekre alkalmazandóak.

A továbbiakban, a kutatás terjedelmi korlátaiból fakadóan, kizárólag az online vitarendezésről, és azon belül is az 524/2013/EU számú fogyasztói jogviták online rendezéséről szóló rendeletről kívánok részletesebben értekezni, kiemelve az online vitarendezési platform hatályát, a konkrét vitarendezés menetét, illetve a platform pozitív és negatív aspektusait.

Online vitarendezés alatt értjük azt az eljárást, amely „*lehetővé teszi, hogy a felek vitájukat online eszközök – mint például az internet vagy a virtuális kommunikációt lehetővé tevő más eszközök – segítségével oldják meg, anélkül, hogy a feleknek egy helyiségben kellene tartózkodniuk*"[9]. Richard Susskind értelmezésében pusztán azokban az esetekben beszélhetünk online vitarendezésről, ha a felmerülő jogviták rendezésének folyamata, kiváltképp a megoldása nagyrészt vagy teljes mértékben interneten keresztül történik.[10]A nemzetközi szakirodalom értelmezésében online vitarendezésről beszélhetünk többek között abban az esetben is, ha a klasszikus értelemben vett vitarendezés az interneten, e-mailen, weboldalakon vagy akár *streaming* szolgáltatókon keresztül valósul meg.[11]Kijelenthető, hogy az online vitarendezés egyik legfontosabb jellemzője, hogy a jogvitában érintett felek között a kommunikáció a vitarendezés során virtuális térben zajlik[12], a feleknek nem szükséges egyidejűleg, fizikailag jelen lenniük.

[9] *Malik*: i. m. 300. o.

[10] Richard *Susskind*: Az ügyvédség vége? A jogi szolgáltatások természetének ujragondolásáról. CompLex, Budapest 2012. 196. o. Idézi: *Malik*: i. m. 300. o.

[11] Biljana *Duricin*: A Handbook of Alternative Despute Resolution and Mediation. Terms. Univerzitet Crne Gore, Podgorica 2013. 43. o.

[12] Uo.

Az online vitarendezés egyre szélesebb nemzetközi elterjedésében három fő ok játszik kiemelt szerepet:

– globális szinten a teljes kiskereskedelmi értékesítés 7.4%-a zajlott online térben 2015-ben, ám a folyamatos növekedésnek köszönhetően ez a szám 2020-ra elérte a 18%-ot;

– mind az államok vezetői, mind a digitális kereskedelemben érdekelt társaságok elköteleződtek az online vitarendezés szükségessége mellett;

– valamint az online térben otthonosan mozgó generációk számára az úgynevezett „click-based" megoldások számítanak alapvetőnek, így esetükben az online vitarendezés a legtermészetesebb megoldás egy jogvita fennállása esetén.[13]

Az online vitarendezési platformok elterjedése két, egymástól alapvetően elkülönülő jelenséget vont maga után nemzetközi téren: egyrészt a már meglévő, tradicionális alternatív vitarendezési módszerek kiterjedtek az online térbe is, másrészt megjelentek olyan új alternatív vitarendezési eljárások, amelyek sok esetben nem csak online, de offline is igénybe vehetőek.[14] Tehát kijelenthetjük, hogy az online vitarendezési platformok létrehozása nemzetközi szinten pozitív hatással volt az alternatív vitarendezési módszerek elterjedésére.

Az 524/2013/EU számú rendelet legfőbb célja, a rendelet 1. cikke alapján, egy olyan európai online platform létrehozása, amely elősegíti a fogyasztók és a kereskedők közötti jogviták független, pártatlan, átlátható, eredményes, gyors és méltányos, bírósági eljáráson kívüli online rendezését. A rendelet indoklásában a közösségi jogalkotó kiemeli, hogy a létrehozott online vitarendezési platform célja nem a bírósági eljárások helyettesítése és nem is a kereskedők és a fogyasztók bírósági jogorvoslathoz való hozzáférésének korlátozása, hanem pusztán egy alternatív, gyorsabb és költségkímélőbb megoldás kialakítása és felkínálása. Ahogyan azt a szakirodalomban is megfogalmazták, az alternatív vitarendezési eljárások esetében a fogyasztók az eljárás bármely pillanatá-

[13] Teresa *Ballesteros*: International Perspectives on Online Dispute Resolution in the E-Commerce Landscape. International Journal on Online Dispute Resolution 2021/1. sz. 86. o.

[14] Benjamin G. *Davis*: International Commercial Online and Offline Dispute Resolution: Addressing Primacism and Universalism. The Journal of American Arbitration 2005/4. sz. 83. o.

ban kiléphetnek, ha nem elégedettek annak menetével.[15]

II. Az uniós online vitarendezési platform hatálya

Az 524/2013/EU rendelet 2. cikke kiemelten rendelkezik az online vitarendezési platform hatályáról. E cikk értelmében a rendelet, és ezáltal az online vitarendezési platform hatálya az Unióban tartózkodási hellyel rendelkező fogyasztók és az Unióban letelepedett kereskedők között megkötött online adásvételi vagy szolgáltatási szerződésekből eredő kötelezettségekkel kapcsolatban felmerülő jogviták bírósági eljáráson kívüli rendezésére alkalmazandó.

Fontos kiemelni, hogy bár az irányelv az Európai Unió tagállamaira vonatkozik, ugyanakkor a platform az Európai Gazdasági Térség másik három tagállamában is hatályos, így Izland, Liechtenstein és Norvégia esetében is fordulhatnak a kereskedők és a fogyasztók a platform segítségével az alternatív vitarendezési fórumokhoz.[16]

A fogyasztó és a kereskedő fogalmának meghatározására a rendelet a 2013/11/EU fogyasztói alternatív vitarendezési irányelvre tesz utalást, amely irányelv konkrétan megadja mind a fogyasztó, mind a kereskedő fogalmának tartalmát. Az említett irányelv 4. cikk (1) bekezdésének a) pontja értelmében fogyasztó „*bármely természetes személy, aki nem kereskedelmi, üzleti vagy szakmai célból jár el*". Ugyanezen bekezdés b) pontja tartalmazza a kereskedő fogalommeghatározását, amelynek fényében kereskedőnek tekintendő „*bármely természetes vagy jogi személy, függetlenül attól, hogy magán- vagy állami tulajdonban van-e, aki vagy amely kereskedelmi, üzleti vagy szakmai tevékenységi körét érintő célból jár el, beleértve azt is, ha helyette vagy nevében más személy jár el*".

A rendelet tehát, a kereskedők és fogyasztók között, úgynevezett B2C (Business to Consumer) kapcsolatokban fennálló jogviszonyok kapcsán felmerülő jogvitákra terjed ki.[17]

Érdemes ezen a ponton röviden kitérni a letelepedés fogalmára, amelynek sem az elsődleges, sem a másodlagos uniós jogban nincs meghatározása, tartalmát

[15] *Goicovici:* i. m.

[16] A továbbiakban elsősorban az Európai Unió tagállamaira összpontosítok, ám a statisztikai adatok ismertetésénél az Európai Gazdasági Térség egészére vonatkozó információkat kívánok ismertetni.

[17] *Milassin:* i. m. 98. o.

az Európai Unió Bíróságának gyakorlata adja. E gyakorlat érelmében „a letelepedés állandó helyszínen (telephelyen), határozatlan ideig ténylegesen végzett gazdasági tevékenységet jelent”[18]. Letelepedésről beszélünk ugyanakkor, abban az esetben is, ha egy társaságot határozott időre alapítanak, ha nem rendelkezik a tevékenysége végzéséhez használt épület tulajdonjogával vagy ha azon tagállam, ahol a letelepedés esedékes csak korlátozott időre nyújt engedélyt bizonyos gazdasági szolgáltatásokra.[19]

A rendelet alapján a kereskedők letelepedésének helyét a 2013/11/EU fogyasztói alternatív vitarendezési irányelv 4. cikkének (2) és (3) bekezdéseiben foglaltak alapján kell meghatározni. A (2) bekezdés értelmében, ha a kereskedő természetes személy, akkor ott tekintendő letelepedettnek, ahol üzleti tevékenységét végzi, amennyiben azonban a kereskedő jogi személy, vállalkozás illetve természetes vagy jogi személyek társasága, akkor letelepedési helyének az tekinthető, ahol létesítő okirat szerinti székhelye, központi ügyvezetése vagy üzleti tevékenységének fő helyszíne található.

A kereskedő tekintetében érdemes kitérni a rendelet 2. cikkének (2) bekezdésére is, amely értelmében egy kereskedő csak abban az esetben kezdeményezhet online vitarendezést egy fogyasztóval szemben, ha a fogyasztó szokásos tartózkodási helye szerinti tagállam jogszabályai lehetőséget nyújtanak arra, hogy a felmerülő jogvitákat valamely alternatív vitarendezési fórum közreműködésével rendezzék.[20]

Ahogyan az a vizsgált rendelet preambulumának (14) pontjából is kitűnik, a rendelet (és ezáltal az online vitarendezési platform) nem alkalmazandó a fogyasztók és a kereskedők közötti azon jogvitákra, amelyek nem internetes úton jöttek létre. A rendelet 3. cikk (1) bekezdésének e). pontja konkrét meghatározást nyújt az online adásvételi vagy szolgáltatási szerződés fogalmára. Eszerint online adásvételi vagy szolgáltatási szerződés minden olyan adásvételi vagy szolgáltatási szerződés, amelynek értelmében a kereskedők vagy a kereskedő közvetítője egy weboldalon vagy egyéb elektronikus eszközön keresztül kínál megvételre valamilyen árut vagy szolgáltatást, és a fogyasztó az

[18] *Metzinger* Péter: Letelepedési jog. In: EU-jog (szerk. *Osztovits* András). HVG-ORAC Kiadó, Budapest 2021. 481. o.

[19] Uo.

[20] Bővebben lásd: *Smarandache* Lavinia Elena: Mecanisme de soluționare extrajudiciară a conflictelor dintre instituțiile de credit și consumatori.Revista Română de Drept al Afacerilor 2016/7. szám.

adott weboldalon vagy elektronikus eszközön kereztül rendeli meg az árukat vagy szolgáltatásokat. Fontos kiemelni, hogy az egyenlő versenyfeltételek érdekében az online vitarendezési platformok elérhetőek mind a határokon átnyúló, mind a belföldi internetes ügyletek kapcsán felmerülő jogviták orvoslatára.

A szakirodalomban kritikaként fogalmazódott meg az online vitarendezési platform hatálya tekintetében, hogy az nem alkalmazandó sem a fogyasztó és kereskedő között, a tárgyalások során felmerülő, sem két vagy több kereskedő kapcsolatában megjelenő jogviták kezelésére.[21]

III. Az online vitarendezési platform az 524/2013/EU rendelet fényében

A vizsgált rendelet indoklásából kitűnik, hogy az online vitarendezési platform egy olyan interaktív weboldal, amely egyetlen belépési ponton keresztül mind a fogyasztók, mind a kereskedők számára megközelíthető az online ügyleteik kapcsán felmerülő viták bírósági eljráson kívül történő rendezése céljából. Az online vitarendezési platform fejlesztése, üzemeltetése és karbantartása az Európai Bizottság feladatkörébe tartozik.

Az online vitarendezési platform mindamellett, hogy tájékoztatást nyújt az alternatív vitarendezési módszerekről, lehetőséget biztosít, hogy a hatálya alá eső jogvitákat az Unió intézményeinek hivatalos nyelvein rendezzék. Ennek érdekében a platformnak biztosítania kell, mind a kereskedők, mind a fogyasztók számára a szükséges nyilatkozatokhoz való szabad hozzáférést mindezen nyelveken. Ugyanakkor a platform legfontosabb eleme az elektronikus ügykezelő eszköz, amely lehetőséget nyújt a felmerülő jogviták, alternatív vitarendezési fórumok általi, online rendezésére. Kitűnik tehát, hogy az online vitarendezési platform a már meglévő alternatív vitarendezési fórumokra épül, amely fórumok közösségi szabályozásának keretét a 2013/11/EU irányelv adja.

Az online vitarendezési platform tehát nem egy új, alternatív vitarendezési módot hoz létre, hanem a már meglévő, tagállami (illetve az Európai Gazdasági Térség nem uniós tagállamaiban székelő) alternatív vitarendezési fórumokat fogja össze és biztosítja az e fórumokhoz történő online hozzaférést. Ugyanakkor, a platform nem garantálja (és nem is garantálhatja, hiszen az egyes fórumok a saját eljárási szabályaik mentén döntenek), hogy maguk az alternatív vitarendezési fórumok is online térben járnak el, pusztán

[21] *Goicovici:* i. m.

a döntés online közlését teszi kötelezővé.

A vizsgált rendelet preambulumának (21) pontja értelmében az online vitarendezési platform az „Európa Önökért"[22] portálon keresztül érhető el. E portál egy egész Európára kiterjedő, többnyelvű online információs oldal, amely a vállalkozások és az uniós polgárok számára kínál szolgáltatásokat. Az rendelet említett pontja továbbá azt is kiemeli, hogy az online vitarendezési platformom az „Európa Önökért" portálon belül jól észrevehető helyen kell feltüntetni.[23]

Ugyanakkor, a vizsgált rendelet 5. cikkének (6) bekezdésével összhangban az oldalon fellelhető mindazon alternatív vitarendezési platformok jegyzéke, amelyek megfelelnek a 2013/11/EU irányelv által támasztott feltételeknek. A bejegyzett alternatív vitarendezési fórumokat előzőekben a tagállamok választják ki, bizonyos kritériumrendszer alapján, majd szintén ők küldik meg a Bizottságnak a kiválasztott fórumok jegyzékét.[24]

Az online vitarendezési platform által ellátott konkrét feladatokat a fogyasztói online vitarendezési rendelet 5. cikkének (6) bekezdése taxatíve felsorolja. E rendelkezés értelmében az online vitarendezési platform a következő feladatokat látja el: elérhetővé teszi a panaszok bejelentésére szolgáló elektronikus űrlapot; tájékoztatja az ellenérdekű felet a panaszról; meghatározza a hatáskörrel rendelkező vitarendezési fórumot vagy fórumokat, és eljuttatja a panaszt ahhoz (abban az esetben, ha a panasz több fórum hatáskörébe is betartozik a platform a felek által megállapodott fórumnak küldi meg a panaszt); díjmentesen biztosít egy elektronikus ügykezelő eszközt, amely lehetővé teszi

[22] A portál az alábbi linken érhető el: Segítség és tanácsok az uniós polgárok és családtagjaik számára. Your Europea. https://europa.eu/youreurope/citizens/index_hu.htm (2022. 05. 28.)

[23] A konkrét online vitarendezési platform az alábbi címen érhető el: Online Dispute Resolution. https://ec.europa.eu/consumers/odr/main/?event=main.home2.show. (2022. 05. 28.) Az oldalon megjelenő menüsorban külön fül áll rendelkezésre a rendszer működésének közérthető elmagyarázása, a fogyasztói jogok ismertetésére, valamint az ügy elindítására is.

[24] *Smarandache*: i. m. Jelenleg az alternatív vitarendezési fórumok jegyzékében, az online vitarendezési platformon elérhető jegyzék alapján, Románia csak két intézménnyel képviselteti magát: A Nemzeti Fogyasztóvédelmi Hatóság alternatív vitarendezési igazgatósága (Autoritatea Națională pentru Protecția Consumatorilor – Direcția de Soluționare Alternativă a Litigiilor), illetve az Alternatív vitarendezési testület a nem banki pénzügyek területén – SAL-FIN (Entitatea de Soluționare Alternativă a Litigiilor în domeniul financiar nonbancar – SAL-FIN). Magyarország tekintetében, ugyanakkor valamivel jobb a helyzet a listázott alternatív vitarendezési fórumok tekintetében, hiszen a jegyzékben szerepelnek a megyei Békéltető Testületek, a fővárosi Békéltető Testület, illetve a Pénzügyi Békéltető Testület is.

az eljárás online térben történő lebonyolítását; biztosítja a szükséges információk fordítását; biztosítja az alternatív vitarendezési fórum számára az eljárás eredményének közlésére szolgáló űrlapot; visszajelzési rendszert működtet a platform működésével, illetve az alternatív vitarendezési fórumokkal kapcsolatos vélemények kifejtésére; illetve biztosítja az egyes közérdekű adatokhoz való szabad hozzáférést.

Mindemellett, az online vitarendezési platform kialakítja az online vitarendezést segítő kapcsolattartó pontok hálózatát, a vizsgált rendelet 7. cikke alapján. Az online vitarendezési kapcsolattartó pontok célja a platformon keresztül benyújtott panaszokkal kapcsolatos jogviták rendezéséhez való segítségnyújtás.

Annak érdekében, hogy az online vitarendezési platform minél szélesebb körben elterjedjen, és ezáltal a fogyasztók jogai még nagyobb védelmet élvezzenek, mindazon, az Unióban letelepedett kereskedők, amelyek online adásvételi vagy szolgáltatási szerződéseket kötnek meg, kötelesek a weboldalukon feltöntetni az online vitarendeséi platform elérhetőségeit.[25]

Ugyan, a tagállamok szintjén Románia áll a legrosszabbul az elérhető vitarendezési platformok számának tekintetében, a vitarendezési platformhoz beérkezett panaszok tekintetében nem olyan rossz a helyzet.

Az Európai Bizottság legfrissebb, 2020-as évre vonatkozó statisztikája alapján a beérkezett panaszok az alábbi módon oszlanak meg, a 15 legtöbb panasszal bíró állam tekintetében:

Ország	**Fogyasztó által benyújtott panasz**	**Kereskedő által benyújtott panasz**
Németország	2776	2982
Olaszország	2781	1351
Egyesült Királyság[26]	2653	2495
Franciaország	2460	1625

[25] *Smarandache*: i. m.

[26] Az Egyesült Királyság 2020. december 31-ig volt az Európai Gazdasági Térség tagja, így a 2020-as statisztikában még szerepel.

Spanyolország	1792	2928
Lengyelország	867	483
Portugália	617	340
Románia	412	110
Hollandia	395	1311
Belgium	333	196
Magyarország	326	1322
Ausztria	296	189
Görögország	240	204
Bulgária	178	102
Írország	177	591

1. Táblázat[27]

Szintén az Európai Bizottság által közzétett statisztikából kitűnik, hogy melyek azon gazdasági ágazatok, amelyek esetében a legtöbb panasz felmerült. A 2020-as évben e gzdasági ágazatok/szereplők a következők voltak: légitársaságok (az összes beérkező panasz 25.16%), személygépkocsik és egyéb szállítóeszközök kiegészítőit és alkatrészeit forgalmazó kereskedők (6.38%), hotelek és egyéb vakációs üdülőhelyek (6.22%), ruházati és lábbeli termékeket forgalmazó kereskedők (6.11%), információ- és kommunikáció-technológia (5.15%), elektronikai eszközök forgalmazása (3.37%), illetve lakberendezés (3.32%).[28]

IV. Az online vitarendezési eljárás menete

Az online vitarendezési platform által felkínált eljárás menetére vonatkozóan a vizsgált 524/2013/EU rendelet átfogó szabályokat határoz meg. A rendelet 8. cikkének értelmében a panaszos fél az online vitarendezési platformhoz a panaszok bejelentésére szolgáló elektronikus űrlap kitöltésével nyújthat be panaszt. A panaszok benyújtásakor

[27] Az adatok forrása: https://ec.europa.eu/info/sites/default/files/2021-report-final.pdf (2022. 03. 14.)

[28] Az adatok forrása: https://ec.europa.eu/info/sites/default/files/2021-report-final.pdf (2022. 03. 14.)

megadandó információk tekintetében a rendelet mellékletében találunk releváns felsorolást, amely tételesen felsorolja mindazon információkat amelyeket a panaszok benyújtása esetében kötelezésen meg kell adni (ilyen például, hogy a panaszos fél fogyasztó vagy kereskedő; a fogyasztó, illetve a kereskedő neve, e-mail és postacíme; a panaszos fél képviselőjének a neve; az árú vagy szolgáltatás típusa; a megvásárolt áruk vagy szolgáltatások ára; a panasz típusa vagy a panasz ismertetése). A panaszos fél által megadott információknak elégségeseknek kell lenniük a hatáskörrel rendelkező alternatív vitarendezési fórum megállapításához. Továbbá, a panaszos fél a dokumentumhoz csatolhat minden olyan dokumentumot, amely szükséges a panasz alátámasztásához.

A panaszok benyújtására szolgáló űrlap hiánytalan kitöltését követően megkezdődik a beérkezett panaszok feldolgozása és továbbítása, ellenkező esetbe, ha az űrlap hiányos, a panaszos felet értesíteni kell a hiányosságokról. A hiánytalanul benyújtott panaszokat az online vitarendezési platform, késedelem nélkül, közli az ellenérdekelt féllel, az e fél által választott nyelven (amely ugyanakkor az Unió intézményeinek egyik hivatalos nyelve kell legyen). Az online vitarendezési platform a panaszt a rendelet 9. cikkének (3) bekezdésében meghatározott információkkal együtt küldi meg az ellenérdekelt félnek. A felek, az illetékes alternatív vitarendezési fórumra vonatkozó megállapodását követően az alternatív vitarendezési platform automatikusan és haladéktalanul továbbítja a panaszt a felek megállapodásának tárgyát képező fórumhoz. A megkeresett alternatív vitarendezési fórum tájékoztatja a feleket a panasz befogadásáról vagy elutasításáról. Abban az esetben, ha a felek a panasz benyújtásától számított 30 napon belül nem tudnak megegyezni az illetékes alternatív vitarendezési fórumról, vagy a megkeresett fórum elutasítja a beérkezett panaszt, további feldolgozásra nem kerül sor.

A megkeresett alternatív vitarendezési fórum a saját eljárási szabályait alkalmazza, beleértve a díjakra és illetékekere vonatkozó saját normákat is. Ugyanakkor, ezen rendelkezések mellett a vizsgált rendelet előírásait is tiszteletben kell tartania.[29]

A vizsgált rendelet 10. cikke kimondja az alternatív vitarendezési fórumnak a beérkezett panaszokkal kapcsolatos kötelezettségeit. Ennek fényében, a 2013/11/EU irányelv 8. cikkének e) pontjával összhangban az alternatív vitarendezési fórum köteles a panaszt a beérkezéstől számított 90 naptári napon belül lezárni, ugyanakkor, kivált-

[29] *Smarandache*: i. m.

képp a rendkívül összetett panaszok esetében, az alternatív vitarendezési fórum ezen időszakot saját belátása szerint meghosszabíthatja. E kötelezettség mellett az alternatív vitarendezési fórumnak tartózkodnia kell a felek (vagy azok képviselőik) fizikai jelenlétének megkövetelésétől. E tilalom alól kivételt képeznek mindazon esetek, amikor a felek a fizikai jelenlétbe beleegyeztek, illetve az adott vitarendezési fórum szabályai a fizikai jelenlétet lehetővé teszik.

Az alternatív vitarendezési fórum köteles haladéktalanul továbbítani az online vitarendezési platform felé a panasszal kapcsolatos ügyirat beérkezésének időpontját, a jogvita tárgyát, a vitarendezés lezárásának dátumát és az eljárás kimenetelét.

Az online vitarendezési platform eljárásának menetével kapcsolatban megfigyelhető, hogy valóban sikerült egy olyan módszert a kereskedők és a fogyasztók rendelkezésére bocsátani, amely a rendes bírósági eljárásnál gyorsabb és méltányosabb alternatívát képez az online adásvételi vagy szolgáltatási szerződések kapcsán felmerülő jogviták kezelésére.

V. Személyes adatok védelme az online vitarendezési platform keretében történő eljárásokban

Meghatározása szerint az adatvédelem „olyan jogi védelem, amely az egyének magánszférájának védelmét célozza az egyénnel kapcsolatba hozható adatok (személyes adatok) kezelésére vonatkozó szabályok előírásával".[30] Magától értetődő, hogy az online térben a személyes adatok védelme még hangsúlyosabbá kell váljon, hiszen, amint azt az Európai Parlament és a Tanács 2016/679/EU számú általános adatvédelmi rendelete is kiemeli preambulumában, a természetes személyek összefüggésbe hozhatók az általuk használt online azonosítókkal (pl. IP-címekkel, cookie-azonosítókkal), amelynek következtében olyan nyomok keletkezhetnek, amelyek más információkkal összekapcsolva felhasználhatók az adott természetes személy profiljának létrehozására, vagy az adott személy azonosítására.

Mindezek fényében az online vitarendezési platform esetében is szükséges volt a személyes adatok védelmére, kiváltképp annak tudatában, hogy e platform számos olyan információt tárol a jogviták megoldása érdekében, amelyek a felekre nézve sok

[30] *Jóri* András – *Soós* Andrea Klára: Adatvédelmi jog. Magyar és európai szabályozás. HVG-ORAC Kiadó, Budapest 2016. 24. o.

esetben kényes, nem nyilvános adatokat tartalmaznak.

Például, annak érdekében, hogy egy fogyasztó megfelelően kitöltse a panaszra vonatkozó elektronikus űrlapot, meg kell adnia nevét, lakcímét, e-mail címét és fakultatívan a telefonszámát is. Továbbá, a fogyasztó köteles megadni az általa vásárolt termék, vagy igényelt szolgáltatás megnevezését és árát is. Tulajdonképpen, az űrlap kitöltésével olyan adatok kerülnek bevezetésre a rendszerbe, amelyekből nem csak a fogyasztó személyazonosságát lehet feltárni, de adott esetben az anyagi helyzetét is fel lehet térképezni (annak alapján, hogy milyen termékeket vagy szolgáltatásokat és milyen értékben vásárolt).

E személyes adatok védelmére, teljesen megalapozottan, az az 524/2013/EU számú fogyasztói jogviták online rendezéséről szóló rendeletet részletesen kitér. Már a rendelet indoklásának (28) pontja leszögezi, hogy a jogvitában érintett feleket, a Bizottság által közzétett általános adatvédelmi nyilatkozat útján, tájékoztatni kell személyes adataik feldolgozásáról, amelyhez beleegyezésüket kell kérni. Továbbá, az adatvédelmi nyilatkozat egyszerű és közérthető nyelven kell leírja a platform egyes szereplőinek felelőssége alatt végrehajtott adatfeldolgozási eljárásokat. A személyes adatok védelme érdekében, a preambulum (36) pontjával összhangban, a Bizottságnak konzultálnia kell az európai adatvédelmi biztossal.

A rendelet 5. cikkének (1) bekezdése továbbá kiemeli, hogy felhasználók adatait már a tervezés szakaszától, az úgynevezett beépített adatvédelem elvének segítségével védeni kell a vitarendezési platform létrehozása, működtetése és fenntartása során. A 2016/679/EU számú általános adatvédelmi rendelet 25. cikke értelmében a beépített adatvédelem elve az adatkezelő azon kötelezettséget foglalja magába, hogy, a tudomány és a technológia mindenkori állása valamint a megvalósítás költségei figyelembevételével, olyan technikai és szervezési intézkedéseket hajtson végre amelyek célja az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába. A rendelet konkrétan nevesíti az álnevesítést, mint beépített adatvédelmi mechanizmust, de emellett megemlíthető, mint hasonló módszer az adatok titkosítása is. Emellett, ahogyan arra az általános adatvédelmi rendelet preambulumának (78) pontja is kitér, a beépített adatvédelem magába foglalja a személyes adatok kezelésének minimálisra csökkentését, a személyes adatok mihamarabbi álnevesítését, a személyes adatok funkcióinak és kezelésének átláthatóságát is.

Kijelenthető tehát, hogy az online vitarendezési platform létrehozásáról és működéséről szóló, vizsgált rendelet előírásaiban a közösségi jogalkotó kiemelten próbált figyelni a személyes adatok megfelelő szintű védelmére, így tehát megalkotta azon keretet, amely egy védőhálót biztosít a jogvita megoldása során közölt adatok szavatolására.

VI. Az online vitarendezési platform előnyei és hátrányai

Az Európai Unió természetéből fakadóan a tradicionális vitarendezési megoldások reformja egyidőben zajlott tagállami és közösségi szinten, ez a terep pedig nagy mértékben hozzájárult az online vitarendezési platform elterjedéséhez, és mintegy a klasszikus vitarendezési megoldások alternatívájaként tudott megjelenni az online vitarendezés.[31]

A szakirodalomban kialakult nézet szerint, az Európai Unió az online vitarendezési eljárások tekintetében két fő célkitűzést követ: egyrészt a fogyasztói érdek elsődleges védelmét, az online eljárásban történő érdekérvényesítés elősegítésével, másrészt a felmerülő viták nem bírósági, hanem online úton történő rendezését.[32]

Elfogadva a fenti álláspontot, kijelenthetjük, hogy az online vitarendezési platform létrehozásával az Európai Unió tovább kívánta csökkenteni a kereskedők és a fogyasztók közötti egyenlőtlenséget, és ezáltal előmozdítani a fogyasztói érdek teljesebb védelmét. Ugyanakkor a fogyasztói érdek online térben történő védelme előmozdíthatja a fogyasztók biztonságérzetének növelését is. Továbbá megteremtheti mindazon feltételeket, amelyek a fogyasztó esetleges sérelmének fennállásakor biztosítják a megfelelő jogorvoslatot.

Amint az a rendelet I. fejezetének 1. cikkének célmeghatározásából is szembetűnik, az Európai Unió célja a magas szintű fogyasztóvédelem megvalósítása. A magas szintű fogyasztóvédelem megjelenik az Európai Unió működéséről szóló szerződés 169. cikkében és az Európai Unió Alapjogi Chartájában is.[33] „*Mindezek alapján egyértelmű az Európai Bizottság, mint az EU végrehajtó szervének szilárd eltökéltsége arra, hogy az áruk és a szolgáltatások online értékesítése kapcsán biztosítsa a fogyasztók bizalmát a közös*

[31] *Ballesteros*: i. m. 97. o.

[32] *Milassin*: i. m. 98. o.

[33] Uo.

belső piac e szegmensének működéséhez."[34]

Az online térben megkötött adásvételi vagy szolgáltatási jogügyletek esetében a fogyasztók védelme még hangsúlyosabb szerepet kell nyerjen. Egyrészt a vásárolt termékek esetében nem áll fenn azok tényleges, természetbeni kézhezvétele, vizsgálata a szerződés megkötése előtt, így a fogyasztó nagyobb kockázatnak van kitéve, mint az egyidejű fizikai jelenléttel megkötött szerződések esetében. Másrészt, sok esetben az ilyen online adásvételi vagy szolgáltatási szerződések nemzetközi, az Európai Unió tekintetében határon átívelő elemmel bírnak, amely megnehezíti a megfelelő jogorvoslat biztosítását. Így tehát, ha az alternatív vitarendezési eljárások az igazságszolgáltatáshoz való jobb hozzáférést biztosíthatják[35], akkor e megállapítás még inkább érvényes az alternatív vitarendezési eljárások online térben történő végbemenetelére. Az Európai Unió által megteremtett online vitarendezési platform pont egy ilyen gyors, a felek egyidejű fizikai jelenlétét nem igénylő és anyagilag nem megterhelő eszközt biztosít a hatálya alá eső jogügyletek esetében felmerülő jogviták rendezésére. Ugyanakkor, megfigyelhető, hogy az Európai Bizottság, azáltal, hogy konkrétan szerepet vállal az online vitarendezés folyamatában (például azzal, hogy ő a platform üzemeltetője és karbantartója) az európai fogyasztók érdekeinek védelmét tartja elsődlegesen szem előtt.[36]

Kijelenthetjük továbbá, hogy az Európai Unió tevékenységének pozitív hozadéka lehet a tagállamok polgárainak jogtudatossága fokozásában is[37], azáltal, hogy egy, bárki számára, akár otthonról is elérhető eszközt biztosít a jogviták rendezésére, ösztönözve ezáltal a mind a fogyasztókat, mind a kereskedőket a jogvitában felmerülő panaszok törvényes keretek között történő megoldására. Azáltal, hogy a felmerülő jogvitákat már nem csak a klasszikus, bírói úton lehet orvosolni, csökkenthető az úgynevezett „*racionális tétlenség*", hiszen igényei érvényesítésének „*költség-haszon vizsgálata során*" a fogyasztók már nem kell azon, a gyakorlatban sok esetben elrettentő következtetésre jussanak, hogy a jogorvoslat túlságosan költséges és hosszadalmas számukra.[38]

Ugyanakkor, az online vitarendezési platform jelenleg számos hiányossággal is

[34] Uo.
[35] *Malik:* i. m. 293. o.
[36] *Milassin:* i. m. 99. o.
[37] *Malik:* i. m.293. o.
[38] *Simon:* i. m. 64. o.

küzd. Egyrészt, néhány tagállam esetében korlátozott azon alternatív vitarendezési fórumok száma, amelyekhez az online vitarendezési platformon keresztül panasszal lehet fordulni (például Finnországból három; Litvániából, Írországból, Görögországból, Hollandiából és Észtországból négy alternatív vitarendezési fórumhoz lehet a platform igénybevételével fordulni, ám e szempontból a tagállamok közül Románia áll a legrosszabbul, hiszen pusztán a két, már említett fórum érhető el). Ugyanakkor, az elérhető alternatív vitarendezési fórumok „*európai képe kaotikus*"[39], sok esetben az Európai Bizottsághoz bejelentett alternatív vitarendezési fórumok listáját nem aktualizálták, a tagállamok nem frissítették a bejelentéseiket.[40]

Másrészt az online vitarendezési platform jelenleg csak a kereskedők és fogyasztók között online adásvételi vagy szolgáltatási szerződések tekintetében felmerülő jogviták tekintetében alkalmazandó. Véleményem szerint fontos lenne a platform hatályának kiterjesztése a fogyasztók és a kereskedők között felmerülő, szerződéskötés pillanatát megelőző, illetve a két (vagy több) kereskedő között létrejövő online adásvételi vagy szolgáltatási szerződések kapcsán kialakult jogvitákra is. Az elmúlt pár év eseményei, a világjárvány és az ezzel párhuzamosan fokozottabban virtuális térbe szoruló ügyintézés kiváltképp szükségessé tenné az online vitarendezési platform hatályának kiterjesztését, hogy ezáltal a kereskedelemben felmerülő jogviták gördülékenyebben, gyorsabban és egyszerűbben kerüljenek megoldásra.

Ugyanakkor, azon tényt is szükséges szem előtt tartani, hogy az összetetteb, több problémakört érintő jogviták online rendezése nehézségeket vethet fel. Ezen oknál fogva érthető, hogy az online vitarendezés elsősorban a kisebb, ismétlődő jellegű jogviták megoldása tekintetében vált elterjedté. A jelenlegi nemzetközi gyakorlat fényében az online vitarendezés az egyszerűbb jogviták esetében optimális.[41]

A legmarkánsabb kritika mégis az online vitarendezési platform szerepét kérdőjelezi meg, hiszen munkája tulajdonképpen pusztán a tagállami alternatív vitarendezési fórumok fogyasztók általi felkeresésére korlátozódik, a „testületek formáját, működési kereteit" nem rendezi, teljesen szabad kezet ad a tagállamoknak saját vitamegoldó fóru-

[39] Uo. 67. o.

[40] Uo. 68. o.

[41] *Ballesteros*: i. m. 100. o.

mainak kialakítására.[42]

A megfogalmazott kritikák figyelembevétele mellett ugyanakkor, kijelenthető, hogy az online vitarendezési platform létrehozásával és működtetésével sikerült mind a fogyasztók védelmét, mind a jogviták gördülékenyebb orvoslását egy magasabb szintre emelni, kihasználva a digitális fejlődés által nyújtott lehetőségeket. A jogviták megoldásának virtuális térbe költöztetésére annál is inkább szükség van, mivel a fiatal generációk felnőtté válásával, az online eszközök térnyerésével összhangban, a vitarendezések módja és az egyes vitarendezési eljárások igénybevétele is módosulni fog.[43]

Ugyanakkor az uniósjogalkotónak el kellene gondolkodnia egy olyan, a vizsgált rendelet által létrehozott platform hatályánál szélesebb körű, vitarendezési megoldás megteremtésén is, amely szintén online térben biztosítana megfelelő jogorvoslatot, ám a tagállami vitarendezési fórumok helyett egy újonnan létrehozott, közösségi szintű, teljes egészében online térben eljáró szerv igénybevételét feltételezné. A jelenleg elérhető platform az online vitarendezés pozitív fejlődési folyamatának egyik fontos állomása, ugyanakkor nem lehet annak csúcspontja.

[42] *Simon*: i. m. 77. o.

[43] *Malik*: i. m. 301. o.

Pohl Dóra Luca
joghallgató (PTE ÁJK), az ÓNSZ Bűnügyi Tagozatának tagja

Telegdy Blanka
joghallgató (PTE ÁJK), az ÓNSZ Bűnügyi Tagozatának tagja

Kiberbűncselekmények elleni küzdelem

I. Bevezetés

A XX. század második felében már csak egy lépés választotta el az emberiséget az ezredforduló legnagyobb technológiai innovációjától: az internettől.[1] A világháló feltalálása és kifejlesztése sok szempontból megkönnyítette életünket, hiszen a korábbi kommunikációs formákkal ellentétben elmondhatjuk, hogy gyorsabb, közvetlen adatátvitelre képes, mindezek mellett pedig használatával többoldalú, interaktív kapcsolatot tudnak megvalósítani a résztvevők,[2] azonban árnyoldalairól sem szabad megfeledkeznünk, amit a kiberbűncselekmények számának nagymértékű növekedése is jól mutat.

A bűnüldözés kezdetleges módszerei, valamint a társadalom védelmére való törekvés már a történelem korai időszakában megfigyelhetőek voltak,[3] majd az idő előrehaladtával a bűnüldöző szervek igyekeztek az adott kor elkövetési tendenciáihoz igazodni, mindazonáltal az elmúlt két évtizedben a technológiai fejlődés rohamosan felgyorsult, így a végbemenő változások eredményeképp olyan világméretű problémává vált az informatikai vagy más néven kiberbűnözés elleni küzdelem és annak szabályozása, hogy nem csak nemzeti, de uniós szinten is szükség van a jogalkotói és jogalkalmazói korszerűsítésre.[4]

Tanulmányunkban bemutatjuk a kibertér fogalmát és a kibertérben elkövetett bűncselekményeket, továbbá kitérünk az ezzel szembeni küzdelemre hazai és nemzet-

[1] *Kiss* Tibor: Kibervédelem a bűnügyi tudományokban. Dialóg Campus, Budapest 2020. 45. o.

[2] *Dornfeld* László: A bűncselekmények nyomozásának XXI. századi kihívásai. Különös tekintettel a kiberbűnözésre. Miskolci Egyetem 2015. 8. o.

[3] *Fenyvesi* Csaba: Az ősrobbanástól a modern kriminalisztikáig. A kriminalisztika alaptudományi és történeti vázlata. Magyar Rendészet 2016/4. sz. 16. o.

[4] *Gyaraki* Réka: A számítógépes bűnözés nyomozásának problémái. PhD értekezés. Pécs 2018. 8. o.

közi vonatkozásban.

II. Kibertér, kiberbűncselekmények

II.1. A kibertér definíciója

Annak érdekében, hogy foglalkozni tudjunk a kibertérben elkövetett bűncselekményekkel, mindenekelőtt meg kell értenünk a kibertér fogalmát, amit először William Gibson fogalmazott meg 1984-ben, Neuromancer című regényében.[5] Gibson szerint ez egy olyan világ, amit számítógép-hálózatok teremtettek és mesterséges intelligenciával rendelkező lények „lakják".[6] Tőle származik a „cyberspace" és a „cybercrime" kifejezés is, amelyek fordításait – a „kiberteret" és a „kiberbűnözést" – alkalmazzuk hazánkban. A kibertér elnevezést Gibson abból a célból alkotta meg, hogy megfelelő, tág körű értelmezéssel rendelkező kifejezést használhassunk egy olyan globális számítógépes hálózat vonatkozásában, amely összeköti az embereket, a számítógépeket és az információforrásokat.[7]

Fontos megjegyezni, hogy jelenleg nincs nemzetközileg elfogadott definíció a kibertér fogalmának megállapítására, [8] azonban Magyarországon 2013-ban megalkottak egy egységes fogalmat a Magyarország Nemzeti Kiberbiztonsági Stratégiája nevet viselő 1139/2013. számú kormányhatározatban, ami alapján „*a kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett.*"[9]

---

[5] *Mezei* Kitti: A kiberbűnözés szabályozási kihívásai a büntetőjogban. Ügyészek lapja 2019/4-5. sz. 21. o.

[6] *Berki* Gábor: Kiberháborúk, kiberkonfliktusok. Geopolitikai Tanács Közhasznú Alapítvány – Műhelymunkák 2016/1. sz. 248. o.

[7] *Mezei*: i. m. 21. o.

[8] Fréderick *Douzet*: A geopolitikai kibertér megértéséhez. In: A virtuális tér geopolitikája (szerk. *Pintér* István). Geopolitikai Tanács Közhasznú Alapítvány, Budapest 2016. 23. o.

[9] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III.21.) Korm. határozat. 2. o.

Ez tehát azt jelenti, hogy a kibertér a magyar szabályozás szerint nem foglalja magába azokat az önálló számítógépeket, amelyek nincsenek a hálózatba kötve, mert azok nem tartoznak bele az összekapcsolt elektronikus információs rendszerek és hálózatok összességébe, amik a kiberteret alkotják.[10]

Figyelembe kell vennünk azt is, hogy nem csak vezetékkel lehetséges az összekapcsolás, hanem vezeték nélkül is, így az elektromágneses spektrumokat szintén a kibertér részének kell tekintenünk. A vezeték nélküli összekapcsolások körébe sorolható például a mindenki által ismert Wi-Fi, valamint a mobilinternet is. [11]

II.2. A kiberbűncselekmények

II.2.1. A kiberbűncselekmények fogalma

A kiberbűncselekmény fogalmának meghatározásakor mindenekelőtt tisztában kell lennünk a bűncselekmény definíciójával, amit a magyar Büntető Törvénykönyv a következőképpen határoz meg: „4. § (1) Bűncselekmény az a szándékosan vagy – ha e törvény a gondatlan elkövetést is büntetni rendeli – gondatlanságból elkövetett cselekmény, amely veszélyes a társadalomra, és amelyre e törvény büntetés kiszabását rendeli.

(2) Társadalomra veszélyes cselekmény az a tevékenység vagy mulasztás, amely mások személyét vagy jogait, illetve Magyarország Alaptörvény szerinti társadalmi, gazdasági, állami rendjét sérti vagy veszélyezteti.

5. § A bűncselekmény bűntett vagy vétség. Bűntett az a szándékosan elkövetett bűncselekmény, amelyre e törvény kétévi szabadságvesztésnél súlyosabb büntetés kiszabását rendeli, minden más bűncselekmény vétség."[12]

A jogszabály szövegét értelmezve megállapítható, hogy három fogalmi elem megléte esetén nevezhetünk egy cselekményt bűncselekménynek. Tényállásszerűnek kell lennie, ami azt jelenti, hogy a Büntető Törvénykönyv büntetni rendeli; bűnös, tehát szándékos (az elkövető látja cselekménye következményeit és kívánja azok bekövetkezését) vagy gondatlan (cselekménye következményeit előre látja, de könnyelműen bízik

[10] *Dornfeld* László – *Keleti* Arthur – *Barsy* Miklós – *Kilin* Józsefné – *Berki* Gábor – *Pintér* István: Műhelymunkák. A virtuális tér geopolitikája. (szerk. *Pintér* István). Geopolitikai Tanács Közhasznú Alapítvány, 2016/1. szám, Budapest 2016 249. o.

[11] Uo.

[12] A Büntető Törvénykönyvrő szóló 2012. évi C. törvény 4. § (1) – (2) bekezdés; 5. §

azok elmaradásában, vagy azért nem látja előre, mert a tőle elvárható figyelmet vagy körültekintést elmulasztotta) az elkövetés módja; valamint jogellenes, a társadalomra veszélyes.[13] Ezeknek a fogalmi elemeknek a kiberbűncselekmények esetében is meg kell jelenniük azzal a kiegészítéssel, hogy a bűncselekmény elkövetéséhez eszközként használják a digitális hálózatot, vagy a cselekmény megvalósításának nélkülözhetetlen kelléke a kibertér.[14]

Összefoglalva tehát a kiberbűncselekmény kifejezést az alábbi módon tudjuk definiálni: olyan jogellenes cselekmény, amelyet számítógépen vagy számítógépes rendszer ellen, illetve ezek segítségével követnek el.[15]

II.2.2. A kiberbűncselekmények csoportosítása

A kiberbűncselekmények esetében fontos elhatárolnunk a számítógép mint eszköz ellen és a számítógépes rendszer ellen elkövetett bűncselekményeket. A számítógépre elkövetett fizikai támadás nem minősül kiberbűncselekménynek; ebben az esetben a lopás, rongálás stb. tényállása valósul meg, míg az utóbbi esetben az információs rendszer vagy az abban tárolt adatokkal összefüggésben elkövetett bűncselekmény már kibertámadásnak minősül.[16] Tanulmányunkban az utóbbi esettel foglalkozunk.

A kiberbűncselekmények két tágabb csoportra bonthatók: vannak olyan bűncselekmények, amelynek pusztán színtere a kibertér, valamint olyanok, amelyek kizárólag az informatikai rendszerhez és térhez köthetők.[17]

Az első kategóriába tartoznak az ún. „klasszikus" bűncselekmények, amik más módon, informatikai megoldások alkalmazása nélkül is elkövethetőek, azonban a végrehajtás helye vagy eszköze gyakran a kibertér. Ezeknek a jogellenes magatartásoknak a számítógépes környezet csupán új színtérként szolgál, egyfajta könnyebbséget, többletlehetőséget jelent. Jellemzően ilyen magatartásnak számít a rágalmazás, becsületsér-

[13] *Balogh* Ágnes – *Tóth* Mihály: Magyar Büntetőjog. Általános rész. Osiris Kiadó, Budapest 2015. 81. o.

[14] *Kiss*: i. m. 45. o.

[15] *Szász* Antónia: A kiberbűnözés társadalmi kontextusa. In: A normán innen és túl. (szerk. *Kovács* Janka – *Kökényessy* Zsófia – *Lászlófi* Viola). ELTE BTK Történeti Intézet, Budapest 2017. 95. o.

[16] *Gyaraki* Réka: A kiberbűncselekmények megjelenése és helyzete napjainkban. In. A bűnügyi tudományok és az informatika (szerk. *Mezei* Kitti). Budapest-Pécs 2019. 90. o.

[17] *Kiss*: i. m. 34–35. o.

tés, zaklatás, csalás, különböző titoksértések, gyermekpornográf felvétellel visszaélés, a dark weben való kábítószer- és fegyverkereskedelem lebonyolítása és egyéb hagyományos bűncselekmény, amelynek nem szükségszerű eleme a kibertér.[18]

Az utóbb említett csoportba tartozó deliktumokat tekintve az internetes hálózat a bűncselekmény megvalósulásának elengedhetetlen eszköze, tehát máshogy nem lehet megvalósítani ezeket a jogellenes magatartásokat, mert a bűncselekmény csak számítógépes rendszerek ellen követhetők el vagy jellegét tekintve kizárólag a kibertérben mehetnek végbe. Ez utóbbi kategóriára példa a *malware*, a *hacking* és a *social engineering*.[19]

A *maleware* a rosszindulatú számítógépes programok összefoglaló neve, ami magába foglalja a vírusokat, kémprogramokat, agresszív reklámprogramokat stb. Az előbbinél népszerűbb kifejezés, a *hacking* az elektronikus rendszerekbe történő jogtalan behatolást jelenti. A *hackinggel* szemben a *social engineering* esetében nem a programok állnak a cselekmény középpontjában, hanem az ember, mint a biztonsági rendszerek leggyengébb láncszeme, ugyanis az emberek megtévesztésével, kijátszásával történik a jogtalan információszerzés, illetve az információkhoz való jogosulatlan hozzáférés. A *social engineering* egyik gyakran alkalmazott módszere *phishing*, ismertebb nevén az adathalászat. A cél itt is abban áll, hogy az elkövető hozzáférjen a sértett(ek) adataihoz, amelynek érdekében különböző csalárd módszereket alkalmaznak: például valamilyen előnyt helyeznek kilátásba (valótlan nyereményjátékok, leárazások), vagy hátrány elkerülését teszik lehetővé (figyelmezteti a felhasználót, hogy adatai védelme érdekében cselekedjen), aminek következtében az üzenetek, hirdetések címzettje a valósnak hitt tartalom miatt egy rosszindulatú webhelyre kerül, ahol hozzáférnek adataihoz.[20]

II.2.3. A kiberbűncselekmények kiemelt veszélyessége

A kibertérben rejlő lehetőségek az egyszerű bűnelkövetőkön túl megfelelő táptalajt nyújtanak a szervezett bűnözés számára, továbbá a fejlett technikai eszközök kihasználásának köszönhetően csekélyebb az esély e csoportok felderítésére.[21]

Ha szervezett bűnelkövetésre gondolunk, fogalmi elemek között feltétlen szere-

[18] *Nagy*: i. m. 34. o.
[19] Uo. 35–36. o.
[20] Uo.
[21] *Gyaraki*: i. m. 85. o.

pelnie kell a nagyfokú rendszerezettségnek, és az átfogó tervezésnek, ezeket megfelelően biztosítja a szervezeten belüli lehető legnagyobb mértékű anonimitás. Az első és egyik legfontosabb előnynek tekinthető, hogy a világ pontjait összekötő internetes hálózatnak köszönhetően az elkövetőknek már nem kell fizikailag egy helyen tartózkodniuk, sőt, akár más országból, más kontinensről is szövetkezhetnek a bűnelkövetők a jogellenes magatartás véghezvitele céljából. A személyes találkozások mellőzése elősegíti a bűnszervezet tagjai között az egymással szembeni névtelenség megőrzését, ami nagymértékben megnehezíti vagy sok esetben ellehetetleníti a teljes szervezet felfedését.[22]

A szervezett bűnözésen belül fontos megjegyezni, hogy a technológiai fejlődés vívmányai a terroristáknak, a társadalom számára legnagyobb veszéllyel fenyegető elkövetői csoportnak is rendkívül kedveznek. A modernkori terrorfenyegetettség, a kiberterrorizmus két esetéről beszélhetünk: egyik az előbb említett forma, mikor kapcsolattartásra, szervezésre használják az információtechnológiát (az információtechnológia „*soft*" *típusú alkalmazása*), a másik mód pedig amikor kibertámadást hajtanak végre a terrorista csoportok („*hard*" *típusú alkalmazás*).[23]

Mindezek alapján megállapítható, hogy a kibertér a szervezett bűnelkövetők számára a kockázatvállalás minimális szintre csökkentését jelenti, aminek következtében igyekeznek minél szélesebb körben kihasználni a digitális közeg nyújtotta előnyöket.[24] E szempontokat figyelembe véve egyértelműen látszik, hogy a kiberbűncselekmények megfelelő szintű szabályozottsága és a bűnüldöző szervek összehangolt működése kulcsfontosságú szerepet játszik a kibertámadások ellen folytatott küzdelemben.

III. A kiberbűncselekmények elleni védelem

A kiberbűncselekmények elleni harcban nagy nehézséget okoz a kezdetektől megfigyelhető jelentős mértékű látencia. Általánosságban a bűncselekmények felderítése szempontjából kiemelten fontos, hogy a sértett(ek) észleljék az elkövetett cselekményt, valamint, hogy ez a bűnüldöző szervek tudomására jusson, azonban az FBI becslése szerint 95%-ban nem sikerül észlelni a jogellenes magatartást és a bűncselekmény felderítetlen

[22] Uo.

[23] *Bőczné* Neparáczki Anna Viktória: A kiberterrorizmus büntető anyagi jogi megítélése. Ügyészek lapja 2020/1. sz.

[24] *Gyaraki*: i. m. 85. o.

marad.[25] Ennek az is lehet az oka, hogy a sértettek sokszor nem veszik észre, hogy bűncselekmény áldozataivá váltak – például ha egy üzenet vagy e-mail olyan mértékben hasonlít az adott szervezet vagy magánszemély nevében küldött levélre, hogy megkülönböztetésük lehetetlen, vagy nagyfokú körültekintést igényel, könnyen előfordulhat, hogy a sértett érzékelése nélkül, jogellenesen tesznek szert az adataira–, így nem tudják jelezni a hatóságok felé. A látencia növekedését eredményezi az is, hogy ha tudomásukra is jut a sértetteknek a bűncselekmény, mégsem jelzik a hatóságok felé. Ez leginkább a nagy cégekre jellemző, ami érthető, hiszen nem remélnek túl nagy előnyt, ha a rendőrség tudomására hozzák, viszont az ügyfeleik számára gyengeségnek, esetleg megbízhatatlannak tűnhetnek, ha feltörik a számítógépes rendszerüket. Számos esetben a magánszemélyek sem fordulnak a nyomozó hatóságok felé, mert nem kívánnak egy (sok esetben) hosszadalmas eljárás résztvevőivé válni, hanem inkább igyekeznek maguk megoldást találni a problémára, ami nem minden esetben vezet célra.[26]

Véleményünk szerint a kibertérben elkövetett jogellenes magatartásokkal szembeni védelem két legfontosabb pillére az átfogó jogi szabályozás, valamint kiberbiztonsági szervek hatékony működése. Tanulmányunk további részében ezeket a tényezőket vizsgáljuk az Európai Unió vonatkozásában, azt követően pedig áttekintjük a magyarországi intézményrendszert.

III.1. Nemzetközi jogi aktusok és kiberbiztonsági szervezetek Európában

III.1.1. Jogi szabályozás

Az 1970-es évek végétől kezdődően egyre elterjedtebbé vált a számítógépek magáncélú felhasználása, majd az internet megjelenésétől megfigyelhető, hogy a kibertérben elkövetett deliktumok köre fokozatosan bővül, jellegük átalakul, amelynek következtében a jogalkotóknak reagálnia kell ezekre a változásokra. A kiberbűncselekményekkel kapcsolatos szabályozás jellegét tekintve lépcsőzetes: a megalkotott jogforrások – jellemzően ajánlások és irányelvek – a 80'-as évektől napjainkig egyre nagyobb mértékben fedik le az informatikai bűnözés témakörét. Kezdetben az Európa Tanács által elfogadott jogforrások alkották a nemzetközi szabályozás alapját, majd az Európai Unió létrejöttének következtében az uniós jogi aktusok kiegészítették, illetve továbbfejlesztették ezeket a

[25] Uo.
[26] Uo.

normákat.[27]

Az Európa Tanács 1981-ben kiadott ajánlása az első jelentős nemzetközi jogi aktus, ami érintette a kiberbűncselekmények témakörét, azonban mindössze három ilyen jellegű jogsértés található benne. Az 1989-es ajánlás ehhez képest már nagy fejlődést jelentett, mert felsorolt nyolc olyan informatikával kapcsolatos cselekményt, amit a jogalkotónak kriminalizálnia kellene. Ilyen volt például a *számítógépes csalás*, a *számítógépes hamisítás*, illetve az információtechnológiai rendszerekbe való *jogellenes behatolás*.[28]

A tisztán anyagi jogi szabályozási kísérleteket követően az ET 1995-ben újabb ajánlásában az anyagi jogon túl olyan büntető eljárásjogi kérdésekkel is foglalkozott, mint például a kutatás, a lefoglalás, jogorvoslat, valamint a nyomozó hatóságok és egyéb szervek kooperatív munkája.[29]

A 2001-ben megkötött *Számítógépes bűnözés elleni nemzetközi egyezmény* (más néven budapesti egyezmény) jelentette a kiberbűncselekmények nemzetközi szabályozásának következő lépcsőfokát, amit Magyarországon *az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről szóló 2004. évi LXXIX. törvényben* hirdettek ki. A progresszív jogforrás összefüggően kezelte a jogi problémákat és homogén értelmezést nyújtott egyes fogalmakkal kapcsolatban. Négy fő részre osztja a kiberbűncselekményeket:

- számítástechnikai rendszer és a számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekményekre,
- számítógéppel kapcsolatos bűncselekményekre,
- számítástechnikai adatok tartalmával kapcsolatos bűncselekményekre, valamint
- szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekményekre.[30]

[27] *Kiss*: i. m. 45. o.
[28] *Nagy*: i. m. 45–46. o.
[29] Uo. 46. o.
[30] Uo. 46–47. o.

Az Európai Unió egyik legjelentősebb kiberbiztonsági feladatokat ellátó szervét, a European Union Agency for Cybersecurity-t az Európai Tanács 2004/97/EK határozata alkotta meg, amelynek tevékenysége tanulmányunk következő szerkezeti egységében kerül bemutatásra.[31]

Az Európai Unió Tanácsa 2005-ben elfogadta az információs rendszerek elleni támadásról szóló 2005/222/IB kerethatározatot, amelyben a fogalommeghatározások és a szankciók mellett megfogalmazásra került, hogy minden tagállamnak meg kell hoznia a szükséges intézkedéseket annak érdekében, hogy a jogforrásban felsorolt három esetkörrel kapcsolatos magatartások „*legalább a jelentősebb esetekben bűncselekménynek minősüljenek*", valamint megállapítja a kötelezően alkalmazandó legkisebb büntetési tételeket. Az információs rendszerekhez való jogsértő hozzáféréssel, a rendszerbe való jogsértő beavatkozással és az adatokba való jogsértő beavatkozás vonatkozásában szólítja fel a tagállamokat, hogy valamilyen mértékben kriminalizálják az ezekkel kapcsolatos cselekményeket, továbbá kitér a felbujtás, a bűnrészesség, a bűnpártolás és a kísérlet kérdéskörére is.[32] Ezt a jelenséget *minimumharmonizációnak* nevezzük, aminek lényege, hogy oly módon megy végbe a jogharmonizációs folyamat, hogy az Unió felhívja tagállamait a legszükségesebb intézkedések megtételére (minimumszabályok alkotására), emellett azonban tiszteletben tartja azoknak az államoknak a jogi berendezkedését, akik szigorúbb normákat kívánnak alkalmazni.[33] Amint alább látni fogjuk, a 2005/222/IB kerethatározatot az Unió mára egy új irányelvvel váltotta fel, de jelentősége ettől függetlenül fennáll.

2009-ben az Európai Tanács által elfogadott stockholmi program meghatározta a 2010 és 2014 közötti időszakra vonatkozóan a jog érvényesülésén, a szabadságon és a biztonságon alapuló térségre vonatkozó stratégiai célkitűzéseket, valamint az ehhez szükséges lépéseket.[34] A program lényeg *a polgárokat szolgáló és védő, nyitott és biztonságos Európa* megteremtése volt, így fő prioritásként a határokon átívelő

[31] Uo. 48. o.

[32] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[33] *Mohay* Ágoston: Jogharmonizáció az Európai Unióban (oktatási segédanyag). NKE VTKI, Budapest 2016. 11. o.

[34] A Stockholmi Program. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Ajl0034 (2022. 05. 03.)

bűncselekmények felkutatása és szankcionálása került megfogalmazásra, aminek – az emberkereskedelem, a kábítószerrel kapcsolatos, a gazdasági és a nemi erkölcs elleni bűncselekményeken túl – részét képezte az informatikai bűnözés üldözése is.[35] A mérföldkőnek számító dokumentum többek között kiemelte, hogy az Unió jogközelítési folyamatában elengedhetetlen, hogy a tagállamok közös minimumszabályokat alkossanak mind a polgári jog, mind pedig a büntetőjog terén.[36]

A stockholmi program célkitűzéseinek következtében a fent említett 2005/222/IB kerethatározatban meghatározott minimumszabályokra vonatkozó követelmények további részletezésre kerültek az Európai Parlament és a Tanács által elfogadott információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról szóló 2013/40/EU irányelvben.[37] A kerethatározatban megjelenő jogellenes magatartások három csoportja mellett a 2013-as normában megjelenik egy negyedik eset is, a jogellenes adatszerzés, illetve a korábbi jogforráshoz képest további cikkekkel bővül a szabályozás, mint például a bűncselekmények elkövetéséhez használt eszközökről szóló cikk.[38]

Az előbbiekben felsorolt Európa Tanács és az uniós jogi aktusok mellett a kiberbűncselekmények elleni védelem korszerűsítésében a joggyakorlat, különféle kutatások, illetve az alább kifejtett szervek jelentései is nagy szerepet játszanak.

III.1.2. Kiberbiztonsági szervek

Az ENISA az Európai Unió Kiberbiztonsági Ügynöksége (European Union Agency for Cybersecurity), amelynek küldetése, hogy a szélesebb közösséggel együttműködve magas szintű, egységes kiberbiztonságot érjen el az Unió egész területén. Az ENISA hozzájárul az Európai Unió kiberpolitikájához; kiberbiztonsági tanúsítási rendszerekkel növeli az információ- és kommunikációtechnológia (IKT) termékek, szolgáltatások és folyamatok megbízhatóságát; együttműködik a tagállamokkal és az uniós szervekkel. Feladatai közül továbbá kiemelendő, hogy segíti Európát a jövő kiberkihívásaira való felkészülés-

[35] Uo.

[36] A Stockholmi Program – A polgárokat szolgáló és védő, nyitott és biztonságos Európa. (2010/C 115/01))

[37] *Nagy*: i. m. 48–49. o.

[38] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról.

ben.[39] Annak érdekében, hogy megerősítse az összekapcsolt gazdaságba vetett bizalmat, fokozza az Unió infrastruktúrájának ellenálló képességét a tudásmegosztás, a kapacitásépítés és a figyelemfelkeltés eszközeinek alkalmazásával együttműködik az érdekelt szervezeteikkel. Végső soron az ENISA hozzájárul Európa társadalmának és polgárainak digitális biztonságához.[40]

Legfőbb tevékenységei közé sorolható, hogy ösztönzi a tagállami, valamint az uniós kibervédelmi szerveket, hogy működésüket összehangoltan végezzék,[41] továbbá tájékoztatókat és gyakorlatokat tart, valamint megelőzi, kezeli és reflektál a kiberbűnözéssel kapcsolatos problémákra.[42] Az ENISA közös erőfeszítések egymást kiegészítő jellegének biztosítására törekszik azáltal, hogy hozzáadott értéket teremt az érdekelt feleknek, feltárja a szinergiákat és hatékonyan használja fel a korlátozott kiberbiztonsági szakértelmet és erőforrásokat.[43] Emellett tanácsadással segíti a tagállamokat.[44]

Hangsúlyozza, hogy a kiberbiztonságot az uniós politika minden területébe be kell ágyazni, az egyes ágazatok sajátosságainak figyelembevétele mellett. [45]

III.1.3. Europol

Hágában található meg a Bűnüldözési Együttműködési Európai Uniós Ügynöksége, amely 27 EU tagállamot, valamint több EU-n kívüli partnerállamot és nemzetközi szervezetet segít a bűnüldözésben. Legfőbb célja, hogy Európát biztonságosabbá tegye az uniós polgárok számára.[46]

Az Európai Unió egyik fő feladataként határozta meg a kiberbűnözők üldözését.

---

[39] ENISA https://www.enisa.europa.eu/ (2022. 04. 18.)

[40] Uo.

[41] Uo.

[42] *Nagy*: i. m. 48. o.

[43] ENISA https://www.enisa.europa.eu/ (2022. 04. 18.)

[44] Részletes leírás a Csirt – csoportok létrehozásáról. ENISA. 3. o. https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-hungarian/@@download/fullReport (2022.06.13.)

[45] ENISA https://www.enisa.europa.eu/ (2022. 04. 18.)

[46] Europol's highlights of 2021: A year in review. https://www.europol.europa.eu/media-press/newsroom/news/europol%E2%80%99s-highlights-of-2021-year-in-review (2022. 04. 18.)

Erre a célra szolgál a 2013-ban létrehozott Európai Számítástechnikai Bűnözés Elleni Központ (EC3). Az EC3 célja a hatóságok határozott fellépésének megerősítése a kiberbűnözés ellen, valamint az, hogy segítse az európai polgárok, kormányok és vállalkozások védelmét.[47]

III.1.4. Eurojust

Az Eurojust, az Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége, ahol a nemzeti igazságügyi hatóságok szorosan együttműködnek a határokon átnyúló bűnözés elleni küzdelemben. Az Eurojust szerepe, hogy segítse Európát biztonságosabb hellyé tenni azáltal, hogy összehangolja a nemzeti hatóságok – az EU-tagállamok és a harmadik államok – munkáját a nemzetközi bűnözés kivizsgálása és üldözése terén. Az Ügynökségbe minden részt vevő tagállam egy nemzeti tagot delegál, amely tagok alkotják az Eurojust Kollégiumát, amely az operatív munkáért felel.[48]

Tekintettel arra, hogy minden eset más és más, ebből kifolyólag pedig egyéni megközelítést igényel, az Eurojust fő tevékenységei közé tartozik, hogy segít a nyomozásban, azzal, hogy szakértelmét megosztja a társhatóságokkal. Az intézmény meghatározó eszközei közé tartoznak a koordinációs központok, a koordinációs találkozók és az EU igazságügyi együttműködési eszközei. Az Eurojust egyedi ügyeleti szolgáltatást is nyújt, amit igénybe vehetnek azok a nemzeti hatóságok, akiknek a gyanúsítottak gyors felkutatása és elfogása érdekében azonnal intézkedésre van szükségük.[49] Az Eurojust az Europol-lal együtt részt vehet közös nyomozócsoportok megalakításában azért, hogy a rendőrségi együttműködés tovább javuljon.[50]

Megállapítható, hogy az Eurojust a hatóságokkal együttműködve küzd az elé terjesztett, legalább két uniós tagállamot érintő, határokon átnyúló bűncselekmények széles köre ellen.[51] Az is előfordulhat, hogy egy bűncselekmény egy uniós és egy nem

[47] Cybercrime. https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime (2022. 04. 18.)

[48] Eurojust: Europen Union Agecy for Criminal Justice Cooperation. Who we are. https://www.eurojust.europa.eu/about-us/who-we-are (2022. 04. 18.)

[49] Eurojust: Europen Union Agecy for Criminal Justice Cooperation. How we do it. https://www.eurojust.europa.eu/about-us/how-we-do-it (2022. 04. 18.)

[50] Uo.

[51] Uo.

az unió tagállamai közé tartozó államot érint. Arra is volt már példa, amikor egyetlen tagállaman követték el a bűncselekményt, azonban annak következményei a határokon átíveltek.[52] Az Ügynökség irányítja a növekvő európai fenyegetésekre adott igazságügyi választ, lehetővé téve a tagálamok számára, hogy egy lépéssel a bűnüldözők előtt járjanak, elsősorban a szervezett bűnözői csoportokra összpontosítva.[53]

Az Eurojust akképp járul hozzá a kibertérben elkövetett bűncselekmények üldözéséhez, hogy az elektronikus bizonyítékokat összegyűjti és felhasználja. Az internet segítségével elkövetett bűncselekmények ellen bevált gyakorlatokat megosztja az államok hatóságaival.[54]

Szakértelmének és tapasztaltságának köszönhetően az országok az Eurojust felé fordulhatnak joghatósági összeütközések, kiadatás, bizonyítékok elfogadhatósága, vagy a vagyon befagyasztása és behajtása esetében. A gyakorlat azt mutatja, hogy minden megkeresésre gyorsan és eredményesen reagálnak.[55]

III.2. Kibervédelem Magyarországon

III.2.1. Jogi szabályozás

A hazai normákat illetően elsőként 1994-ben, a régi magyar Büntető Törvénykönyvben[56] tűnt fel egy, a kiberbűncselekmények körébe sorolható deliktum, ami a számítógépes csalás volt, azonban a tényállás rendkívül széles alkalmazási körrel rendelkezett.[57]

Az új Btk.[58] már három informatikai bűncselekményt szabályoz:

– az információs rendszer vagy adat megsértését,[59]

[52] Uo.

[53] Eurojust: Europen Union Agecy for Criminal Justice Cooperation. What we do. https://www.eurojust.europa.eu/about-us/what-we-do (2022. 04. 18.)

[54] *Dornfeld* László: A kiberbűncselekmények nyomozásával kapcsolatban folytatott uniós bűnügyi együttműködés fejlődése. Külügyi szemle. 2016/1. sz. 99. o.

[55] Eurojust: Europen Union Agecy for Criminal Justice Cooperation. How we do it. https://www.eurojust.europa.eu/about-us/how-we-do-it (2022. 04. 18.)

[56] A Büntető Törvénykönyvről szóló 1978. évi IV. törvény.

[57] *Nagy*: i. m. 50. o.

[58] A Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.)

[59] Btk. 423.§ (1)-(4) bekezdés

– az információs rendszer védelmét biztosító technikai intézkedés kijátszását,[60] valamint

– az információs rendszer felhasználásával elkövetett csalást.[61]

Az első két bűncselekmény a tiltott adatszerzés és az információs rendszer elleni bűncselekmények című fejezetben, míg az információs rendszer felhasználásával elkövetett csalás a gazdasági bűncselekmények című fejezetben helyezkedik el a kódexben.[62] Ezen tényállások az Európai Unió jogának való megfelelés miatt a 2013/40 EU parlamenti és tanácsi irányelv következtében került bele a hatályos magyar büntetőjogi kódexbe.[63] A tényállások jogi tárgya hasonló, mert mindegyik érinti az informatikai rendszerek zavartalan és biztonságos működését, azonban a harmadik bűncselekmény ezeken felül a vagyoni viszonyokat is védeni kívánja.[64]

Magyarország az Európai Unió tagállamaként köteles az Unió által megalkotott kötelező jogi aktusokat végrehajtani (illetve az irányelvek esetében: a nemzeti jogba implementálni), így a kiberbűncselekmények elleni védelem alapjául szolgáló jogforrások elsősorban az uniós szervek által kibocsátott rendeletek, határozatok, irányelvek, ajánlások vagy vélemények.[65]

III.2.2. Kibervédelmi szervek

A hazai kibervédelmi rendszer két fő szerkezeti egységből tevődik össze: a stratégia és az operatív szintből. A továbbiakban kifejtett intézményeket még kiegészítik egyéb speciális, a kibervédelem egyes részterületivel foglalkozó szervek. A kiberbiztonságért felelős szervezeti rendszer stratégiai szintje a Kiberbiztonsági Fórumból, a kiberkoordinátorból, továbbá az irányítása alatt álló munkacsoportokból áll.[66] A Kiberbiztonsági Fórum szakmai segítséget és támogatást nyújt, a munkacsoportok javaslatokat és véleményeket tesznek a Nemzeti Kiberbiztonsági Koordinációs Tanács felé, ami pedig

[60] Btk. 424.§ (1) bekezdés

[61] Btk. 375.§ (1)-(5) bekezdés

[62] Btk. XXXVI. Fejezet; XLIII. Fejezet

[63] Btk. 465. § (1) bekezdés f) pont

[64] *Nagy*: i. m. 50–58. o.

[65] Az Európai Unió hivatalos honlapja. https://ec.europa.eu/info/law/law-making-process/types-eu-law_hu (2022.04.18.)

[66] *Kiss*: i. m. 45. o.

az együttműködés mellett szabályozza, támogatja és egységes kormányzati álláspontot alakít ki a Nemzeti Biztonsági és Kiberbiztonsági Stratégia részére.[67]

A Nemzeti Kibervédelmi Intézet (NKI), a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (LRLIBEK), a Honvédelmi Minisztérium és az Információs Hivatal saját hálózatbiztonsági vészhelyzeteket elhárító csoportjai (Computer Emergency Response Team, a továbbiakban: CERT) sorolhatóak az operatív szint szervezetei közé. [68]

A központi helyet elfoglaló Nemzeti Kibervédelmi Intézeté a vezető szerep. Felépítését tekintve három szakmai részre osztható, ezek a Kormányzati Eseménykezelő Központ (GovCERT - Hungary), a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) és a Biztonságirányítási és Sérülékenységvizsgálati Osztály. Az előzőekben felsorolt szakterületek különböző feladatokat látnak el, míg a GovCERT a kibertámadásokkal és fenyegetettségekkel foglalkozik, addig a NEIH ellenőrzi, valamint érvényesíti a jogszabályi előírásokat. A Biztonságirányítási és Sérülékenységvizsgálati Osztály sérülékenységvizsgálatot, IT biztonsági tanácsadást végez, valamint EMIR/FAIR struktúrákkal kapcsolatos információtechnológiai biztonsági teendőket lát el.[69]

Az LRLIBEK tevékenységét az Ibtv., a 185/2015. (VII.13.) Korm. rendelet és az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, az információbiztonsági felügyelő feladat- és hatásköréről, valamint a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII.13.) Korm. rendelet által megállapított hatáskör és illetékesség szerint látja el. Tevékenységei közé tartozik az eseménykezelés, tájékoztatás nyújtása, valamint, hogy folyamatos ügyeletet tartson fent.[70]

A Honvédelmi Minisztérium a Katonai Nemzetbiztonsági Szolgálat keretében működő olyan szervezet, amely saját zárt és nyílt rendszerei számára biztosít kibervédelmet, emellett incidenskezelési és hatósági feladatokat is ellát. A szervezet szakfel-

[67] *Kovács* Zoltán: Kibervédelem és biztonság. In: Kibervédelem a bűnügyi tudományokban (szerk. Kiss Tibor) Dialóg Campus, Budapest 2020. 66. o.

[68] *Kovács*: i. m. 69. o.

[69] *Kovács*: i. m. 66–70. o.

[70] Uo. 76. o.

adatai szerint különíthető el. A honvédelemért felelős miniszter vezérlésével látják el a fenyegetések kezelését, az eseménykezelő központtal együttműködve. Az Információs Hivatal szintén független, saját szervezetén belül nyílt és zárt digitális információs rendszereit érintő védelmi események és fenyegetések kezelése érdekében működik.[71]

IV. Konkrét esetek napjainkban

A kibertérben számtalan kisebb-nagyobb bűncselekményt követnek el hazánkban[72] és külföldön egyaránt.[73] Ezek nagy részéről vélhetően nincs tudomásunk.[74] Tanulmányunk ebben a részében egy olyan esetet szeretnénk bemutatni, ami a közelmúltban történt az Egyesült Államokban az egyik leggyakoribb rosszindulatú program használatával.[75] Egy benzint, gázolajat, repülőgép-üzemanyagot és egyéb finomított kőolaj-származékokat szállító céget, a *Colonial Pipeline*t 2021-ben hackertámadás érte. Egy zsarolóvírussal támadták meg, amelynek következtében csaknem másfél milliárd forintértéknek megfelelő dollárt kellett váltságdíjként kifizetniük és csak ez után, egészen pontosan hat napra rá tudták újrakezdeni az üzemanyagvezeték-hálózat újraindítását.[76] A zsarolóvírus lényegében egy olyan kártékony szoftver, amelynek segítségével pénzt tudnak kicsikarni a megtámadott tulajdonostól. Ezt úgy tudják elérni, hogy a vírussal titkosítják az eszközön lévő adatokat, majd a képernyőn megjelenik egy követelést tartalmazó dokumentum vagy tartalom.[77]

Egy hazai példát is megemlítve, 2021. áprilisában egy nő tett bejelentést a rendőrségen, miszerint valaki az ő azonosítójával lépett be a gimnáziumok által használt

[71] Uo. 77. o.

[72] *Gyömbér* Béla: Hatalmasat nőtt a kiberbűncselekmények száma Magyarországon. Jogalappal. 2021. március 24. https://jogalappal.hu/hatalmasat-nott-a-kiberbucselekmenyek-szama-magyarorszagon/ (2022. 04. 15.)

[73] Európai Parlament: jelentés a kiberbűnözés elleni küzdelemről (2017/2068(INI)) https://www.europarl.europa.eu/doceo/document/A-8-2017-0272_HU.html (2022. 04. 18.)

[74] *Kiss*: i. m. 156. o.

[75] Alexander *Warschum*: Kiberbiztonság: hogyan védekezhetünk az adathalászattal és más veszélyekkel szemben. Unite. 2022. január 18. https://unite.eu/hu-hu/kozlemenyek/tortenetek-es-informaciok/kiberbiztonsag-hogyan-vedekezhetunk-az-adathalaszattal-es-mas-veszelyekkel-szemben (2022. 04. 24.)

[76] Kibertámadás áldozatok a közelmúltból. Marsh. https://www.marsh.com/hu/hu/services/cyber-risk/insights/kibertamadas-aldozatok-a-kozelmultbol.html (2022. 04. 17.)

[77] A zsarolóvírus. Hogyan védje meg számítógépét ezektől a kártékony szoftverektől? ESET Tudástár. https://www.eset.com/hu/zsarolovirus/ (2022. 04. 17.)

oktatási rendszerbe, a Krétába, emellett pedig az e-mail fiókját is feltörték. A rendőrségi nyomozás során, amely információs rendszer vagy adat megsértésének gyanúja miatt indult, kiderült, hogy egy adathalász játék megnyitásával kerültek az azonosítók a hacker birtokába. Az elkövető egy 13 éves fiú volt, aki az azonosító adatokat úgy szerezte meg, hogy az internetről letöltött egy nyílt forráskódú programot, majd az adathalász rendszerhez ő írta meg a program második részét.[78] Abból a célból választottuk ezt a hazai példát, hogy érzékeltessük, milyen egyszerűen el lehet követni egyes kiberbűncselekményeket.

V. Összegzés

A technika fejlődésének eredményeképpen napjaink egyik legégetőbb problémájává vált a kiberbűnözés elleni küzdelem és annak szabályozása, azonban a jog nem képes ilyen ütemben megújulni,[79] melynek következtében joghézagok alakulnak ki.

Láthattuk, hogy számtalan akadály gátolja a hatékony védekezést a kibertámadások ellen (nincs megfelelő jogi szabályozás, magas látencia, szervezett bűnözés, a bűnelkövetőket fejlett technikai eszközök segítik), azonban a jogalkotás folyamatosan fejlődik, újabb és újabb szervezetek jönnek létre, amelyek segítik felvenni a harcot az elkövetőkkel szemben, vagy éppen hozzájárulnak a védekezéshez, a felderítéshez és útmutatást adnak a hatékony szankcionáláshoz.

Számos, a kiberbűncselekmények elleni védekezést elősegítő uniós és hazai szerv működik, amelyek közül részletesebben foglalkoztunk az Europollal, Eurojusttal és az ENISA-val. Hazánkban a kibertérben elkövetett bűncselekmények megelőzését és felderítését végző szervek közül bemutattuk a Nemzeti Kibervédelmi Intézetet, a Nemzeti Elektronikus Információbiztonsági Hatóságot és a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központot. Áttekintettük a tevékenységüket, valamint, hogy hogyan járulnak hozzá a hatékony védelemhez a tagállamokat segítve.

---

[78] 13 éves magyar fiú volt a keresett hacker – íme a beszámoló. Infostart. 2021. augusztus 14. https://infostart.hu/bunugyek/2021/08/14/13-eves-magyar-fiu-volt-a-keresett-hacker-ime-a-beszamolo# (2022. 04. 15.)

[79] *Bőczné* Neparáczki Anna Viktória: A kiberterrorizmus büntető anyagi jogi megítélése. Ügyészek lapja 2020/1. sz.

Úgy gondoljuk, mi annyiban tudunk hozzájárulni a hatóságok munkájához, hogy ha kibertámadást észlelünk, azt mindenképpen jelentjük a rendőrségen, így a hatóságok ezen adatok segítségével elfoghatják az elkövetőt vagy elkövetőket.

Globális szinten az jelenthetné a megoldást, ha az ezzel foglalkozó intézmények megalkotnának egy azonos definíciót, és az abból következő szemlélettel igyekeznének egységesen fellépni a bűnözéssel szemben. Megállapíthatjuk, hogy a bűncselekmények számának növekedésével a nemzetközi együttműködés egyre nagyobb Európában, azonban amíg nincs megfelelő szintű egységes szabályozás, addig nem lesznek képesek megállítani a kibertérben elkövetett deliktumok ilyen nagy arányú emelkedését.[80]

[80] *Dornfeld* László: A kiberbűncselekmények szabályozásának története az Egyesült Államokban és Európában. Studia Iurisprudentiae Doctorandorum Miskolciensium – Miskolci Doktoranduszok Jogtudományi Tanulmányai. Miskolc 2015. 82. o.

Szentes Dalma
joghallgató (PTE ÁJK), Óriás Nándor Szakkollégium Elméleti-történeti Tagozatának tagja

A szuperintelligens robotok jogalanyiságának egyes kérdései a klasszikus magánjogi gondolkodás tükrében

„A mesterséges intelligencia az egyik olyan kivételes ügy, amely esetében a szabályozás terén proaktívnak, és nem reaktívnak kell lennünk. Mire reagálni kezdenénk, az már túl késő lenne…"[1]

– Elon Musk –

I. Bevezetés

A XXI. században a technológia már mindennapjaink alapvető részét képezi. Amiről az 1950-es években még csak álmodhattak a tudósok, az mára valóság lett. Az internetnek köszönhetően bármely kérdésünkre egy pillanat alatt választ kaphatunk, a munkahelyünkről irányíthatjuk a háztartási eszközeinket, s önvezető autók kényelmét élvezhetjük. A folyamatosan fejlődő technológia megköveteli az adekvát jogi szabályozást, így a jogalkotókra hárul a feladat, hogy a lehető leghamarabb megteremtsék a változásokra reagálni tudó jogszabályi hátteret.

A közeljövő nagy kihívása a mesterséges intelligenciával rendelkező robotok jogi helyzetének megoldása. E tanulmány célja, hogy jogelméleti és jogtörténeti aspektusból bemutassa a magánjogban elismert személyek rendszerét, valamint a római jog rabszolgákra vonatkozó szabályait, mint alternatív megoldást, amelyek a hatályos jogba való átültetésükkel alkalmazhatóak lehetnek a szuperintelligens robotok jogi személyiségének megalkotásakor.

[1] „*AI is a rare case where we need to be proactive about regulation instead of reactive. Because I think by the time we are reactive in AI regulation, it's too late…*" ld. James *Vincent*: Elon Musk says we need to regulate AI before it becomes a danger to humanity. The Verge. 2017. július 17. https://www.theverge.com/2017/7/17/15980954/elon-musk-ai-regulation-existential-threat (2022. 04. 22.)

II. A jogalanyiság kérdése

2016 márciusában a mesterséges intelligencia-kutatás mérföldkőhöz érkezett, amikor a Google AlphaGo nevű algoritmusa győzelmet aratott a Go táblajáték mestere, a dél-koreai Lee Sedol felett. A kutatókat is meglepte a játék kimenetele, hiszen korábban úgy kalkuláltak, hogy még hosszú évek munkája szükséges egy ilyen eredmény eléréséhez.[2] Mindez azt bizonyította, hogy a mesterséges intelligencia képes meghaladni az emberi teljesítményt és tudást.

A kiemelkedő intelligencia mellett, az ún. humanoid robotok külsőleg is tökéletes másai az embernek. Felmerülhet tehát az igény, hogy jogilag is rendezzük helyzetüket. Adódik a kérdés: eljuthat-e valaha arra a szintre a technológiai fejlődés, amely már nélkülözhetetlenné teszi, hogy a robotok jogi személyiséget kapjanak?

II.1. Személyek a polgári jogban

Ahhoz, hogy megoldást találjunk a robotok jogi megítélésére, mindenekelőtt át kell tekintenünk a magánjog[3] által elismert, jogi értelemben vett személyek rendszerét. Ehhez elsőként az ember mint természetes személy jogalanyiságának kialakulását vizsgálom, figyelemmel a történeti előképekre. Ezt követően rátérek a jogi személy magánjogi megítélésére, ismertetve az egyes iskolák elméleteit.

II.1.1. Az ember mint jogalany

A jogviszonyok legáltalánosabb alanya az ember mint természetes személy. A Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban Ptk.) deklarálja az ember jogképességét, vagyis olyan entitásnak ismeri el, amely jogokkal és kötelezettségekkel rendelkezik. Ez a képesség tehát minden embert megillet, kortól, nemtől, származástól, s bármilyen más tulajdonságtól függetlenül.

A társadalmi fejlődés során azonban voltak olyan periódusok, amikor a jogalanyiság nem volt mindenki számára egyenlő. A klasszikus római jogászok alaptételként

[2] Steven *Borowiec*: AlphaGo seals 4-1 victory over Go grandmaster Lee Sedol. The Guardian. 2016. március 15. https://www.theguardian.com/technology/2016/mar/15/googles-alphago-seals-4-1-victory-over-grandmaster-lee-sedol (2022. 04. 22.)

[3] Jelen tanulmányban a magánjog és a polgári jog kifejezéseket Lábady Tamás nyomán „*valóságos szinonimákként*" használom. ld. *Lábady* Tamás: A magánjog általános tana. Szent István Társulat, Budapest 2018. 26. o.

ugyan kimondták, hogy a szabadság mint természetes képesség minden embert megillet („*Libertas est naturalis facultas eius quod cique facere libet, nisi si quid vi aut iure prohibetur*"),[4] az ókori civilizációk mégis rendre különbséget tettek szabad és nem szabad ember között, sőt Rómában a nem és a családi állapot is meghatározó tényező volt a jogképesség tekintetében.[5] A római polgár lehetett hatalom alatt álló (*alieni iuris*) vagy hatalom alatt nem álló, tehát önjogú személy (*sui iuris*).[6] Ennek megfelelően alakultak gazdasági és személyi viszonyai is, mivel a hatalomalatti nem rendelkezhetett saját vagyonnal, jogi aktusát pedig sajátos „beszámítás" útján a felette hatalmat gyakorlónak kell tulajdonítani.[7] Hermann Vultejus, német jogtudós volt az első, aki különbséget tett *homo* (ember) és *persona*[8] (személy) között. Vultejus szerint minden emberi lény – jogállásától függetlenül – *homo*, *persona* azonban csak olyan ember lehet, aki polgári státusszal is rendelkezik.

A felvilágosodás eszmerendszerének központjában az ember „felszabadítása" állt, gondoljunk csak a francia forradalom jelszavaira (Szabadság, Egyenlőség, Testvériség). Az Emberi és Polgári Jogok Nyilatkozata kimondja: „*Minden ember szabadnak és jogokban egyenlőnek születik és marad; a társadalmi különbségek csakis a közösség szempontjából való hasznosságon alapulnak*", valamint minden embert megillető – természetes és elévülhetetlen – jognak tekinti a szabadságot, a tulajdonhoz és biztonsághoz való jogot, illetve a mindenkori hatalommal szembeni ellenállás jogát.[9] Az amerikai függetlenségi háború közepette megszületett Függetlenségi Nyilatkozatban ugyancsak ezeket az alapvető jogokat találjuk.

---

[4] Ld. Flor. D. 1, 5, 4 pr. *Bessenyő* András: Római magánjog. Dialóg Campus Kiadó, Budapest-Pécs 2010. 147. o.

[5] A jogképesség római jogi fogalmához ld. *Jusztinger* János – *Pókecz Kovács* Attila: A római személyi jog alapfogalmai. In: A római jog alapfogalmai (szerk. *Csoknya* Tünde Éva – *Jusztinger* János), Dialóg Campus Kiadó, Budapest-Pécs 2018. 39. o.

[6] *Bessenyő*: i. m. 148. o.

[7] Uo.

[8] A latin *persona* szó eredeti jelentése „álarc", majd „jellem, személyiség" volt. Kezdetben personának minősítettek minden embert, szabadot és rabszolgát, és a posztklasszikus korban kezdték a kifejezést kiváltképpen a szabadokra használni. ld. *Földi* András – *Hamza* Gábor: A római jog története és institúciói. Oktatáskutató és Fejlesztő Intézet, Budapest 2015. 203. o. Vö. Max *Kaser*: Das Römische Privatrecht I. Beck, München 1971. 271. o.; Max *Kaser* – Rolf *Knütel*: Römisches Privatrecht. Beck, München, 2014. 89. o.

9 Az Emberi és Polgári Jogok Nyilatkozata. https://mek.oszk.hu/00000/00056/html/228.htm (2022. 04. 22.)

System des heutigen römischen Rechts című művében Friedrich Carl von Savigny, a természetjog nagy gondolkodója is foglalkozott a jogalanyiság kérdésével.[10] Megállapítása gyakorlatilag megfelel a hatályos polgári jogi terminológiának: azt tekinti személynek, aki jogképességgel rendelkezik.[11] A jogképesség azonban nem elegendő ahhoz, hogy a személy jognyilatkozatokat tehessen és jogügyleteket köthessen, mindehhez cselekvőképességre is szüksége van. Ezzel a képességgel pedig az a nagykorú személy rendelkezik, aki megfelelő érzelmi és értelmi intelligenciával bír.

Láthatjuk, hogy hosszú folyamat eredményeként jutott el arra a szintre a polgári fejlődés, hogy a ma ismert és alkalmazott fogalmakat kialakítsa. Meg kell jegyeznünk azt is, hogy az emberként vagy személyként való elismerés nagyban függ a politikai-társadalmi berendezkedéstől is, elég akár a méhmagzat jogalanyisága körüli vitákra gondolnunk.[12]

II.1.2. A jogi személyek

A szuperintelligens robotok előtt talán a jogi személyek jogalanyisága volt az utolsó olyan kérdés, amely komoly fejtörést okozott a jogászoknak. A személy- és dologegyesülések azonban nem a modernkor jogának vívmányai, a római jogban már ismert volt a testület (*universitas personarium* vagy *collegium*) mint több természetes személynek egy közös célra alapított egyesülete, valamint az alapítvány (*universitas bonorum* vagy *corpus*), vagyis egy állandó célra lekötött vagyontömeg.[13]

A történeti előzmények ellenére egészen a XIX. századig kétséges volt a társulások jogi megítélése. Georg Friedrich Puchta[14] és Savigny[15] az ún. fikciós-elmélettel kívánta alátámasztani a jogi személyek jogba való beemelésének szükségességét. Puchta úgy vélte, a jogi személyek eszmei léttel bírnak, a személyiségük alanya pedig pusz-

[10] Friedrich Carl von *Savigny*: System des heutigen Römisches Rechts. Berlin, 1840.

[11] *Pólay* Elemér: A pandektisztika hatása a magyar magánjog tudományára. Szegedi József Attila Tudományegyetem Állam- és Jogtudományi Kar, Szeged 1976. 33. o.

[12] Ld. 64/1991. (XII. 17.) AB határozat, ABH 1991/297.

[13] *Marton* Géza: A római magánjog elemeinek tankönyve Institúciók. „Méliusz" Könyvkereskedés, Debrecen 1948. 75. o.

[14] Georg Friedrich *Puchta*: Pandekten. Leipzig 1838.

[15] Friedrich Carl von *Savigny*: Vom Beruf unserer Zeit von Gesetzgebung und Rechtswissenschaft. Heidelberg 1814. 32. o.

tán egy fogalom, amely vagy személyek egyesülete, vagy vagyon.[16] Savigny az elmélet magyarázataként visszautalt egy római jogból ismert fikcióra, amelyet abban az esetben alkalmaztak, ha a vidéki városok képviselői együtt, egy ember helyett jártak el.[17] A jogképesség ilyenkor nem az eljáró személyeket illette külön-külön, hanem a jogi célok szolgálatára létrejött új alanyt, a jogi személyt.

Teljesen újszerűnek számított Alois Brinz ún. célvagyon elmélete is, amely gyakorlatilag felváltotta a történeti iskola képviselőinek nézetét.[18] Brinz szerint a vagyon kétféle természetű, lehet egy személyé, vagy valamilyen célé: a jogi személyt ennek megfelelően nem személynek, hanem célvagyonnak kell tekinteni.[19]

A kánonjog erkölcsi személyként nevezte meg a jogi személyeket, azonban ezt Puchta és Savigny elvetendőnek tartotta, mivel a fikcióval létrejött egyesülés nem bírhat morális vonatkozásokkal.[20] Azért sem szerencsés ez a terminológia, mert azt a képzetet kelti, mintha a természetes személy ennek ellentéte, vagyis erkölcstelen lenne.

A realitás elmélet képviselője, Heinrich Dernburg tagadta a jogi személy fikciós megközelítését, s bizonyos mértékben inkább „kigondoltnak", realitásnak tartotta[21]. Dernburg (a jusztiniánuszi források alapján) kifejtette a jogi személy kritériumait is, amelyek később annak jogi kialakítása során alkalmazást is nyertek.[22]

A magyar jogtudósok közül érdemes megemlíteni Szászy-Schwarz Gusztávot[23] és Moór Gyulát,[24]akik ugyancsak kísérletet tettek a jogi személyek jogalanyiságának igazolására.

Az angolszász jogban – egészen egyszerű módon – visszavezették a jogi személyeket az őket alkotó természetes személyekre, és így e személyek váltak a jogi személy

[16] *Pólay*: i. m. 39. o.

[17] Uo.

[18] Alois *Brinz*: Lehrbuch der Pandekten. Erster Band. Erlangen 1873. 201-207. o.

[19] *Kecskés* László: Magyar Polgári Jog Általános Rész. II. A személyek joga. Dialóg Campus Kiadó, Budapest-Pécs 1999. 141. o.

[20] *Pólay*: i. m. 39. o.

[21] Heinrich *Dernburg*: Pandekten. Erster Band. Berlin, 1888. 135-136. o.

[22] *Pólay*: i. m. 60. o.

[23] Ld. *Szászy-Schwarz* Gusztáv: A jogi személy magyarázata. Franklin, Budapest 1907.

[24] Ld. *Moór* Gyula: A jogi személyek elmélete. Magyar Tudományos Akadémia, Budapest 1931.

jogainak és kötelezettségeinek „hordozóivá".[25]

A Ptk. 3:1. §-a egyértelművé teszi a természetes és jogi személyek közötti jogi különbséget: a jogi személyt jogképesnek kell tekinteni, azonban csak olyan jogokkal és kötelezettségekkel bírhat, amelyek jellegüknél fogva nem csak az emberhez kötődhetnek. Ennek megfelelően a jogi személy nem rendelkezik cselekvőképességgel, azt csupán képviselője biztosítja.

Láthatjuk, hogy a polgári jogban a jogképességtől függ a – jogi vagy természetes – személy minősége. A hatályos jog szabályai tehát nem teszik lehetővé a robotok, vagyis az ún. elektronikus személyek[26] ily módon történő elismerését. Visszanyúlva a „gyökerekhez", a továbbiakban kísérletet teszek annak megállapítására, hogy vajon alkalmazhatóak-e a mesterséges intelligenciával bíró humanoid robotokra a rabszolgák helyzetét rendező római jogi szabályok.

II.2. A római jog rabszolgákra vonatkozó szabályai alkalmazásának lehetősége a szuperintelligens humanoid robotok esetén

A római jog egyik alaptételének tekinthető, hogy „*servi res sunt*", vagyis a rabszolgák dolgok.[27] Ulpianus megállapításának ellenére a rabszolgák mégsem estek azonos megítélés alá más, közönséges dolgokkal. Ennek oka, hogy eredendően a patriarchális házközösség tagjai voltak, valamint a testi erejükön felül szellemi munkájukat, vállalkozó kedvüket is kihasználták a rabszolgatartók.[28] Ahogy Rómában a *dominus* használta rabszolgáit, úgy használja ma az ember a robotokat munkájának tehermentesítésére. E hasonlóságot alapul véve, kísérlem meg a rabszolgákra vonatkozó szabályok alkalmazását a humanoid robotokra.[29] Mindehhez elengedhetetlen a rabszolgaság mint különös jogi helyzet bemutatása, figyelmet fordítva annak keletkezésére és megszűnésének egyes eseteire is.

[25] *Rácz* Lilla: A személy és dolog fogalmának (lehetséges) változásai a mesterséges intelligencia és a kriptovaluták világában. Állam- és Jogtudomány 2020/4. sz. 91. o.

[26] Az angol e-person/i-person kifejezés magyar megfelelője.

[27] Ulp. 19, 1

[28] *Földi – Hamza*: i. m. 204. o.

[29] A római jogi szabályok „újbóli felhasználásnak" gondolata már az 1950-es években megjelent, napjainkban Ugo Pagallo olasz jogászprofesszor képviseli ezt az álláspontot. ld. Ugo *Pagallo*: Vital, Sophia, and Co.––The Quest for the Legal Personhood of Robots. Information 2018/9. sz. 230. 5-7. o. https://www.mdpi.com/2078-2489/9/9/230 (2022. 04. 25.)

II.2.1. A rabszolgaság keletkezése és megszűnése a római jogban

Ahogy az ember jogalanyisága kapcsán tett megállapításokból kitűnik, Rómában az emberek vagy szabadok (*liberi*), vagy rabszolgák (*servi*) voltak.[30] A rabszolgaság nem a római társadalom sajátja, minden népnél bevett volt a leigázott lakosság vagy a hadifoglyok ily módon való „hasznosítása". A római jog szerint több módja is volt a rabszolgaság keletkezésének. Fogságba ejtéssel elvesztette szabadságát a hadifogoly, és az az idegen, akinek állama Rómával nem állt szerződéses viszonyban, személye a *ius civile* alapján tehát szabad zsákmány tárgya volt.[31] Születésével rabszolgává lett a rabszolganő gyermeke. Létezett azonban egy különös szabály (a császárkorban), amelynek értelmében szabadnak születik annak a nőnek a gyermeke, aki a terhesség alatt akár egy pillanatra is szabad volt.[32] A *favor libertatis* elve szerint kétes esetben a szabadság szempontjából kedvező döntést kellett meghoznia a jogalkotónak. Láthatjuk, hogy a szabadság eszméje már a rómaiaknál is jelen volt, ezt fejezi ki a következő regula is: „*libertas omnibus rebus favorabilior est*", vagyis a szabadság olyan felbecsülhetetlen érték, amely minden másnál előbbre való.[33] Az ismertetett eseteken kívül, büntetésből is rabszolgává válhatott a tetten ért tolvaj vagy a fizetésképtelen adós is. Érdekes, hogy a régi civiljog szerint ezeket a rabszolgákat csak külföldre lehetett eladni, mert római földön római polgár nem lehetett rabszolga.[34]

A rabszolgaság megszüntetése klasszikusan felszabadítás (*manumissio*)[35] útján ment végbe. Ez történhetett színleges, ún. szabadságperrel[36] (*liberalis causa*), amely során a rabszolgáját felszabadítani kívánó úr pert indíttatott maga ellen egy bizalmasa (*assertor*) által. A prétor előtt megjelenve az *assertor* – rátévé pálcáját a rabszolgára – elmondta a *vindicatio* formuláját, amelyre az úr nem kontravindikált, hanem a rabszolgát körben megforgatva eleresztette, akit a prétor pedig szabadnak nyilvánított.[37] A felsza-

[30] Gai. 1,9

[31] *Marton:* i. m. 57. o.

[32] Marc. D. 1, 5, 5, 3

[33] Gai. D. 50, 17, 22

[34] *Marton:* i. m. 57. o.

[35] A *manumissio* irodalmához ld. Óriás Nándor: A manumissio. Tanulmány a római jogból. Eger 1929.

[36] A szabadságper eredetileg rendes perként is létezett annak eldöntésére, hogy valaki szabad-e vagy rabszolga ld. *Marton:* i. m. 58. o.

[37] *Marton:* i. m. 59. o.

badítás ezen kívül tipikusan végrendelet, valamint *census*-lajstromba való beíratás útján is történhetett. A császárkorban a rabszolgaság megszűnt a beteg, öreg rabszolga kitételével[38] is, vagy hitbizomány útján, ha a végrendelkező meghagyta örökösének, hogy a rabszolgát halála után szabadítsa fel.[39]

II.2.2. Elektronikus személyiség mint a *peculium* sajátos alkalmazása

Jogi tartalma szerint a rabszolgaság egy olyan állapot (helyesebben jogállás), amelyben a rabszolgát nem személynek, hanem dolognak tekintjük. Fontos hangsúlyozni a korábbiakra tekintettel, hogy a rabszolga – a szigorú szabályok ellenére – mégiscsak ember, aki dolog mivoltától függetlenül természetes személyiségnek (*persona servilis*)[40] is érezhette magát.[41] A rabszolga tehát több volt egy „tárgynál", ezt támasztja alá az is, hogy a felette gyakorolt tulajdonosi hatalmat nem a dologi jogban használt *dominium* mint tulajdonjog kifejezéssel illették, hanem rabszolgatartói hatalomnak (*dominica potestas*) nevezték.[42] A rabszolga ezenfelül részt vehetett a házi kultuszban, és sírhelye ugyanúgy *locus religiosus*nak minősült, mint a szabadoké.[43]

Érdemes megkísérelnünk e szabályok alkalmazását szuperintelligens robotokra. Ha elképzelünk egy emberi küllemmel és rendkívüli intelligenciával rendelkező humanoid robotot, kétségtelen, hogy a külseje ellenére biológiailag különbözik egy rabszolgától, hiszen valójában gép, semmiképp sem emberi lény. A rabszolga azonban nem személy, hanem dolog, vagyis jogi szempontból azonos megítélés alá tartozik, mint bármilyen más testi tárgy, amely fizikai hatalom alá hajtható. Láthatjuk, hogy a római jogi szabály e tekintetben jól illeszkedhet a robotokra,[44] hiszen tulajdonságaik folytán egyszerűen meg tudjuk ítélni, hogy személyek-e vagy dolgok.

2017 februárjában az Európai Parlament elfogadott egy állásfoglalást, amely-

[38] *Földi – Hamza*: i. m. 215. o.

[39] *Bessenyő*: i. m. 165.

[40] Ulp. D. 50, 17, 22

[41] *Marton*: i. m. 58. o.

[42] *Földi – Hamza*: i. m. 213.

[43] *Marton*: i. m. 58. o.

[44] Andreas *Nanos*: Roman slavery law: a competent answer of how to deal with strong Artificial Intelligence? Review of robot rights with view of Czech and German constitutional aw and law history. Prague Law Working Papers Series 2020/3. sz. 3. o.

ben a robotikára vonatkozó polgári jogi szabályokról szóló ajánlásokat fogalmazott meg. Felszólította a Bizottságot, hogy végezzen hatásvizsgálatot egy specifikus, kizárólag robotok számára megalkotott jogalanyiság bevezetésével kapcsolatban. Az állásfoglalás szerint a legkifinomultabb autonóm robotokat sajátos jogokkal és kötelezettségekkel kellene felruházni, amelyek segítségével elektronikus személyként önálló döntést hozva eljárhatnának harmadik felekkel való kapcsolatuk során.[45] Az ajánlást erős kritikával illette a szakma és a közvélemény is. Egyes vélemények szerint a robotok jogi személyiséggel való felruházása felerősítené a társadalom technológiától való félelmét, és nemes egyszerűséggel az emberi fajt is lefokozná a „gépek szintjére".[46] Ződi Zsolt szerint „nagyon nehezen látható be", hogy milyen hasznai lehetnek egy olyan konstrukciónak, amely a robotokat is jogok és kötelezettségek gyűjtőhelyeként kezelné, hasonlóan a jogi személyekhez. [47] A felelősség tekintetében ez felvet bizonyos problémákat: míg egy gazdasági társaság szankcionálása valóságos hátrányt okoz a társaságot alkotó személyeknek, addig a robotoknál erre nincs lehetőség, mivel a robotot nem személyek alkotják, illetve erőforrásainak elvonása nem feltétlenül okoz hátrányt az embernek. Udvary Sándor álláspontja szerint az elektronikus személyiség konstrukciója ebben a formában nem támogatható, mivel a nyugati-keresztény kultúra nem ismerheti el a robotok egyenlőségét, vagyis személyként jogalanyiságot kizárólag az ember kaphat.[48]

A római jog alkalmazott egy, az állásfoglalás ismertetett pontjához nagyban hasonlító szabályt, amely bizonyos értelemben korlátozott cselekvőképességet nyújtott a rabszolgáknak: a rabszolga jogcselekményeket végezhetett ura helyett, e szerződésekből azonban a *dominus* csak jogosítva volt, a kötelezettségek a rabszolgát terhelték (*delictum* elkövetése esetén azonban a kötelezettség az urára is kiterjedt).[49] A klasszikus kor római joga azonban vagyoni önállóságot is kínált a rabszolgáknak: különvagyont (*peculium*) kaphattak uruktól, amelyek keretében gazdálkodhattak, kereskedelmi tevékenysé-

[45] Ld. Az Európai Parlament 2017. február 16-i állásfoglalása a Bizottságnak szóló ajánlásokkal a robotikára vonatkozó polgári jogi szabályokról (2015/2103(INL))

[46] *Birher* Nándor – *Fábryné Keszler* Nikolett – *Kulifay* Bálint – *Regős* Franciska: A mesterséges intelligencia alkalmazásának társadalmi hatásai a normaalkotásra, jogi és erkölcsi szempontok alapján. Humán Innovációs Szemle 2019/1. sz. 9. o.

[47] *Ződi* Zsolt: Platformok, Robotok és a Jog. Új szabályozási kihívások az információs társadalomban. Gondolat, Budapest 2018. 191. o. 206. o.

[48] *Udvary* Sándor: Fémrabszolga vagy rivális életforma? A robotok jogi szabályozásának első lépései. Gazdaság és Jog 2018/12. sz. 17. o.

[49] *Marton*: i. m. 58. o.

get folytathattak (gyakran még saját rabszolgára is szert tehettek).[50] Ugo Pagallo, olasz jogászprofesszor vetette fel elsőként a *peculium* szabályának alkalmazását a robotokra, mivel a különvagyon tárgyaival a rabszolga jogalanyiság nélkül is rendelkezhetett.[51] A *peculium*mal kiküszöbölhető lehet az a probléma, amelyet Ződi Zsolt megfogalmazott a robotok felelősségének körében, mivel a peculium mint önálló erőforrás elvonható lehetne a robot károkozása esetén.[52]

Pagallo álláspontja szerint a robotok esetében elválasztható egymástól a jogi képviselet (*legal agenthood*) és a jogi személyiség (*legal personhood*).[53] Rácz Lilla dogmatikailag vitatja az elmélet helyességét, mivel a jogi képviselővé válás előfeltétele a jogi személlyé válás, amely viszont csak jogképességgel bíró személy esetében tételezhető fel. A lánc utolsó szeme pedig a cselekvőképesség mint a jognyilatkozatok megtételének képessége, csak jogképes személynél állhat fenn. Ha mégis megadnánk a cselekvőképességet jogképesség nélkül, akkor – Rácz Lilla értelmezésében – „*szemet hunynánk a dogmatikai engedékenység felett*".[54]

Álláspontom szerint az elektronikus személyiség kidolgozása a közeljövő egyik legégetőbb jogászi problémája, s a megoldás érdekében talán szükséges lesz a dogmatika áttörése, és a jogképesség-cselekvőképesség rugalmasabb szabályozása. Bár nagy nehézségek árán jutott el a jogtudomány arra a pontra, hogy jogképességgel ruházzon fel egyes gazdasági társulásokat, az évezredek tapasztalatai azt vetítik előre, hogy idővel képes lehet kompromisszumot kötni a robotok esetében is, ahogyan azt megtette a jogi személyek elismerése kapcsán is.

II.2.3. A ius patronatus és a mesterséges érzelmi intelligencia

Az utópisztikusnak tűnő jövőbe tekintve, tételezzük fel, hogy a humanoid robotok nem csak értelmi, de érzelmi intelligenciával is rendelkeznek majd. Mit is jelenthet mindez? Az értelmi intelligenciával bíró robot tudja magáról, hogy egy gép, amely arra hivatott,

[50] *Földi – Hamza*: i. m. 213. o.
[51] *Pagallo*: i. m. 5. o.
[52] *Ződi*: i. m. 206–207. o.
[53] *Pagallo*: 5–7. o.
[54] *Rácz*: i. m. 98. o.

hogy ellássa a tulajdonosa által rábízott feladatokat, kiszolgálja annak szükségleteit. Ha emellé érzelmi intelligencia is párosul, akkor a robot megérti, hogy nincs saját szabadsága, nem teheti azt, amit valóban szeretne, amire igazán vágyna. A mesterséges intelligencia e magas szintjén felmerülhet az igény arra, hogy tulajdonosától elszakadva önálló életet éljen. A robotok szabaddá bocsátása komoly veszélyeket is hordozhat magában. Meglátásom szerint a római jogban alkalmazott *ius patronatus* biztonságosabb alternatívát nyújthat egy ilyen szituáció esetén.

A *ius patronatus* esetében a rabszolga (ekkor már *libertus* vagy *libertinus*) kvázi félszabad jogállásúvá vált, mivel a felszabadítójával (*patronus*) továbbra is bizonyos bizalmi, függőségi viszonyban állt, amely jogokat és kötelezettségeket hozott létre mind a *libertinus*, mind a *patronus* számára. A felszabadított *patronus*a nevét viselhette, aki iránt tisztelettel és engedelmességgel tartozott. Bizonyos tiszteletbeli szolgálatokat (*operae officiales*) is teljesített a *patronus*nak, például kíséretet, ajándékokat. A *patronus* megbízása alapján más munkákat (*operae artificiales*) is köteles volt ellátni.[55] Ha a *patronus* elszegényedett, akkor *alimentatió*val tartozott, vagyis el kellett tartania őt, illetve a felszabadítónak örökjoga is fennállt a *libertinus* után.[56]

A *libertinus* számára is kedvező megoldást jelentett a *ius patronatus*, mivel a *patronus* köteles volt őt megvédeni, támogatni, szükség esetén pedig eltartani. A serdületlen vagy nőnemű felszabadított (*libertina*) a *patronus* gyámsága alatt állt.[57] A *patronus* jogai megszűntek, ha az említett kötelezettségeit nem teljesítette, vagy ha a *libertinus* császári privilégiummal elnyerte az „aranygyűrűk viselésének jogát" (*ius anulorum aureorum*)[58], amellyel már szabad születésűnek számított.[59]

A *ius patronatus* átvételével egy olyan viszony maradhat fenn a szuperintelligens gép és egykori tulajdonosa között, amely tartalmának köszönhetően részben megadja azt az önállóságot, amelyre a humanoid robotok vágynak, de egyfajta kontrollt is

[55] E szolgálatok ellátása mindennapos kötelezettséget jelentett a *libertinus* számára ld. Paul. D. 38, 1, 1

[56] *Földi – Hamza*: i. m. 216–217. o.

[57] *Marton*: i. m. 61. o.

[58] *Földi – Hamza*: i. m. 217. o.

[59] A rabszolgaszármazás hátrányos következményei – így a *patronus*i jogok – csak a császár által adományozott *restitutio natalium* által szűnhettek meg, éppen ezért annak adományozásához a *patronus* beleegyezése is szükséges volt ld. *Marton*: i. m. 63. o.

biztosítanak a „felszabadító" tulajdonosok számára. Fontos megjegyezni, hogy a római jog részletesebben nem szabályozta a jogviszonyt, így a jogok és kötelezettségek – legfőképpen a *libertinus*t terhelő munkák – mértéke a *patronus* választásától függött.[60] Ezt a diszpozitivitást fontosnak tartom a robot-tulajdonos viszonylatban is, mivel így a jogviszony dinamikáját a tulajdonos úgy alakíthatja, hogy az megfeleljen a robot szabadság iránti vágyának, mindvégig biztonságos keretek között tartva annak mértékét. A *ius patronatus* megfelelő működését szolgálja Comodus császár egyik rendelkezése is, amely szerint a *libertinus* visszakerülhetett *patronusa* hatalma alá, ha vele szemben goromba, durva magatartást tanúsított vagy ínségben magára hagyta.[61] A kötelezettségek megsértésének szankciói véleményem szerint alkalmasak arra, hogy a robotot és a tulajdonost is egyaránt arra sarkallják, hogy a jogviszony céljának megfelelően járjanak el, így a *ius patronatus* mint sajátos jogi megoldás iránymutatásként szolgálhat a jogalkotás számára.

Láthattuk, hogy a szuperintelligencia megjelenése a magánjog személyi rendszerének jelentős átdolgozását kívánja meg. Az Európai Parlament Jogi Bizottságának korábban említett kezdeményezése óta komoly előrelépés uniós szinten egyelőre nem történt az elektronikus személyek jogi elismerésének vonatkozásában. A Közel-Kelet azonban – meglepő módon – a mesterséges intelligencia-kutatások élén jár: elsőként Szaúd-Arábia adományozott állampolgárságot egy Sophia nevű humanoid robotnak,[62] 2017-ben pedig megalakult az első mesterséges intelligencia-ügyi minisztérium az Egyesült Arab Emirátusokban.[63]

III. Összegző gondolatok

E tanulmány mottóját Elon Musk amerikai mérnök-vállalkozótól választottam, aki a mesterséges intelligencia-kutatások egyik legaktívabb támogatója. Musk szerint a jognak mindig meg kell előznie a technológia eredményeit, hogy adott ponton biztosítani tudja az adekvát jogszabályi hátteret. Ehhez elengedhetetlennek tartom a jogászok és a kutatók közötti kooperációt, mert a robotikát érintő kérdések olyan természetűek,

[60] *Földi – Hamza*: i. m. 217. o.

[61] Mod. D. 25, 3, 6, 1

[62] *Birher – Fábryné Keszler – Kulifay – Regős*: i. m. 13. o.

[63] *Pokker* Zoltán Péter: A mesterséges intelligenciával rendelkező robotok jogi szabályozása, különös tekintettel az élethez való jog sérelmére. In: Acta Universitatis Szegediensis Forum Publicationes Discipulorum Iurisprudentiae, Szeged 2019. 325. o.

amelyekre a jog nem tud megfelelő választ adni technológiai szakértelem hiányában.

Az új jogi megoldások kialakítása mellett, azonban érdemes olykor visszatekinteni, és „ihletet meríteni" a múltban alkalmazott normákból. Jelen tanulmányban éppen ezért a klasszikus magánjog rendszeréből kiindulva vizsgáltam a mesterséges intelligenciát, mint a XXI. század egyik legnagyobb jogi kihívását. Az ember jogképességét igyekeztem jogelméleti szempontból is megközelíteni, tekintettel a felvilágosodás eszmeiségére, a jogi személyek kapcsán pedig olyan jogtudósok teóriáit mutattam be, akik munkásságukkal mai napig hatást gyakorolnak a magánjogra. Hangsúlyozandó, hogy a XIX. században éppoly megoldhatatlannak tűnő feladatként tekintettek a személy- és vagyonösszességek jogba való beemelésére, mint napjaink jogászai a szuperintelligens robotok jogalanyiságának kialakítására. Hiszem, hogy a technológia és a jog összhangjának megteremtésével a jogtudomány képes lesz átlendülni a nehézségeken.

Az elektronikus jogi személyiséget a római jog felől közelítettem meg: igyekeztem rámutatni arra, hogy a rabszolgákra vonatkozó szabályok érdemesek arra, hogy alapként szolgáljanak a mesterséges intelligenciával bíró robotok jogi helyzetének rendezésekor. A *ius patronatus* mint sajátos jogállást biztosító bizalmi viszony recipiálására valószínűleg csak a távoli jövőben kerülhet sor. A jognak azonban mindig több lépéssel a technológia előtt kell járnia, így talán érdemes ezt az alternatívát is a jogalkotó figyelmébe ajánlani.

Vajon a jog megfelelően reagál a technológiai kihívásokra? Vajon a jogi eszközök mennyiben befolyásolják társadalmunk digitalizációhoz fűződő kapcsolatát? Egy hagyományokra épülő tudományág mennyiben fér meg egy innovációra szomjazó és rohamosan fejlődő területtel?

Az Óriás Nándor Szakkollégium és a Collegium Iuridicum Szakkollégium szakkollégistái által megírt tanulmányok erre keresik a választ. A Nemzeti Tehetségprogram Pályázat keretében támogatott kötetben betekintést nyerhetünk többek között a robotjog római jogra visszavezethető alapköveibe, a kiberbűncselekmények magyar és román szabályozásába, az online vitarendezés új lehetőségeibe, emellett a félvezető autók iparjogvédelmi és személyjogi kérdéseibe, illetve az okosotthonok adatvédelmi és energiajogi kihívásaiba.

Készült az Emberi Erőforrások NTP-SZKOLL-21-0018. sz. Nemzeti Tehetség Program pályázat keretében.