BŰNÖZÉS AZ INFORMÁCIÓS TÁRSADALOMBAN

Alkotmányos büntetőjogi dilemmák az információs társadalomban

Doktori értekezés

Szerző: Szathmáry Zoltán

Témavezető: Balogh Zsolt György

Pécsi Tudományegyetem

Állam-és Jogtudományi Kar Doktori Iskolája

„Informatikai és Kommunikációs Jog" Program

Budapest

2012.

„Hajt az idő gyorsan - rendes útján eljár –

Ha felűlünk, felvesz, ha maradunk, nem vár;”

/Arany János: Toldi estéje/

TARTALOMJEGYZÉK:

BEVEZETÉS: A KUTATÁSI FELADATOK ÉS A VIZSGÁLAT MÓDSZERE

1. AZ ÉRTEKEZÉS TÁRGYA

Az információs társadalom által életre hívott új életviszonyok változásainak vizsgálata számos jogterület képviselőinek aktuális kutatási tárgya, nincs ez másként a büntetőjogászok esetén sem. A büntetőjog számára is időszerű kihívásként merült fel annak megválaszolása, hogy miként hatott a kiérlelt alapelvekkel, szilárd dogmatikával rendelkező büntetőjogi jogalkotásra és jogalkalmazásra a szabályozási környezet változása, és milyen újabb kihívásokat támaszt feléjük az információs társadalom töretlen fejlődése. A kutatás középpontjában tehát egy, a változó információs társadalom és az alapvetően merev büntetőjogi jogszabály- és intézményrendszer feszültsége áll. A témaválasztás indokát az adja, hogy az igazságszolgáltatás egyre többször találja magát szembe olyan élethelyzetekkel, amelyek helyes megítélésére vagy nem áll rendelkezésére kialakult rutin, gyakorlat, vagy jogérzéke azt sugallja, hogy a jogalkotó által megteremtett jogszabályi és intézményi környezet nem koherens, nem alkalmazható.

Feltételezhető, hogy az anomáliák okai nem feltétlenül és nem kizárólag a hibás jogalkotói döntések között keresendők, hanem az információs társadalommal együtt megjelenő új jelenségek eleve magukban hordozzák a büntetőjogi szabályozási minták alkalmazhatatlanságának lehetőségét. Amennyiben az információs társadalom a társadalmi együttélés minőségileg új formájának tekinthető – vagy legalábbis rendelkezik újszerű jegyekkel –, úgy a változás gazdasági, társadalmi és kulturális hullámai is szükségszerűen új társadalmi viszonyokat, értékeket, érdekeket, valamint azokat sértő új jellegű devianciákat termelnek ki. Az új devianciák közül a számítástechnikai eszközökkel érintett bűncselekmények szabályozása a korábbi minták hiányában gyakran nem megfelelően kiérlelt, a büntetőjogi dogmatika a legújabb kori, kommunikációs forradalom előtti fogalomkészletével és alapelveivel nem minden esetben képes megfelelően kezelni az egyes bűncselekményeket, ami gyakran vezet a büntetőjogi értékek feloldásához.[1]

Mivel a büntetőjog a jogrendszer szankciós zárköve, ekként feladata nem a társadalmi viszonyok fejlesztése, hanem a már kialakult értékrend védelme, ezért ebben a tekintetben alapvetően konzerváló gondolkodásmód jellemzi. Az sem szorul bővebb magyarázatra, hogy a jogalkotás büntetőjogi válaszlépései reflexióként, egy-egy nem kívánatos magatartáshoz képest mindig utólagosan, lemaradva jelennek meg. Mindez helyesen van így, ha a válaszadás megfontoltan, a várható hatásokra figyelemmel, a védendő értékekre vonatkozó szabályrendszerhez igazodva történik. Azonban egy eddig soha nem látott ütemben változó környezet büntetőjogi szabályozása esetén ennél többre van szükség, mégpedig előretekintésre. A jövőbe tekintés elmulasztása elkerülhetetlenül vonja maga után a lassan születő büntetőjogi rendelkezések alkalmazhatatlanságát, halálra ítélve a legjobb szándékú törekvéseket is, hiszen a jelen és a közelmúlt történéseire adott büntetőjogi válaszok rövid időn belül igazításra, kiterjesztő értelmezésre szorulhatnak, azaz a jogbiztonságot veszélyeztető jogalkalmazói műveletek áldozatává válhatnak.

Amennyiben tehát az információs társadalom által a büntetőjogi gondolkodás felé támasztott kihívásoknak kívánunk megfelelni, nem vonatkoztathatunk el magától a „változás" elemétől. Ahhoz, hogy a büntetőjogi dogmatika, az alkotmányos büntetőjog értékeit megőrizni, sőt bővíteni lehessen, ismerni kell a fejlődés folyamatát, azaz eredőjét a

[1] A továbbiakban a „büntetőjog" kifejezés tágabb értelmű alkalmazása indokolt, az anyagi jogi szabályok mellett felöleli a büntető eljárási jog és a büntetés-végrehajtási jog rendszerét is.

múltban, a jövőbe mutató irányát, valamint a haladás motorját. Utóbbi tényező nem más, mint maga a technológiai fejlődés, a szellemi tőke, az innovatív gondolkodás, amely újabb, praktikusabb, használhatóbb, a kitűzött céloknak mind jobban megfelelő termékek és szolgáltatások teremtésére törekszik. A fejlődés történelmi alapelemének tekinthető számítógép megjelenésétől kiindulva a számítástechnika tömegtermékké válásával, majd az eszközök mindent körbevevő hálózatba kötésével ma már a virtuális világ születésének lehetünk a tanúi. E változás eredményeként a szabályozandó élettér idővel megkettőződik, és a fizikai világ olyan életszférával egészül ki, amely a pontos korlátokat igénylő büntetőjog fogalmi és alkalmazási kereteit szétfeszíti.

A megfelelő büntetőjogi tényállások megalkotása azonban önmagában még nem elegendő. A kellően rugalmas, a jogbiztonságnak mégis megfelelő jogszabályok kidolgozása mit sem ér, ha azok érvényesítése elbukik a nemzetközi büntetőjogi együttműködés vagy a bűnüldöző szervek felkészültségének hiánya emelte akadályokon. Ezen probléma megoldása viszont elvezethet a számítástechnikai bűnözés tárgyalása kapcsán kezdetektől fogva felmerülő problémakörhöz, a hatékony bűnüldözés, az állami szuverenitás és az internet, a virtuális világ feszültségéhez, amelynek a feloldására törekvő megoldások már nem csak büntetőjogi szempontból tekinthetők aggályosnak.

Az eddig érintőlegesen vázolt problémák után a következő kérdésekre keresendő a válasz: Miként adható helyes válasz az információs társadalom társadalmi és gazdasági rendet sértő cselekményeire? A hatályos magyar büntetőjogi jogszabályok adta válaszok megfelelnek-e a magyar alkotmányos büntetőjog elveinek? Az értekezés ezekre a kérdésekre keresi a választ abból kiindulva, hogy az alapelvek maradéktalan érvényesülését kizárólag úgy lehet biztosítani, ha a számítástechnikai eszközökkel érintett bűncselekmények szabályozását a maguk önálló alapjaiból építkezve, a találkozó tudományterületek által alkalmazott fogalmak segítségével próbáljuk a büntetőjogi alapelvekkel összeegyeztethetővé tenni.

2. AZ ÉRTEKEZÉS FELÉPÍTÉSE

Az előfeltevések igazolásához elsőként az elemzés tárgyát képező szabályozási környezet, az információs társadalom és új típusú bűnözésének jellemzése, bemutatása szükséges, mégpedig annak folyamatában – tehát kezdeti, jelenlegi és várható állapotát is figyelembe véve –, amelynek során azonosítani célszerű valamennyi tényezőt, amely befolyásolhatja a változás irányát és jellegét. Ezt követően kell elhelyezni jelenlegi státuszunkat, megmásíthatatlan elveinket a már körvonalazott rendszerben és kijelölnünk a fejlődés irányát, tekintettel a már folyamatban lévő jogalkotási törekvésekre is. A vizsgálat ezen szakaszában nyílik lehetőség a szabályozandó környezet változásainak és a jogalkotás, illetőleg jogalkalmazás reakcióinak összevetésére, igazolva utóbbiak alkalmasságát vagy alkalmatlanságát. Végül a megszerzett ismeretek alapján a változásokkal együtt élő szabályozás kialakítását szem előtt tartó javaslatok kidolgozása következhet.

A fenti szempontok figyelembevétele miatt az értekezés szerkezete – hasonlóan a magyar büntetőtörvény felépítéséhez – alapvetően két fő részből, egy rövidebb „általános” és egy terjedelmesebb „különös részből” áll.

Az általános rész tárgya az infokommunikációs technológiával érintett bűncselekmények szabályozási környezetének, az információs társadalom és fejlődésének, várható jövőképének vizsgálata főként technológiai megközelítés alapján, valamint mindezek büntetőjogi szabályozás szempontjából lényeges aspektusainak a meghatározása. Ennek

keretében kerül sor az információs társadalom új típusú devianciáinak, azok ösztönzőinek, lehetséges okainak bemutatására is abból a célból, hogy minél érzékletesebb kép születhessen a technológiával érintett társadalmi változásokról. Mivel az információs társadalom bűncselekményeinek elemzése többszörösen interdiszciplináris területen történik, az érintett alkotmányjogi alapok ismertetését követően, a későbbi specializált vizsgálatok megalapozása érdekében egyfajta fogalmi rendszerezés is indokolt a nemzetközi elvárásokra figyelemmel. Az első, általános rész feladata tehát a szabályozandó környezet elemzése, az alkotmányos büntetőjogi elvárások kidolgozása, valamint az infokommunikációs eszközökkel érintett bűncselekmények dogmatikájának megalapozása.

Az értekezés második része három bűncselekményi tényállás dogmatikai elemzésének és alkalmazásának részleteit öleli fel, kifejezetten azon cél által vezérelve, hogy felfedje a kriminalizáció szülte anomáliákat. Joggal merül fel a kérdés, hogy miért éppen a három bűncselekmény vizsgálatára kerül sor, hiszen hiba volna azt feltételezni, hogy más, informatikai vonatkozással bíró bűncselekmény szabályozása ne rendelkezne valamely dogmatikai vagy eljárási defektussal. Az el nem hanyagolható terjedelmi korlátok mellett a meghatározott bűncselekményekre eső választás első oka, hogy a számítástechnikával érintett bűncselekmények közül elsősorban olyan deliktumok vizsgálata indokolt, amelyek a lehetséges legjellemzőbb szabályozási anomáliákat vetik fel. Másrészt – figyelemmel az információs társadalom egyik kulcsfogalmára, a távközlés, a számítástechnika és a tartalomszolgáltatás összefonódását jelölő konvergenciára – célszerű egy, magát a számítástechnikai infrastruktúrát támadó *(számítástechnikai jelleg)*, egy a számítástechnikai rendszereket eszközként igénybe vevő *(távközlési jelleg)*, és egy a rendszeren közvetített tartalmak vonatkozásában *(a közvetített tartalom jelleg)* felmerülő bűncselekmény szabályozásának elemzése. A választás mellett szólt továbbá az Európai Közösségek Bizottságának a számítógépes bűnözés elleni küzdelemre vonatkozó általános politikáról kiadott közleménye is, amely a számítógépes bűnözésnek alapvetően e három megközelítési módját emelte ki.[2] Az említett szempontok alapján az egyik legtöbb kritikát elszenvedő deliktumok, a szerzői jogi *tartalmat* érintő bűncselekmények (Btk. 329/A. és 329/B. §), továbbá a számítástechnikai *infrastruktúrát* sértő számítástechnikai bűncselekmények (Btk. 300/C. és 300/E. §), valamint az infokommunikációs technológia *eszközként* való felhasználásával járó fiatal bűncselekmény, a zaklatás (Btk. 176/A. §) vizsgálata célszerű. Az anyagi jogi szabályozás mellett a „különös rész" kitér az eljárásjogi szabályozás és a nemzetközi bűnügyi együttműködés egyes kérdéseire is.

Hangsúlyozni kell továbbá, hogy az értekezés tárgya az információs társadalom fent említett bűncselekményeire adott jogalkotói és jogalkalmazói válaszok alkotmányos büntetőjognak való megfelelésének vizsgálata. Ekként az egyébként szerteágazó témakör szorosan behatárolt, az elemzésen kívül maradnak az egyes bűncselekményekhez egyébként köthető, egyéb büntetőjogi diskurzusok tárgyát képező, de alkotmányos büntetőjogi relevanciával nem rendelkező problémakörök. Az értekezésnek tehát nem célja az információs társadalom bűnözésének globális vizsgálata.

3. A VIZSGÁLAT MÓDSZERE

Az információs társadalom bűncselekményeinek elemzése több szempontból is interdiszciplináris kérdésnek tekinthető egyrészt az informatika és a jogtudomány, másrészt utóbbin belül is a polgári jog, a szerzői jog, a büntetőjog valamint az

[2] COM(2007) 267 végleges.

alkotmányjog találkozása okán. Az értekezés vizsgálódásai éppen ezért több irányból, a felsorolt tudományterületek fogalmainak és kutatási eredményeinek feldolgozása révén közelítik meg az információs táradalom bűnözésének az alkotmányos büntetőjogra kiható jellemzőit.

Az alkotmányos büntetőjog és az információs társadalom egymásnak feszülésének kontextusában a vizsgálat alapvetően a hatályos magyar joganyag értelmezésével, valamint a jogalkalmazási anomáliákra figyelemmel az ügyészi és bírói döntések gyakorlati tapasztalatainak bemutatásával történik. Az értekezés tárgyának különleges volta okán a vizsgálat csak a szükséges mértékben tér ki a külföldi jogi minták feldolgozására – azaz a dolgozatot elsősorban nem az összehasonlító módszer jellemzi –, hiszen az alkotmányos büntetőjog érték- és szabályrendszere nyilvánvalóan a magyar alaptörvényhez kötött, annak értelmezése és az információs táradalom büntetőjogra kiható jellemzőinek kiemelése javarészt a magyar információs társadalmi átalakulás keretében képzelhető el. Amennyiben viszont az értekezés célkitűzése engedi, a vizsgálat során a rendelkezésre álló hazai és – a korábbi tapasztalataik okán megfelelő példaként szolgáló – angolszász szakirodalom feldolgozására is sor kerül.

ÁLTALÁNOS RÉSZ

TARTALOM:

I. FEJEZET: AZ INFORMÁCIÓS TÁRSADALOM

1. AZ INFORMÁCIÓS TÁRSADALOM BÜNTETŐJOGI ASPEKTUSAI

Mivel maga az információs társadalom nem tekinthető egzakt fogalomnak, ekként definiálásához, tartalmának kibontásához is számos megközelítési mód lehetséges. Az „információs társadalom" szószerkezete – a mai értelemben használt összefüggésben – az 1960-as évek japán *társadalomtudományi* diskurzusaiban jelent meg először, majd újabb és újabb értelmezési szintekkel gazdagodott.[3] A tudományos diskurzusokon kívül az információs társadalom kifejezéssel a mindennapokban sokszor inkább a *technológiai forradalom*-mal, *politikai* és *gazdasági programokkal* összefüggésben találkozhatunk, míg jelentésének megragadása, vagy éppen jövőbeli kialakításának tervezése számos tudományterület, és különböző szintű (nemzeti, regionális, globális) politikai fórum aktuális vitáinak középpontja.

Ezért alapvetően más-más szempontok szerint közelít a fogalomhoz az informatika, az antropológia, a szociológia, a politikatudomány és a jogtudomány. Lévén, hogy az információs társadalom különböző okokból képezi az említett területek képviselőinek vizsgálati tárgyát, és sokszor még csak nem is egységes fogalomkészlettel dolgoznak, abban sem értenek egyet, hogy az élet mely területén tekinthető a változás olyan mértékűnek, hogy azzal az egész társadalmat jellemezni lehessen, feltéve hogy maga az információs társadalom valóban rendelkezik egyáltalán a korábbiakhoz képest újfajta minőséggel.

Mindezek miatt eltérő absztrakciós szintű és változó alkalmazhatósággal bíró koncepciók születtek az információs társadalom bemutatására. Az információs társadalom kezelhető képének keresését tovább bonyolítja az egyes teóriák által vizsgált társadalmi-technológiai állapotok időtényezője, azaz a fejlődés maga, amelynek eredményeképpen az információs társadalomra vonatkozó koncepciók a vizsgált korszakok szempontjából is eltérők.

Hogyan közelítsen az információs társadalomhoz a büntetőjogász? Egy jogág a hasonló életviszonyok szabályozására létrehozott jogforrások és dogmatika koherens rendszere. *Simon Éva* szerint[4] az információs társadalom joga tág értelemben mindazokat a szabályozott élethelyzeteket jelenti, amelyek az információs társadalomban felmerülnek, indokolt azonban – figyelemmel a későbbiek során elemzett alkotmányos büntetőjogi szempontokra is – ennél szűkebb értelemben használni, mégpedig a kommunikációs hálózatokra épülő társadalmi viszonyokat szabályozó normákra vonatkoztatva.

Az információs társadalom joga tehát – a Simon szerinti szűk értelemben, és a teljesség igénye nélkül – magába foglalja a hozzáférési kérdéseket, a szellemi alkotások jogát, a

[3] A kifejezés japán változata *(joho shakai, johoka shakai)* Kisho Kurokawa építész és Tadao Umesao történész-antropológus 1961-es beszélgetései során születik meg. Írásban, egy tanulmány címeként 1964 januárjában jelenik meg először: a szerző ugyan Jiro Kamishima, de a címet a szerkesztő, Michiko Igarashi adja a tanulmánynak (Az információs társadalmak szociológiája). Az „információs társadalom" szószerkezetet később Yujiro Hayashi 1969-es bestsellere (*Johoka Shakai: Hado No Shakai Kara Sofuto no Shakai e*), Yoneji Masuda és Konichi Kohyma 1968-as bevezető-népszerűsítő könyvei (*Joho Shakai Nyumon*) használták. A fogalom születése és gyors megszilárdulása tehát egyaránt a szigetországhoz kötődik: 1971-ben Japán már rendszerező „szótárt" ad ki az információs társadalmakról (*Johoka Shakai Jiten*). Forrás: Z. KARVALICS, L., Információs társadalom – Mi az? Egy kifejezés jelentése, története és fogalomkörnyezete. In: Pintér Róbert (szerk). *Információs társadalom,* Gondolat Kiadó, Új Mandátum, 2007. pp. 29-30.

[4] SIMON, É., Bevezetés az információs társadalom jogi szabályozásába. In: Pintér Róbert (szerk). *Információs társadalom,* Gondolat Kiadó, Új Mandátum, 2007. p. 114.

személyes adatok védelmét, a szólásszabadságot, a távol lévők közötti kereskedelmet, a sajtójogot, a számítástechnikai bűncselekmények egyes típusait, az elektronikus aláírást, a nemzetközi jogi joghatósági kérdéseket. Simon felfogásában, míg a büntetőjog, az alkotmányjog vagy a polgári jog olyan részterületek, amelyeknek sajátos szabályozási rendjük és alapelveik vannak, addig az információs társadalom joga a vertikálisan felállított jogrendszert horizontálisan szövi át.

A különböző korszakokban és különböző tudományterületek hagyományaiból építkező, a fent ismertetett szempontokból kiinduló koncepciók mellett azonban nem mellőzhető annak meghatározása, hogy a *büntetőjogi gondolkodás számára* melyek a vizsgálandó irányok anélkül, hogy állást kellene foglalni bármelyik elmélet kizárólagossága mellett.

Abban valamennyi információs társadalom-koncepció felépítése hasonló, hogy mindegyikük azon kritériumok kiemelésére, azonosítására törekszik, ami új. Az információs társadalom és az alkotmányos büntetőjog konfliktusának megértéséhez tehát az említett tagozódás metszéspontját szükséges megragadni, éppen ezért a továbbiakban nem kerül sor az információs társadalom fogalmának, jelenségének definiálására, valamint valamennyi koncepció ismertetésére sem. Mindezek után a kérdés kizárólag az, hogy az információs társadalom diskurzusain belül melyek a büntetőjogi szempontból releváns új elemek?

1.1. A szabályozás jogi környezete: az EU és a magyar információs stratégia

Érdemes egyrészt az információs társadalom nemzetközi és hazai szabályozási környezetét górcső alá venni, azon belül is az Európai Unió információs társadalom stratégiáit, lévén, hogy az annak keretében alkotott programok és jogforrások – akár közvetve vagy közvetlenül – alapvetően meghatározzák a magyar információs társadalom kiépítésének normatív követelményeit, köztük a büntetőjogi jogszabályok tartalmát is. Egyfelől tehát *az információs társadalom mint politikai program* bemutatása indokolt, amely azonban nem lehet független magát a politikát életre hívó technológiai és társadalmi folyamatoktól.

1.2. A védendő értékek, az új jogi tárgyak és környezetük

Az információs társadalom egyik legjellemzőbb indikátora, az infokommunikációs eszközök általános elterjedtsége és használata, amely alapvető, gyökeres változásokat eredményezett szinte valamennyi társadalmi viszony területén. Mivel a büntető anyagi jogi szabályozás egyik kulcsfogalma a veszélyeztetett társadalmi viszonyok differenciálására és értékelésére épülő kriminalizáció, ezért a továbbiakban részletesebb kifejtést igényelnek az információs társadalom új, értéket képviselő és jogi védelmet követelő társadalmi viszonyai.

A technológiai környezet a hagyományos társadalmi viszonyok informatizálása révén egyrészt a már létező társadalmi értékek új szféráját, másrészt egészen új értékeket és azok veszélyeztetési potenciálját hozta létre. A büntetőjogi vizsgálat számára az említett jogi tárgyak, absztrakt értékek változására, az új értékek megjelenésére és a végbemenő társadalmi változásokra többek között a jogi tárgyak konkrét megnyilvánulási formái, az elkövetési tárgyak és azok felhasználási módjai utalnak, utóbbiak elemzése tehát inkább technológiaközpontú megközelítést követel majd. E problémakörrel foglalkozik jelen fejezetnek *az információs társadalom technológiai megközelítését* részletesen kifejtő alcíme.

1.3. Az információs társadalom embere

A büntetőjogi felelősségre vonás egyik meghatározó eleme az egyéni felelősség, a bűnösség vizsgálata. Az a változás, ahogy az új eszközök és az azokra épülő szolgáltatások eddig soha nem látott mértékben telepednek rá az emberek mindennapjaira, a társadalom jelentős része – főképp az idősebb generációk és a technológiai trendektől tartózkodók – számára gyakran érthetetlen. Az infokommunikációs eszközök használatával jellemzett kommunikációs környezet sajátosságai, a technika általa nyújtott lehetőségek miatt számolni kell a társadalmi erkölcs változásával is, szélesedik a deviánsnak tekintett magatartások skálája az új technológia nyújtotta lehetőségeket rendszeresen használók, és az azoktól tartózkodók közötti feszültségek miatt. Az infokommunikációs eszközök által behálózott környezetbe születő fiatalok aktív felhasználóvá válása e konfliktusban azt is jelenti, hogy az új társadalmi és technológiai kapcsolatrendszer normáit már egyre inkább ők maguk alakítják.

Az említett folyamatok miatt a bűnösség elemeire befolyással bíró jelenségek – köztük is főképp az infokommunikációs eszközök sajátos felhasználói környezete, a felhasználói trendek – kiemelt figyelmet érdemelnek. E témakört részletesebben jelen fejezetnek az *információs társadalom emberképéről* szóló alcíme, majd az információs társadalom új típusú devianciáival foglalkozó fejezet vizsgálja.

A továbbiakban e három, a büntetőjogi vizsgálatok számára jelentős irányvonal mentén kerül sor az információs társadalom értelmezésére.

2. AZ INFORMÁCIÓS TÁRSADALOM NARRATÍVÁI

2.1. Az információs társadalom megközelítései módjai

Az információs társadalom stratégiáinak elemzése előtt még érdemes röviden kitérni az információs társadalom témakörének átfogó ismertetésére, utalva a kialakult problémakörökre, egyben meghatározva az értekezés által alkalmazott megközelítési mód helyét is az információs társadalom elméletei között. A különböző korokban alkotó és más-más szemléletmódot képviselő szerzők munkásságának eredményeképpen született számos koncepció fogalmi rendszerezéséhez, kezelhetőségéhez többen próbáltak már valamilyen zsinórmértéket adni.

Egyrészt ***Z. Karvalics László*** rendszerezését érdemes alapul venni, aki a kifejezés helyénvaló kezeléséhez három narratívát vezetett be.[5] Az első, úgynevezett makroszintű *„nagy narratíva”* a magas absztrakciós szintű civilizációelméleti, társadalomfilozófiai, kultúraelméleti kontextusban tárgyalt elméleteket öleli fel. Z. Karvalics ide sorolja Tadao Umesao, Marshall McLuhan, Alvin Toffler elméleteit. A mezoszintű *„kis narratíva”* által jelölt koncepciók még mindig magas absztrakciós szinten foglalkoznak a társadalmi alrendszerek változásának kérdéseivel, azonban erőteljesebben körvonalazódtak bennük bizonyos kiemelt problémahalmazok. A szint egyik legjelentősebb képviselője Manuel Castells. A harmadik, talán kissé magyartalannak hangzó *„mininarratíva”* szintjéhez kapcsolódó vizsgálatok jelentős részét a valóság egy-egy kisebb szegmensére fókuszáló, gyakorlati szempontokat előtérbe helyező diskurzusok teszik ki, amelyek az érintett részterületekbe történő közvetlen beavatkozások megtervezéséhez nyújthatnak kiváló alapot, ilyennek tekinthető a technológiai központú megközelítési mód.

Pintér Róbert szerint[6] négyféleképpen definiálhatjuk az információs társadalmat: *Technológiai értelemben* az információval és a tudással végzett műveletek és az ezekhez kapcsolódó infokommunikációs eszközök állnak az információs társadalom középpontjában. *Társadalmi értelemben* a hálózati társadalom és hálózati gazdaság kialakulása, a közösségiség, a folyamatos adaptáció, az újfajta egyenlőtlenségek és a globalizáció jellemzik. A *fejlesztési narratíva értelmében* az információs társadalom utal egy korszak- és paradigmaváltásra (ipari társadalom utáni korszak), illetve egy gondolkodásmódra (amely leírható mint eszme vagy fejlesztési szupernarratíva). Végül az információs társadalom a *tudományos vizsgálat tárgyaként* is megjelenik *(information society studies).*

Szépvölgyi Ákos szerint[7] az információs társadalom, mint társadalomfejlődési paradigma kialakulása több, egymással időben és tartalmi szempontból is átfedéseket mutató, de megközelítési módjában jól elkülöníthető fejlődési szakaszokra bontható. Az *első hullám* a globális infokommunikációs-technológiai hálózatok kialakulásával, az információ, mint nyersanyag előtérbe kerülésével, a foglalkoztatás átrétegződésével jellemezhető. Ezen első állomás szakirodalmának megközelítései egyrészt a technológia fontosságát emelik ki,

---

[5] Z. KARVALICS, L., Információs társadalom – Mi az? Egy kifejezés jelentése, története és fogalomkörnyezete. In: PINTÉR Róbert (ed.), *Információs társadalom.* Gondolat Kiadó, Új Mandátum, 2007. pp. 41-42.

[6] PINTÉR, R., Divatos hívószavak, nagy elméletek, fejlesztési szupernarratívák és metanarratívák – Az információs társadalom jelentésvilága. In: PINTÉR Róbert (ed.), *Információs társadalom.* Gondolat Kiadó, Új Mandátum, 2007. pp. 212-223.

[7] SZÉPVÖLGYI Á., Az infomációs társadalom térszerkezet alakító hatásai. Doktori (PhD) értekezés, 2007. pp. 12-15. Forrás: http://www.rkk.hu/rkk/publications/phd/szepvolgyi_ertekezes.pdf [2012-04-15]

másrészt jellemzően gazdasági irányultságúak. A korszak képviselői például Daniel Bell, Fritz Machlup, Yonei Masuda. Mindegyikükre jellemző az úgynevezett technokrata szemléletmód, azaz az információs társadalom alapvetően technológiavezérelt felfogása, amelynek gyökere az automatizált adatfeldolgozást lehetővé tevő számítógépek megjelenése és elterjedése. Ezen megközelítések által kijelölt új paradigma alapja, hogy az információ mint nyersanyag, a hozzá kapcsolódó új technikák az összes emberi tevékenységre (gazdaság, társadalmi) hatással vannak.

A *második hullámban* jelennek meg a széles körű társadalmi változások, az innovációs folyamatok felértékelődnek, a „tudásintenzív" tevékenységek terjednek, a globalizáció erősödik, a kulturális közösségek lazulnak. A második hullám képviselői nem kérdőjelezik meg az első hullámhoz kapcsolódó megállapítások helytállóságát, csak azok kizárólagosságát. A második hullám képviselőinek tekinthetők például: John Naisbitt, Ari-Veikko Anttiroiko. Utóbbi szerint az információs társadalom a globalizáció egyik elemeként olyan változási folyamatok hatására jön létre, mint a globális gazdaság kialakulása, technológiai fejlődés, az instrumentális hálózatok fejlődése, a kultúra és az identitások változása. A fejlődés dinamikájának fenntartásában és növelésében a nem anyagi erőforrások szerepe tovább növekszik. E rendszerben a tudás válik a legfontosabb erőforrássá és a tanulás a legfontosabb folyamattá. A korszak fő képviselője Manuel Castells.

A fejlődés *harmadik hullámaként* alakul ki a tanulás társadalma, melynek jellemzői: az adaptáció, a folyamatos, kollektív tanulás, a bizalom, a lokalizáció növekvő szerepe, az új szerepkörök és életterek megjelenése. Szépvölgyi álláspontja szerint a második és a harmadik hullám közötti határvonalat az jelenti, hogy az információ elérésénél fontosabbá válik annak kezelése, azaz az adaptációs készség, ami nem más, mint az információk kreatív, értéktöbbletet termelő módon történő felhasználása.

Az információs társadalom tudományának kutatása alapján a különböző teóriák könnyebb kezelhetősége érdekében ***Frank Webster*** az információs társadalom *technológiai, gazdasági-foglalkozásszerkezeti, térszerkezeti,* és *kulturális* szempontú kutatási irányait különböztette meg, amelyeket a továbbiakban érdemes részletesebben is kibontani.[8]

2.2. Technológiai megközelítés

A technológiai megközelítés szerint azért élünk információs társadalomban, mert a társadalmi együttélés minden területén elterjedtek és egyre fontosabb szerepet játszanak az infokommunikációs technológiák, amelyek alapjaiban alakították át a társadalmak működését, beleértve a politikát, a gazdaságot, a kultúrát és a hétköznapi életet. Az ilyen irányú vizsgálódások középpontjában a következő kérdések állnak:[9] milyen új technológia terjedt el az elmúlt évtizedekben, ami az információs társadalom infrastruktúráját jelenti? Hogyan jönnek létre ezek a technológiák? Arra a célra szánták-e őket, amire végül ténylegesen felhasználták őket? Hogyan terjednek el a társadalomban és milyen pozitív, illetve negatív attitűdök nyilvánulnak meg velük kapcsolatban? Milyen a technológia és a társadalom viszonya? Mennyi technológiától áll be minőségi változás a társadalmi együttélésben?

[8] WEBSTER, F., *Theories of the Information Society,* Routledge, London – New York, Third edition 2006. A fejezet főként e mű felhasználásával készült.

[9] PINTÉR R., Úton az információs társadalom megismerése felé. In: PINTÉR Róbert (ed.). *Információs társadalom,* Gondolat Kiadó, Új Mandátum, 2007. (a továbbiakban Pintér 2007b) pp. 11-28.

Az információs társadalom technológiai szemléletű vizsgálói közül Yonei Masuda mai napig aktuálisnak tekinthető víziója szerint[10] az információs társadalom olyan új típusú társadalom (lesz), amelynek mozgatója az információs erőforrások mind hatékonyabb kihasználása, amely új típusú közösségeket, értékrend váltást, a környezethez való viszony változását eredményezi majd. Az információs társadalomban a masudai technokrata felfogás szerint az innovációs technológia alapja a számítógép, aminek egyik alapvető funkciója a szellemi munkaerő helyettesítése és kiegészítése, amelyre az információs termelőerő (az optimális cselekvésválasztás képességének növekedése) épül. Társadalmi-gazdasági szerkezeti szempontból az információs közművekben (információs hálózatok, adatbankok) zajló információk és technikai ismeretek termelése jelenti az alapot, amelynek társadalmi hatásaként az ismeretek határa kitolódik, kialakul egyfajta információs tér és egy sokközpontú funkcionális társadalom.

A tudomány, a technológia és a társadalom kölcsönhatásaival foglalkozó tudományos irányzat *(Science, Technology and Society studies, STS)* ugyan nem tekinthető a vizsgált terület uralkodó társadalomtudományos paradigmájának, de számos olyan előnye van, amely nélkülözhetetlenné teszi az információs társadalom és az attól elválaszthatatlan infokommunikációs technológiák vizsgálatánál, úgymint az alapvetően empirikus megalapozottságú elméletalkotás, valamint az a komplex megközelítési mód, amivel a technológia és a társadalom kölcsönös összefüggésrendszere vizsgálható.[11]

Az STS gondolati iskoláján belül több, egymást is kritikával illető, de alapjában véve egymást kiegészítő iskola létezik, például a „technológia társadalmi felépítésének" elmélete *(Social Construction of Technology, SCOT)*. A SCOT elméleti keretrendszerének egyik fő eleme, hogy egy technológia alakulását a releváns társadalmi csoportok határozzák meg, amelyeknek a tagjai lehetnek egyének, szervezetek és intézmények is, minden olyan csoport, amely számára a technológiával kapcsolatos problémák relevánsak.[12] Az elmélet társadalmi mozzanata úgy foglalható össze, hogy valamely technológia funkcionalitását leginkább az határozza meg, hogy azt mire és milyen módon akarják használni, míg a technológia alapjául szolgáló tudományos eredmények és mérnöki tervezés olyan keretrendszert szolgáltat, ami a felhasználói igények mozgásterét megszabja. Ebben a rendszerben az egyes technológiák formai és funkcionális átalakulása, az innovációk használatbavétele során variációk, mutációk és hibridek alakulnak ki (asztali számítógép, majd hordozható notebook, palmtop, PDA, „okostelefonok"). Ugyanakkor a releváns társadalmi csoportok által a technológiának tulajdonított funkciókat a csoport normái és értékei határozzák meg, ami viszont a szélesebb kontextusnak, vagyis a szociokulturális és politikai környezetnek a technológiára gyakorolt hatásáról árulkodik.

2.3. Foglalkozásszerkezeti és gazdasági megközelítések

A foglalkozásszerkezeti és gazdasági megközelítések szerint azért élünk információs társadalomban, mert a mezőgazdasági és ipari korszakon túllépve ma az információs szektor és az információs jellegű munkavégzés dominál a gazdaságban. Az irányzat képviselőinek fő kutatási kérdései:[13] Hogyan változott meg az iparban, illetve a

[10] MASUDA, Y., *Az információs társadalom*, OMIKK, Budapest, 1988.
[11] KINCSEI A., Technológia és társadalom az információ korában. In: BALOGH G., (ed.) *Az információs társadalom*, Gondolat-Új Mandátum, Budapest 2007. (a továbbiakban Kincsei, 2007.) pp. 50-51.
[12] PINCH, Trevor J. & BIJKER, Wiebe E., Tények és termékek társadalmi konstrukciója – avagy hogyan segítheti egymást a tudományszociológia és a technikaszociológia. *Replika* 2005., 51–52. szám. pp. 57–87. Forrás: http://www.replika.hu/pdf/51/51-03.pdf [2012-04-15]. Ismerteti: KINCSEI, 2007.
[13] PINTÉR, 2007b. pp. 11-28.

szolgáltatási szektorban foglalkoztatottak száma az elmúlt évtizedekben, és hogyan változott az általuk végzett munka, illetve az általuk birtokolt és alkalmazott tudás minősége? Megjelentek-e az úgynevezett információs munkakörök, központi szerepet tölt-e be a számítógép a termelésben? Érezhető-e a konvergencia – azaz a távközlés, a média és a számítástechnika – sokszor hangoztatott közeledése, egymásba olvadása?

A gazdasági elméletek szerint az információs társadalom alapja, az információ is egy vagyoni értéket megtestesítő dolog, jószág, amelynek jellemzője, hogy valamilyen hordozóhoz kapcsolódik, és azért vagy annak szolgáltatásáért kell fizetni. Ennek eredménye, hogy az információ-áramláshoz, mint üzleti folyamathoz mindig értéklánc *(value-chain)* tartozik, amelyben az információ feldolgozása és továbbítása során gyakran hozzáadott érték is keletkezik *(value added services)*, és amely értékláncokhoz a gazdaság egyre nagyobb hányada csatlakozik, kialakítva így az információs társadalmat.[14]

A gazdasági szemlélet egyik első képviselője, *Fritz Machlup* az 1960-as években az árukra és szolgáltatásokra fordított kiadásokat nemzetgazdasági szinten vizsgálva meghatározta, hogy mekkora kiadások függnek össze a tudással és információáramlással kapcsolatos tevékenységekkel. Kutatásai alapján az 1950-es évek Amerikai Egyesült Államában a nemzetgazdaság még csupán 30%-a származott az információs iparból, a foglalkoztatottaknak pedig csak 40%-a dolgozott ebben az ágazatban.[15] Később *Marc U. Porat* felülvizsgálta és továbbfejlesztette Machlup elméletét, amely eredményeképpen a gazdaságot inkább információ vezérelt (vagy információs) gazdaságnak értelmezte, valamint az információs ágazatot érdemesnek tartotta a gazdaság negyedik szektorának tekinteni. Megállapításaihoz hozzátartozik, hogy az 1970-es évekre az USA dolgozóinak már közel 50 %-a dolgozott az információs ágazatban.[16]

Webster szerint azonban fenntartással érdemes kezelni Porat és Machlup megállapításait, mivel az információs szektorok statisztikai hátterében jelentős súlyú önkényes értelmezés és értékítélet húzódik meg attól függően, hogy mit is sorolunk az információs szektorokhoz.

A hazai szerzők közül *Szabó Katalin* és *Hámori Balázs* szerint az ipari kapitalizmusból az információgazdaságba történő átmenet korszakát éljük, amely a közgazdaságtan számára még jelentős kihívásokat tartogat. A gazdasági megközelítés nehézsége abban ragadható meg, hogy míg a közgazdaságtan tárgykörébe a szűkösen rendelkezésre álló, kisajátítható javak tartoznak, addig a tudás nem tekinthető ilyennek: korlátlan és kisajátíthatatlan, azaz a közgazdaságtan hagyományos eszköztára nem alkalmas az immateriális javak vizsgálatára, nincsenek megfelelő elméletek és modellek. Az általuk képviselt irányzat a hagyományos tőkeelemek helyett az emberi tudásra és a digitális térben lévő információkra épít. Szabó és Hámori szerint ma már majdnem minden termék részben tudásjószág: a termék értékét a benne tárgyiasult tudás adja meg.[17] Mindez összhangban van *Peter Drucker*-nek már az

[14] BUDAI B., E-közigazgatás axiomatikus megközelítésben, PhD doktori értekezés, 2008. p. 61. Forrás: http://doktori-iskola.law.pte.hu/files/tiny_mce/File/Archiv2/budai/budai_balazs_ertekezes.pdf [2012-04-15]

[15] MACHLUP, F., *The Production and Distribution of Knowledge in the United States*, Princeton, John Wiley and Sons, 1962. Ismerteti: WEBSTER, F., *Theories of the Information Society*, Routledge, London – New York, Third edition 2006.

[16] PORAT, M. U., *The Information Sector: Definition and Measurement*, Washington, DC: U.S. Department of Commerce, Office of Telecommunications, 1976. Ismerteti: WEBSTER, F., *Theories of the Information Society*, Routledge, London – New York, Third edition 2006.

[17] SZABÓ, K., HÁMORI, B., *Információgazdaság – Digitális kapitalizmus vagy új gazdasági rendszer*, Akadémiai, Budapest, 2006.

1960-as években megfogalmazott észrevételével, miszerint a modern gazdaság alapjának már a tudás és a szervezés tekinthető.[18]

2.4. Térszerkezeti megközelítés

A térbeli megközelítése szerint az információs társadalmat, mint a fejlett kommunikációs és információs technológiák hatására kialakuló globális társadalmat a fizikai terek és az emberek kölcsönös összekapcsoltsága, hálózatba szerveződése jellemzi.[19] A térszerkezeti koncepciók szerint azért élünk információs társadalomban, mert az információs technológiák használatának és a globalizációnak köszönhetően egyre kevésbé meghatározó a fizikai tér szerepe, hiszen ma már hálózatok vesznek körbe minket, amelyek új keretet adnak a társadalmi folyamatoknak, úgymint a termelésnek, az elosztásnak, a politizálásnak stb., ugyanakkor az időtényező is megváltozott, amennyiben a kommunikációs egyidejűsége is általánossá vált.

A koncepciók nagyrészt szociológiai és közgazdaságtani alapokra is építkeznek, amikor a következő szempontokat emelik ki. Az új stratégiai erőforrás az információ, amely az információs hálózatokra épülő világgazdaság szerveződését alapvetően meghatározza. A szükséges infrastruktúrát biztosító információs technológiák kiemelt fontosságúak a szuverén államok határain átívelő, globálisan szervezett termelési folyamatok összehangolásában, mindamellett a globalizáció nem kizárólag gazdasági téren, hanem a földrajzi távolságok csökkenésével az egymástól korábban elkülönülten élő közösségeket összekapcsoló társadalmi kapcsolatok elmélyülésével is jellemezhető.[20] A gazdaság átalakulása szempontjából tehát a multinacionális vállalatok térnyerése jellemző, amelyek párhuzamosan több kontinensen működve osztják meg sok esetben a termelést, az irányítást, az értékesítés, valamint a kutatás és fejlesztés funkcióit. Az egész földre kiterjedő termelési és értékesítési módot az információs és kommunikációs technológiák robbanásszerű fejlődése tette lehetővé, a térszerkezeti megközelítés ebben a tekintetben tehát részben szintén technológiai meghatározottságú.

Az elméleti megközelítés fő kérdései itt a következők:[21] Hogyan változott meg az emberek térbeli kötődése? Hálózati logikát követ-e a világ működése? Létezik-e, kialakul-e globális társadalom? Mi a globális hálózatok belső logikája: ki az, aki ezekhez tartozik, és miért? Milyen társadalmi, illetve gazdasági tőke kell a hálózatokba való belépéshez és a bennmaradáshoz? Milyen a hálózatok belső kapcsolatrendszere, és abban mi a szerepe az új információs és kommunikációs technológiáknak?

2.5. Kulturális megközelítés

A kulturális megközelítés szerint azért élünk információs társadalomban, mert globális, egyre inkább digitalizálódó médiakultúra vesz körül minket, ami az értelem- és jelentésadás elsődleges forrásává válik meghatározva ezzel életünk kereteit. Az információs társadalom kultúrájával foglalkozó elméletek olyan új globális kultúra

[18] DRUCKER, P., The Age of Discontinuity, London, 1969. Ismerteti: WEBSTER, F., *Theories of the Information Society,* Routledge, London – New York, Third edition 2006.

[19] KOLLÁNYI, B., Térhasználat az információs társadalomban. In. PINTÉR Róbert (ed.). *Információs társadalom,* Gondolat Kiadó, Új Mandátum, 2007. p. 87.

[20] A kemelt térszerkezeti megközelítésekhez sorolhatjuk Anthony Giddenstől az *Elszabadult világ: Hogyan alakítja át világunkat a globalizáció?,* Napvilág Kiadó, Budapest, 2005., David Harveytól a *The Condition of Postmodernity: An Enquiry into the Origins of Cultural Change,* Blackwell, Oxford, England; Cambridge, Mass. 1990. című műveket.

[21] PINTÉR, 2007b. p. 24.

kontextusát írják le, amit egyetemleges referenciakeretként használhat a média. A legfontosabb változás e megközelítés szerint abban áll, hogy az információ korában a média kiemelt helyzetbe kerül, a társadalmi viszonyok egyik legfőbb meghatározójává válik és fordítva.[22] A kulturális megközelítések egyik központi tárgya az internet, amely mint az információs társadalom egyik kultikus helye jelentős kulturális változások ösztönzője, amennyiben a társadalmi közösségek által létrehozott kultúra mellett egyre jelentősebb szerepet kap az individuális kiberkultúra. A változás jellemzője, hogy nagymértékben visszaszorul a kultúrát előállító, illetve elfogyasztó szereplők tradicionális különválása, mivel az információs technológiák által hatékonyan támogatott hálópolgárok saját világainak milliárdjai társulnak a kultúra hivatásos konstruktőreinek produktumaihoz.[23]

2.6. Castells összefoglaló törekvése

Manuel Castells valamennyi, korábban ismertetett nézőpontot figyelembe véve próbált meg összefüggő elméletet alkotni az információs társadalomra vonatkozóan.[24] Castells olyan fogalmi rendszer kidolgozására törekedett, amelynek segítségével a modern kori társadalmak legújabb jelenségei megmagyarázhatók. Castells szerint az információs társadalom az emberi együttélés olyan új módja, amelyben az információ hálózatba szervezett előállítása, tárolása, feldolgozása, előhívása játssza a legfontosabb szerepet. A minőségi változás alapjául a mennyiségi változásokat teszi (például több számítógép, több információ áramlása), amelyek minőségileg is megváltoztatják az emberek közötti társadalmi viszonyokat. A társadalom átalakulásának infrastrukturális hátterében az információs és kommunikációs technológia áll, anyagi alapjait pedig az új hálózati gazdaság jelenti, ami – az együttélés más területeihez hasonlóan – erősen globalizálódik. Mindezzel szerinte együtt jár a társadalmi bizonytalanság növekedése, a tervezhetőség és az előrelátás csökkenése, egy új társadalmi egyenlőtlenségi rendszer megjelenése, ami mindenütt jelen van, létrehozva a kirekesztettek „negyedik világát”.

A társadalmi létezés új logikai szervezőelve a hálózati szerveződés: aki benne van a hálózatban, az létezik, aki nincs, az nem. Az ember alapvetően énközpontú, helyhez kötött és kulturálisan meghatározott identitása okán mindez óriási feszültséget eredményez, és ez, a Hálózat *(Net)* és az Én *(Self)* szembenállásából fakadó feszültség szervezi új mozgatóerőként az új társadalmat. A valós tér szerepét egyre inkább átveszi a hálózatokhoz köthető „áramlások tere”, ahol mindaz áramlik, ami fontos és értékes, azaz kialakul a virtuális valóság.

Castells szerint a társadalmi gondokat még tovább növeli, hogy új, globális bűnözőgazdaság jelenik meg, ami egyes államokban összefonódik a legális politikai erőkkel, és végső soron fenyegeti a globalizálódó világ egészét. Összegezve Castells koncepcióját a korábbi korszakokhoz képest az információs társadalom legfontosabb változásai a következők: az új infokommunikációs technológiák széles körű elterjedése, a foglalkozásszerkezet és a gazdasági termelés átstrukturálódása, az információval

[22] PINTÉR, 2007b. p. 25.
[23] ROPOLYI, L., Internethasználat és hálólét-konstrukció, *Információs társadalom: társadalomtudományi folyóirat*, 2006. (6. évf.) 4. sz. pp. 39-46.
[24] CASTELLS, M., *The Information Age: Economy, Society and Culture. Vol. III.: The End of the Millennium*, Blackwell, Oxford 1998., *A hálózati társadalom kialakulása – Az információ kora. I.,* Gondolat– Infonia, Budapest, 2005. [1996], *Az információ kora: Gazdaság, társadalom és kultúra. II. kötet: Az identitás hatalma,* Gondolat–Infonia, Budapest, 2006 [1997].

kapcsolatos szektorok és az információs munka felértékelődése, továbbá a fizikai tér szerepét háttérbe szorító, átfogó hálózatok kiépülésével együtt járó globalizáció, és végül a médiakultúra középpontba helyeződése.

3. AZ INFORMÁCIÓS TÁRSADALOM TECHNOLÓGIAI SZEMLÉLETE: PC-TŐL A VIRTUÁLIS VILÁGIG

A fejezet elején meghatározott vizsgálati szempontokra figyelemmel a továbbiakban az információs társadalom új típusú bűncselekményeinek jogi és elkövetési tárgyait felölelő részletesebb elemzésre kerül sor a Z. Karvalics László-féle „mininarratíva" szellemében és a Webster által jellemzett technológiai megközelítéssel.[25]

3.1. A fejlődés folyamata

3.1.1. A fejlődés technológiai alapja

Az információs társadalom egyik legszembetűnőbb jellemzője a mindent és mindenkit körülvevő információs és kommunikációs technikai eszközök (IKT) számának, sokféleségének, komplexitásának növekedése, valamint ezek folyamatos és szinte követhetetlen tempójú változása.[26] Az új technológia befogadásával kölcsönhatásban – eszközeinek megismerésével, alkalmazásával, fogyasztói igények szerinti fejlesztésével – a befogadó közeg, a társadalom is változik, a környezeti változások viszont alkalmazkodásra kényszerítenek. De mi is a fejlődés alapja?

Maga a technológia görög eredetű kifejezés, amely a *„mesterség"* (τεχνολογια < τεχνη), a *„tan"* (λογος) és egy toldalék (ια) összetételekből épül fel. A technológia az ember által készített olyan célszerű, az egyéni, emberi képességeit megnövelő eszközökről (például gépek, anyagok és eljárások) szóló ismeretek gyűjtőneve, amelyek segítségével az emberiség egyre többet tud megismerni, megváltoztatni, megőrizni az őt körülvevő világból.[27] De mi is az információs társadalomra jellemző technológia, miként segít megismerni és megváltoztatni az embert körülvevő világot? Kincsei Attila szerint a technológiai elem jellemzője ebben a kölcsönhatásban a következő pontokba foglalható össze: az innovációk által életre hívott új technológiai rendszerek megjelenése között múló idő továbbra is rövidül, az infokommunikációs eszközök teljesítménye növekszik, valamint a számítástechnika, telekommunikáció és a média konvergenciája.[28]

Maguk az információs társadalom narratívái is megszületésük idejéhez köthetően, egyesek kifejezetten csak a jövőre vetítetten (pl. Masuda), a változás egy-egy állomásának aspektusából kerestek választ kérdéseikre. Az információs társadalom korai koncepcióinak kidolgozása az automatikus adatfeldolgozás lehetőségét megteremtő technológia megjelenéséhez, az első számítógépek megalkotásához köthető, és ez a technológiai alapú szemlélet a politikai diskurzusoknak is köszönhetően végig meghatározó az információs társadalom jelentéstörténetében.

3.1.2. Első szint: a számítógép

A folyamat kiinduló pontja, első szintje tehát a gazdasági, tudományos és a társadalom egésze számára hozzáférhető, az adatok automatizált feldolgozását, továbbítását, tárolását

---

[25] A fejezet alcíme DÖMÖLKI, B., KÓSA, Zs., KÖMLŐDI, F., KRAUTH, P., & RÁTAI, B., *Égen-földön informatika – Az információs társadalom technológiai távlatai*, Typotex. Budapest, 2008. című műve alapján készült.

[26] KINCSEI A., Technológia és társadalom az információ korában. In. BALOGH G. (ed.) *Az információs társadalom*, Gondolat-Új Mandátum, Budapest 2007. p. 47.

[27] Forrás: Encyclopedia Britannica: http://www.britannica.com/EBchecked/topic/585418/technology [2012-04-15], valamint Wikipedia: http://hu.wikipedia.org/wiki/Technol%C3%B3gia [2012-04-15]

[28] KINCSEI A., Technológia és társadalom az információ korában. pp. 59-60.

lehetővé tevő számítógép megjelenése, amely Masuda koncepciójára visszautalva lehetővé tette az emberi szellemi tevékenység kiváltását, kiegészítését és hatékonyabbá tételét. A számítógép emellett a kreativitás serkentésével új, hozzáadott értékű szolgáltatások és termékek teremtését biztosító kapacitáshoz juttatta a felhasználókat. Az új erőforrás megjelenésétől kezdve fokozott védelmet igényelt, másrészt járulékosan is új jogi tárgyakat, új, védendő társadalmi érdekeket teremtett.

3.1.3. Második és harmadik szint: a számítógép popularitása és a világháló.

Döntő szakasza volt a fejlődésnek, hogy a katonai és tudományos élet területéről kitörve az egyre kisebb méretű, egyre könnyebben kezelhető ám több perifériát csatlakoztatni képes és olcsóbb számítástechnika egyre több és több ember számára vált hozzáférhetővé. 1981-ben az IBM piacra dobta a már nevében is személyeknek szánt PC-t, azaz a *personal computer*-t.

A következő lépcsőfoknak a korábban elszigetelt, önálló egységek hálózatban történő összekapcsolása és az internet megjelenése volt. A világháló a kliens-szerver architektúrák világméretű kiépülése mellett a különféle p2p hálózati rendszerek, grid-rendszerek, és hyperszámítástechnikai rendszerek megjelenésével és terjedésével fejlődött tovább, az újabb fejlesztéseknek meghatározó technológiai alapjává, megannyi szolgáltatás önálló platformjává válva. Közben a személyi számítógépek mellett az emberi környezet egyre több elemében jelentek meg infokommunikációs eszközök (pl.: gépkocsik fedélzeti számítógépe, háztartási berendezések, un. intelligens otthonok rendszerei), amely egy korszak, a *desktop*-számítógépek dominanciájának lezárulását eredményezte.

A technológia fejlődésének irányát a miniatürizáció, mobilizáció, a funkciók konvergenciája, a hálózati működés, valamint mindezek szabványosítása határozzák meg, amelyek hatására újabb és újabb infokommunikációs eszközök váltak minden ember számára elérhetővé (pl.: laptop, netbook, palmtop, PDA, okostelefonok, tabletek, stb.). A komplex személyi hírközlési eszközök integrálták a mobil távközlés, a kép- és mozgóképrögzítés, a hang- és videoalapú szórakoztatás, a navigáció funkcióit, a különböző szolgáltatásokhoz tartozó személyazonosító kártyákat, kódokat, az elektronikus aláírást, és fizetési módokat.

3.1.4. A infokommunikációs konvergencia

A folyamat egyik kulcsfogalma tehát a konvergencia, amelynek bár nincs pontos, általánosan elfogadott használata a szakirodalomban, a téma szempontjából különböző hálózati platformok azon képességét jelenti, hogy alapvetően hasonló szolgáltatási fajtákat hordoznak, de olyan fogyasztói eszközök összefonódását is jelöli, mint például a telefon, televízió és a személyi számítógép. Meghatározó technológiai alapja a digitalizáció, amely műszaki megoldás lehetővé teszi, hogy ugyanaz a tartalom a korábban egymástól elkülönült hálózatokon is átvihető legyen.[29] Az infokommunikációs konvergencia olyan technológia gyökerű folyamat, amely egyszerre több szinten zajlik.

Koppányi Szabolcs szerint[30] a tapasztalható változás nem azt jelenti, hogy a konvergencia hatására az eddigi alszektorokból egy új, egységes, mindent átfogó médium alakulna ki,

[29] TÓTH, A., *Az elektronikus hírközlés és média gazdasági szabályozásának alapjai és versenyjogi vonatkozásai,* HVG-ORAC Budapest, 2008. p. 57.
[30] KOPPÁNYI Sz., *Hírközlési jog az európai közösségben és Magyarországon*, Osiris Kiadó Budapest, 2003. p. 23.

hanem azt, hogy az információk megjelenési formája válik kompatibilissé, amelynek következtében az információhoz különböző kommunikációs eszközök közvetítésével (internet, telefon, televízió) hozzájutva elmosódnak a határok mind a tömeg- és az egyéni kommunikáció, mind pedig az elosztó és közvetítő médiumok között.

Az eszközök fizikai környezetétől kissé eltávolodva tehát a digitalizáció a tartalmak platform-független közvetítésének fejlődésével a korábban elkülönült gazdasági ágazatok, úgymint az informatika, a távközlés és a média közeledését, összeolvadását is elindította. Maga a konvergencia tehát nem egységes jelenség, a szűkebben vett technikai konvergencia, a gazdasági struktúrák változása, valamint a fogyasztói viselkedések konvergenciája egy időben zajlik. A konvergencia így a média, informatika és távközlés területein végbemenő változás, amely folyamatnak a figyelemmel kísérésére többek között azért van szükség, mert meghatározza az informatikai bűncselekmények elkövetésének környezetét nem csak infrastrukturális, hanem kulturális értelemben is.

3.1.5. A technológiai fejlődés társadalmi aspektusai

A közelmúlt és a jelen technológiai szemléletű információs társadalmát tovább jellemezhetjük három társadalmi terület konkrét változásai alapján is.[31] Az *üzleti szféra* tekintetében az elektronikus kereskedelemben az infokommunikációs eszközök és szolgáltatások terjedésével – pl. a weboldalakkal, e-mailekkel, RSS – a vevőkapcsolatok új formái jelentek meg. Egy vagy több termékcsoportra szakosodott elektronikus piacterek születtek, amelyek sok termék tekintetében rövid időn belül háttérbe szorították a hagyományos vásárlási fórumokat. Az új, online fizetési eszközök (pl. online átutalás, mobilhívások, PayPal) helyettesítik, kiváltják a készpénzforgalmat, egyre kényelmesebbé téve a vásárlást. Az infokommunikációs eszközök az elektronikus üzletvitelt is megreformálták az üzleti folyamatok automatizálásával, a közvetlen termelésirányítás és logisztika informatizálásával lehetőség nyílt a piackutatás, a költséghatékonyság, a termelékenység további javítására. Mindezek mellett természetesen új üzletágak is megjelentek, például: a tartalomszolgáltatás, reklámipar, pénzügyi és bankinformatika, tudásmenedzsment, kutatásfejlesztés, stb.

A *közszféra* változásai például a közigazgatás informatizálásában nyilvánulnak meg. A kormányzati portál, az elektronikus ügyfélkapu, a regisztrált tulajdonok (gépjármű, ingatlan) és cégjegyzék elektronikus nyilvántartása, az igazságügyi intézmények elektronikus ügyvitele[32], valamint a társadalombiztosítási és egészségügyi szervezetrendszer mind-mind infokommunikációs hálózatok üzemeltetésével törekednek az állam működésének, az állam és polgára közötti kapcsolat javítására.

Végül a *magánfelhasználás* területén nemcsak a személyek közötti kapcsolattartás alakult át, hanem az otthoni életvitel és háztartási információkezelés is, a szabadidő eltöltésének lehetőségei, az alkotóművészet, munkavégzés és még számos egyéb aktivitás. A web 2.0. trendje kiszorította a média egyirányúságát, helyét átvette az interaktivitás, azaz mindenki, minden felhasználó médium lehet. E korszakban már nem a PC, hanem a web működik platformként, ahol a felhasználók gyakran együttesen állítják elő, osztják meg egymással a tartalmakat könnyen és gyorsan kezelhető interaktív alkalmazások segítségével. Miért volt jelentős e három terület vizsgálata? Mert bemutatásuk révén érzékletes képet kaphatunk a

[31] DÖMÖLKI et al. 2008. pp. 25-44.

[32] Pl.: az ingatlan-nyilvántartás elektonikus alapú TAKARNET-rendszere, a bűnügyi igazgatásban a Robotzsaru, Netzsaru, PraetorPraxis, a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala által üzemeltetett bűnügyi nyilvántartás, MAKÖR, stb.

megjelenő új társadalmi érdekekről, áttételesen a büntetőjogi tényállások jogi tárgyairól, amelyek a gazdasági, állam elleni, személy elleni bűncselekményi csoportosítás elméleti alapját képezhetik.

A technológiai elem (az eszközök és szolgáltatások) biztosította és biztosítja a társadalom számára az intenzívebb információáramlást, az információk tömegéhez való hozzáférést, míg a társadalom oldaláról nézve a hagyományos, fizikai világbeli tevékenységek infokommunikációs technológiai rendszerekkel történő kiegészülése, támogatottsága, mediatizáltsága magának a tevékenységnek a virtuális dimenziójába való kiterjesztését eredményezi.[33] Ezen eszközök relatíve általánosan hozzáférhető volta lehetővé teszi a társadalom minden tagja számára a nemzethatárokon átívelő kommunikációt, kapcsolatteremtést, közösségépítést, megváltoztatva ezáltal a felhasználók szokásait, a magánélet színtereit.

3.1.6. A kommunikáció és környezete

A kommunikáció nem csak személyek között zajlik, hanem egyre inkább a technikai környezet és az ember között is. Az ember-gép interakcióját tekintve az egyre több intelligens vonást mutató, számítástechnikai eszközök által behálózott környezetben a felhasználó személyre szabott módon tudja folytatni kommunikációját, biztosítva a fizikai lét mellett az állandó „online" jelenlétet. E területen folyamatosan zajlik a környezettel történő interakciók lebonyolítására szolgáló *szenzorok* (érzékelők) és *aktuátorok* (beavatkozók) fejlesztése, amelyek az emberi gesztusok, hangok érzékelése alapján hajtják végre az adott számítástechnika rendszer funkcióját. A szenzorok és aktuátorok a (nemcsak) virtuális környezetek és távközlési végberendezések kombinálódásával, ad hoc és vezeték nélküli rendszerré alakulásával a felhasználó cselekedeteit és interakcióit támogató környezet-intelligenciává alakult gépekként egyre inkább a hétköznapi élet szerves részévé válnak.

A vezeték nélküli, önkonfiguráló hálózatokká alakuló, tároló és feldolgozó kapacitással rendelkező apró eszközök, amikben a számítógép beágyazott célhardver formájában van jelen, fizikai tereinket benépesítve egyre fontosabb szerepet kapnak. Az embert, a felhasználót e tárgyakba épített intelligens *interface*-ek veszik körül, a személyre szabott technikai környezet szinte észrevétlenül felismeri jelenlétünket és reagál rá. Ez az intelligens felhasználói felület lehetővé teszi a környezettel való természetes, például hang vagy gesztusok általi, referenciáinknak és a kontextusnak megfelelő interakciót (például: közlekedési, helymeghatározási rendszerekre, helyváltoztatással kapcsolatos egyedi alkalmazásokra, a felhasználó levegővételéről, bőrhőmérsékletéről, testhelyzetéről, mozgásáról adatokat gyűjtő szenzorokra, vagy testbe épített implantátumokra lehet gondolni).[34]

Az „ember-gép" kommunikáció mellett természetesen a szintén egyre több intelligens vonást mutató M2M *(machine to machine)*, „gép-gép" kapcsolatok is rohamosan fejlődnek.[35] A fejlődéssel párhuzamosan az információ-technológia széleskörű

[33] KINCSEI, 2007. pp. 59-60.
[34] DÖMÖLKI et al. 2008. p. 61.
[35] Az M2M alkalmazásfejlesztés uniós vonatkozása, hogy Magyarország 2011 júniusában csatlakozott az európai egységes vészhívó-rendszer létrehozását szolgáló eCall törekvéshez. A közlekedési eszközökben elhelyezett eCall rendszer az utasok és a járművek által is aktiválható készülék, amely automatikus vészhívást indít, ezzel a városi területekre 40 %-kal, vidékre mintegy 50 %-kal gyorsabban érkeznek meg a

elterjedésével a biztonsági kockázatok is nőni fognak, ezért indokolt a szenzorok – ma még hiányzó – kellően differenciált jogi, büntetőjogi védelmének kidolgozása.[36]

3.1.7. Negyedik szint: a virtuális jövő

Az interakciók okán megnövekvő terhelés miatt a hálózati rendszerek hatékonyságának növelésére, az egyes rendszerelemek közötti koordináció és szinkronizáció lebonyolítására az un. köztes szoftverek fejlesztése jelenti az egyik üzleti irányzatot. Felhasználói oldalon az infrastruktúra ma még tipikusan szigetekből áll, azaz egy-egy alkalmazás vagy alkalmazási terület saját külön szerverrel, klaszterrel és hozzá tartozó egyéb berendezésekkel rendelkezik, a növekvő alkalmazások és szolgáltatások okozta terhelés miatt a rendszer hatékonyságának javítása érdekében viszont alapvető érdek, hogy az informatika számára a prioritásokat ne a mindenkori technológiai adottságok átláthatatlan fejlesztése, hanem egyre inkább az üzleti igények és az igényelt szolgáltatásminőség határozza meg.[37]

Ezért kezdődött meg a jelenleg működő adat- vagy informatikai központok virtualizálódása, azaz olyan számítóközpontok létrehozása, ahol az egyes rendszerelemek helye, belső vagy külső volta, konkrét típusa egyre kevésbé játszik szerepet, míg az erőforrások igénybevétele a terheléstől függően dinamikusan változik.[38] A virtualizáció eredményeképpen a rendszer kifelé mutatott viselkedése, külső kapcsolatai és funkciói függetlenné válnak a rendszer belső architektúrájának fizikai felépítésétől, az informatikai erőforrások, a rendszerelemek absztrakt kezelésére lehetőséget nyújtva, azaz a technológia a fizikailag egyébként létező elemeket és működésüket más módon, más platformon logikailag jeleníti meg.[39]

Az informatikai rendszerek üzemeltetése egyre inkább közműjelleggel és szolgáltatásszerűen történik, ami részben abban nyilvánul meg, hogy a felhasználók személyi számítógépein futó programok mind nagyobb része kerül központi szolgáltatásként végrehajtásra, gyakran a felhasználó adatainak nagy részét is a szolgáltató szerverein tárolva. Ennek kockázata, hogy a felhasználók adatai a szolgáltatók birtokába kerülnek, és azokra a felhasználónak pusztán csak igénye van. A téma szempontjából az információtechnológiai közművek kialakulása felé mutató fejlődési iránya a *cloud computing*, hiperszámítástechnikai fejlesztések irányzata.[40] Ez esetben a szolgáltatók igen nagy számú felhasználót vagy különösen nagy leterhelést kezelni is képes, másrészt igen kevés számú felhasználó vagy ritka használat esetén is egyaránt költséghatékony szolgáltatásként nyújtják az információtechnológia által támogatott képességeiket. E

---

mentőcsapatok. Az eCall része az Európai Útbiztonsági Akciótervnek, amelynek célja, hogy 2020-ra 50 %-kal csökkenjen a közúti elhalálozások száma.

[36] A büntetőjogi védelem indokait a szenzorok megannyi alkalmazási területe indokolhatja, így például az egészségvédelmi, vagy ahhoz kapcsolódó jelzőrendszerek szenzorai a környezet változásait érzékelve működnek, azonban hibás, értelmezhetetlen jelek küldésével a rendszerek működése megzavarható. De mivel a szenzor maga nem számítástechnikai rendszer, és az értelmezhetetlen jelek kibocsátása sem tekinthető „műveletnek", a számítástechnikai rendszer elleni támadás nem állapítható meg büntetőjogi szempontból. Az érvelés kifejtésére részletesebben a jogeseteket feldolgozó fejezetben, a traffipax-blokkoló eszközökről szóló címben kerül sor.

[37] DÖMÖLKI et al. 2008. pp. 358-359.

[38] DÖMÖLKI et al. 2008. pp. 358-359.

[39] DÖMÖLKI et al. 2008. p. 66.

[40] Példaként említhető az Amazon online webáruház a fel nem használt kapacitását időszakonként bérbe adja.

jelenség mögött három irányvonal egymáshoz közeledése áll: a szolgáltatásorientáltság, a virtualizáció és az interneten keresztül bonyolódó számítástechnika szabványosítása.[41]

3.2. A jövőkép

A szüntelen technológiai fejlődés vizsgálatára irányuló kutatások alapján körvonalazható jövőkép elemei a következők. A számítógépek és adatátviteli vonalak teljesítményei oly mértékben növekednek, hogy gyakorlatilag nem jelentenek majd korlátot a megoldandó feladatok méreteire vonatkozóan. Teljessé válik az eszközök összekapcsoltsága, nem lesznek elszigetelten működő számítógépek. Az információfeldolgozás és adatátvitel lehetőségei megjelennek az embert körülvevő környezet tárgyaiban (pl. háztartási berendezések, járművek), akár az emberi testben, gondoljunk a különféle bionikus protézisekre, készségjavító implantátumokra. Az informatikai rendszerek működése egyre több intelligens vonást mutat. A rendszerekben a szolgáltatások különböző fajtái kerülnek előtérbe, a felhasználók mind inkább szolgáltatásokat és nem termékeket vásárolnak. Az infokommunikációs rendszerek fokozott mértékben támogatják az őket használó emberek együttműködésének különböző formáit. Az infokommunikációs rendszerek működésének biztonsága egyre nagyobb kihívást jelent.

A fejlődési folyamat eredményeképpen az internet egyre inkább interface-szerepet tölt majd be a helyüket változtató emberek és az őket körülvevő fizikai világ között, végül olyan egységes és programozható rendszerré válhat, amely megtestesíti a korábbi kibertér *(cyberspace)* víziókat.[42] A kibertér fogalma William Gibson írótól származik, aki a *Neuromancer* című regényében a hálózatba kapcsolt számítógép-terminálokról közvetlenül elérhető digitális, navigálható teret jelöli vele.[43] *Mészáros Rezső* szerint a kibertér Gibson felfogásában egy olyan mátrix, amely színes, elektronikus, karteziánus adattájkép, ahol vagy inkább, amelyben a felhasználók interaktív kapcsolatba lépnek az információval, és kereskednek vele.[44] A virtuális környezet és a virtuális környezetben található virtuális tárgyak feletti rendelkezési jogosultságok (módosítás, átruházás, megszüntetés), virtuális tárgyak eltulajdonításáért való felelősség egyúttal számos új szabályozási kérdést vetnek fel.

3.3. A technológiai fejlődés számadatai

A fejlődés jól érzékeltethető néhány számadattal.[45] Az előrejelzések szerint 2014-ben az internetes forgalom négyszer akkora lesz, mint 2010-ben. A mobil hálózatok által lebonyolított internetes forgalom évente átlagosan megduplázódik, az átlagos felhasználó digitális kommunikációjának 40 %-át az interneten bonyolítja le a 2010-ben mért 12 % helyett. Az átlagos sávszélesség megnégyszereződik: 3,5-ről 14,4 Mbps-ra nő, ezzel párhuzamosan szignifikánsan növekszik a nagyobb sávszélességű alkalmazások iránti

[41] DÖMÖLKI et al. 2008. p. 380.
[42] DÖMÖLKI et al. 2008. p. 204.
[43] GIBSON, W., *Neuromancer*. Harper Collins, London. 1984.
[44] MÉSZÁROS, R., A kibertér mint új földrajzi tér. In. Kiss, A., Mezősi, G. & Sümeghy, Z. (ed.), *Táj, környezet és társadalom: ünepi tanulmányok Keveiné Bárány Ilona professzor asszony tiszteletére*, Szeged: SZTE Éghajlattani és Tájföldrajzi Tanszék – SZTE Természeti Földrajzi és Geoinformatikai Tanszék, 2006. p. 493.
[45] Forrás: CISCO Visual Networking index: forecast and Methodology 2009-2014, Bain&Co: Next generation competition, Morgan Stanley, OECD. Ismerteti: Digitális Magyarország Cselekvési Terv 2010-2014. Az újabb eredményeket lásd: CISCO Visual Networking index: forecast and Methodology 2010-2015 forrás: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf [2012-04-15]

igény. Világszerte több milliárd „digitális eszköz” teszi egyszerűbbé és gazdaságosabbá az életet, a mobil internet eszközök száma és az ezekről történő internethasználat meghaladja majd a számítógépekét, az internethasználók számának globális növekedését (18 %) meghaladja az internet használatával töltött idő növekedése (21 %).

Az EUROSTAT legfrissebb adatai szerint Európai kontextusban elmondható, hogy az internetet legalább heti rendszerességgel használók aránya az EU szinte minden országában meghaladja az 50 %-ot, az otthoni internetkapcsolattal rendelkező háztartások aránya is több mint 50 %-os.[46] Az Európa 2020 fejlesztési program Digitális Menetrend[47] kezdeményezésének adatai szerint az évi 660 milliárd eurós piaci értéket teremtő IKT-ágazat az európai GDP 5 %-át termeli meg közvetlenül, a termelékenység általános növekedéséhez azonban ennél jóval nagyobb arányban (közvetlenül 20 %-kal, az IKT-beruházásokkal pedig 30%-kal) járul hozzá. Mindennek hátterében az ágazatra jellemző dinamizmus és magas szintű innováció áll, valamint az a tény, hogy az ágazat meghatározó szerepet játszik a többi ágazat – korábban ismertetett – üzleti tevékenységének alakulásában. Az IKT-k társadalmi hatására és az életminőségbeli változásra utal az is, hogy naponta több mint 250 millió európai használja az internetet, valamint gyakorlatilag minden európai polgár rendelkezik mobiltelefonnal. A Digitális Menetrend előrejelzései szerint 2020-ra a digitális tartalmak és alkalmazások szinte kizárólag a világhálón lesznek elérhetők.

3.4. Az új társadalmi értékek

Az információs társadalom technológiai megközelítése az új társadalmi érdekek és azokon keresztül a büntetőjog által védett jogi és elkövetési tárgyak meghatározását célozta. A technológiai megközelítés alapján az állapítható meg, hogy a társadalom szinte valamennyi alrendszerének – legyen az a politika, jog, gazdasági élet vagy magánélet – informatizálása zajlik, ezáltal a folyamat valamennyi említett terület társadalmi viszonyaira kihatással van. Az érintett, értéket képviselő társadalmi viszonyok büntetőjogi leképeződései a védendő jogi tárgyak, amelyek formális kereteit a fejezet alapján a következőképpen jellemezhetjük.

Egyfelől kiemelt társadalmi érdekként jelent meg magának a kommunikációs *infrastruktúra* biztonsága, megfelelő védelme, hiszen az a rajta keresztül folytatott interakciók, virtuális aktusok mennyisége és fajtája miatt – függetlenül a tartalmukhoz kapcsolódó érdekszféráktól – meghatározó a társadalom legtöbb tagja, entitása (az állami szervek, gazdasági szereplők, magánszemélyek) számára. Maga az infrastruktúra – szűkebb értelemben – lényegében egy számítástechnikai rendszer, illetve ilyen rendszerek összessége, kapcsolata. A büntetőjogi kriminalizáció számára ezen eszközök jelentik elsősorban azon elkövetési tárgyak halmazát, amelyen keresztül az egyes társadalmi érdekek – jellegük és fontosságuk szerint – differenciálva tényállásonként védhetők.

Másrészt a jogi tárgyak tekintetében elmondható, hogy az elemzett technológia olyannyira része a mindennapok életvitelének, az állami és gazdasági életnek, hogy ugyancsak kiemelt társadalmi érdek a fenti infrastruktúrához való *hozzáférés*, és az azon folytatott interakciók *biztonsága, hitelessége, bizalmassága*.

[46] http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/data/main_tables [2012-04-15]
[47] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:HU:PDF [2012-04-15]

4. SZABÁLYOZÁSI KÉRDÉSEK I.: AZ EU INFORMÁCIÓS POLITIKÁJA

Az elektronikában, a számítógépek és távközlő berendezések és a szoftverek tekintetében elért technológiai haladás lehetővé teszi az adatok minden korábbi képzeletet felülmúló továbbítását és feldolgozását, amely fejlődés eredményeképpen – Masuda jóslatával megegyezően – több idő juthat a kreatív gondolkodásnak az információ keresése és a szervezés helyett. A digitális forradalom az informatikára épülő hagyományosan önálló ágazatok konvergenciájára ösztönöz, ami végeredményben egy önálló multimédia ipar megteremtéséhez és új szolgáltatások nyújtásához vezetett és átformálta egész gazdasági, társadalmi és személyes kapcsolatrendszerünket.

A fejlődés irányát felismerve az EU is elkötelezte magát az említett technológiai átalakulásokkal járó politikai következmények felvállalása mellett és a korábban bemutatott fejlődésre reagálva, azt elősegítendő az információs társadalom a különböző politikai platformok egyik hangzatos programeleme lett. Éppen ezért a továbbiakban nem mellőzhető a magyar büntetőjogi tényállásokra is kihatással bíró uniós joganyag és fejlesztési programok ismertetése, egyáltalán a fejlődés politikai-jogi keretének rövid bemutatása.[48]

Politikai programjai közül kiemelkedők az EU információs stratégiái, amelyekről elöljáróban annyit, hogy az információs társadalom fejlesztéséhez szükséges feladatokat és a végrehajtásukhoz nélkülözhetetlen eszközöket alapvetően három területen jelölik ki. Az *„információs közmű" fejlesztése* révén cél a nyilvános információ-feldolgozó és -szolgáltató létesítményekből álló információs infrastruktúra kiépítése, amelynek segítségével bárki, bárhol, bármikor képes lesz az általa igényelt bármilyen információhoz könnyen, gyorsan és olcsón hozzájutni. A *társadalom informatizálásának* célja a legfontosabb társadalmi alrendszerek úgymint a politika, a jog, az egészségügy, az oktatás stb. teljes informatizálása. A harmadik irányt *az információs iparágak fejlesztési politikája* jelenti, amelynek célja néhány húzóágazat kiemelt fejlesztése a gazdaság egészének informatizálása érdekében.

Az információs politika változásáról röviden annyit érdemes kiemelni, hogy kezdetekben szinte kizárólag gazdasági megfontolások alapján történt a fejlesztési feladatok kijelölése, és csak később kaptak hangsúlyosabb szerepet a társadalmi szempontok. 1999. és 2005. között az *eEurope* programcsalád határozta meg az információs társadalom fejlesztésének európai irányvonalait, amelynek elemei elsősorban a gyorsabb és elterjedtebb internethasználatra koncentráló stratégiai koncepciók egymásra épülő programok és akciótervek sorozatában öltöttek testet.

A széles sávú infrastruktúra megteremtéséhez szükséges feltételek biztosítását követően újra megváltozott az EU információs társadalom építése terén követett stratégiája, és az eEurope programot felváltotta az *i2010*. kezdeményezés. Az egységes információs tér megteremtését, a kutatás-fejlesztést, valamint a mindenkit befogadó információs társadalom felépítését a középpontba állító program annyiban visszatérést jelent a gyökerekhez, hogy a további feladatokat újból a lisszaboni célkitűzések jegyében jelölte ki, amelyek Európát a világ legfejlettebb tudásalapú gazdaságává kívánták tenni. Az EU információs társadalommal kapcsolatos politikájára jellemző, hogy lényegében a központi,

[48] A cím az idézett EU dokumentumok mellett a következő mű alapján készült: JUHÁSZ, L., Az Európai Unió információs stratégiája. In: PINTÉR Róbert (ed.), *Információs társadalom.* Gondolat Kiadó, Új Mandátum, 2007. pp. 130-143.

szupranacionális szinten elfogadott célkijelölés és programalkotás, illetve az ehhez kapcsolódó nemzeti szintű akciótervek kettősére épül.

4.1. A Bangemann-jelentés és az út az *eEurope* programig (1993–1999)

4.1.1. A Bangemann-jelentés

Az Európai Bizottság korábbi elnökhelyettese, Martin Bangemann irányításával, számos iparági szakértő, valamint a társadalom különböző szektorait képviselő felhasználó közreműködésével 1994-ben elkészült az *„Európa és a globális információs társadalom – Ajánlások az Európai Tanács számára”* című jelentés.[49] A jelentés az első komolyabb dokumentum e téren, „korszaknyitó” jellege tagadhatatlan, amennyiben pontosan felismerte az információs társadalom fejlesztésének mai napig meghatározó okát és célját, a főbb irányvonalait, amelyek végighúzodtak az újabb stratégiai dokumentumokon. Ezért indokolt a többi dokumentumnál némiképp részletesebben foglalkozni a Bangemann-jelentéssel.

A jelentés első fejezete *az együttélés és az együttműködés új módozatait* emeli ki az információs társadalom egyes területein. A technológia forradalom hatékony kihasználására való törekvés esetén az EU polgárai magasabb életminőséghez, a szolgáltatások, illetve a szórakozás szélesebb választékához juthatnak hozzá, és ami még jelentősebb: a kreativitás érvényre juttatásának új módjaival új termékek és szolgáltatások hozhatók létre.

Államigazgatási téren az állampolgárhoz közelebb álló és alacsonyabb költségekkel járó, hatékonyabb, áttekinthetőbb és jobban reagáló közszolgálatok működtethetők. A gazdasági élet területén a kis- és közepes vállalkozások fejlesztése biztosítható a hatékonyabb irányítás és szervezeti felépítéssel, az oktatási és egyéb szolgáltatásokhoz való hozzáféréssel, a fogyasztókkal és szállítókkal kialakított adatszolgáltatási kapcsolatokkal, ami végeredményben növeli a versenyképességet. A fejlődés elősegítésével több új, hozzáadott értékű szolgáltatás szélesebb választékát biztosító kapacitáshoz juthat a gazdaság, amely ezzel párhuzamosan a szükséges berendezések és szoftverek megnövekvő igénye miatt új és erőteljesebben növekvő hazai és külföldi piacot is kaphat. Ekként ez a jelentős IKT-potenciál egy önmagát gerjesztő működési folyamat során aktivizálódhat.

Az új információs eszközök és szolgáltatások széleskörű hozzáférhetősége lehetőséget teremt egy nagyobb egyenlőségi jogokat biztosító és kiegyensúlyozottabb társadalom kiépítésére, az egyedi teljesítmények fokozására, az európai állampolgárok életminőségének és a társadalmi valamint gazdasági szervezetek hatékonyságának javításával végső soron erősítse a kohéziót.

A jelentés második fejezete egy *piacközpontú információs forradalmat* körvonalaz, míg a harmadik fejezet főként az *új gazdasági szektor* egyes stratégiai elemeit vázolja: a technológiát, a szellemi tulajdonjogok védelmét, az elektronikus védelmet, a jogvédelmet és a biztonságot, a média tulajdonjogot, valamint továbbra is a verseny szerepét.

A negyedik fejezet *az információs társadalom lehetséges építőkockáit* mutatja be, amelyek lehetnek a már meglévő hálózatok megerősítése és az újak létrehozásának felgyorsítása, kiemelve, hogy az élenjáró információs technológiákkal kombinált hírközlő rendszerekre

[49] Forás: http://www.mek.iif.hu/porta/szint/muszaki/szamtech/wan/hatasok/bangemn.hun [2012-04-15]

épülő új alapszolgáltatásokra van szükség. Az idő- és távolságbeli korlátozásokat feloldották az információt hordozó hálózatok és alapszolgáltatások, amelyek lehetővé teszik a felhasználói csoportok számára testre szabott megoldásokat kínáló alkalmazások használatát.

A jelentés ötödik fejezete hangsúlyozta, hogy a politikai beavatkozás szükségessége mellett az információs infrastruktúra kiépítésének és működtetésének *finanszírozása elsősorban a magánszektor feladata,* amelynek biztosításához azonban stabil jogi-szabályozási keretekre van szükség.

A Bangemann-jelentésben tehát a legfontosabb a versenyszellem hangsúlyozása volt, az a meggyőződés, hogy a szabad, de jól szabályozott, egyenlő feltételekkel zajló versengés lehet csak alkalmas a legjobb információs társadalom felépítésére, feltételezve, hogy az információs forradalom majd új piacokat hoz létre, és egyben megváltoztatja a gazdaság működésének logikáját is. A jelentés tehát alapvetően olyan ideológiát képviselt, amely az információs társadalmat inkább szűken, csak gazdasági vonatkozásaiban látta.

4.1.2. A Bangemann-jelentés után

A Bangemann-jelentést követően az Európai Bizottság kidolgozta az „Európa útja az információs társadalom felé: Akcióterv" *(Europe's Way to the Information Society – an Action Plan)* című új dokumentumot, amely eredetileg csak az 1994. és 1995. évekre írt elő feladatokat, de folyamatos felülvizsgálatával naprakész tennivalókat jelölt ki a későbbi évekre is, egészen 1998-ig, érvényét csak az új *eEurope* Akcióterv megjelenésével vesztette el. Az Európai Unióban 1994-ben kibontakozó információs politika tehát elsősorban gazdasági, másodsorban jogi-szabályozási, harmadsorban pedig egyfajta promóciós feladatként értelmezte az információs társadalommal kapcsolatos tennivalókat. Kifejezetten a számítógépes fenyegetésekre vonatkozó védelmi célkitűzések még nem voltak jelen a programokban.

1997-ben az EU az egységesebb infrastruktúra kiépülése érdekében a telekommunikáció, a média és az egész informatikai eszközrendszer konvergenciájának és fokozatos egybeolvadásának az elősegítésére koncentrált, mind a szabályozások terén, mind gazdasági értelemben. A konvergencia piaci folyamatára válaszul a Bizottság kidolgozta a *konvergenciáról szóló Zöld Könyvét*[50], amely javaslatokat fogalmazott meg az infokommunikációs eszközök használatában rejlő előnyök minél átfogóbb kiaknázása érdekében. A zöld könyv alapján a konvergencia kiemelt területei: otthonról végzett banktevékenység, vásárlás az Interneten, hangtovábbítás az Interneten, e-mail, adat- és World Wide Web hozzáférés a mobiltelefon-hálózatokon keresztül, a háztartások és vállalkozások vezeték nélküli kapcsolata, adatszolgáltatások a digitális közvetítési platformokon keresztül, televízióval kombinált on-line szolgáltatások, audiovizuális szolgáltatások web-en keresztüli közvetítése *(webcasting)*. A Zöld Könyv elsősorban a konvergencia alapját képező infrastruktúrára koncentrált, amely az információs társadalom szolgáltatásainak megteremtését és azok fogyasztókhoz való továbbításának lehetőségét teremti meg, és amely a későbbieken megalapozhatja az európai közösség gazdaságának versenyképességét.

[50] European Commission, Green Paper on the convergence of the telecommunications, media and information technology sectors, and the implications for Regulation - Towards an information society approach, COM/97/0623 final, 1997. december 3.

4.2. Európa információs politikája: *eEurope* (1999–2005)

Az *eEurope* program az 1990-es évek európai információs fejlődésének szerves folytatása, mégis új korszaknak tekinthető, mivel 1999-ig az információs politikai intézkedések főként gazdasági célúak voltak. Míg korábban a társadalmi szempontok lényegében csak a retorika szintjén jelentek meg, 1999-től az addig háttérbe szoruló társadalmi érzékenység kezdett konkrét akciókban is testet ölteni. Ezeknek a magas szintű megvalósításához azonban új stratégiára és azon alapuló új akciótervre is szükség volt.

Ennek szellemében 1999. december 8-án az Európai Bizottság útjára indította az „eEurope: információs társadalom mindenkinek" *(eEurope: An Information Society for All)*[51] kezdeményezést (röviden: eEurope), amelynek célja az információs társadalomba való átmenet európai folyamatainak felgyorsítása, az elért eredmények hozzáférhetővé tétele az Európai Unió valamennyi polgára számára. A program jól illeszkedett az Európai Tanács által 2000 márciusában elindított „lisszaboni stratégiá"-hoz, amely célként határozta meg, hogy az Európai Uniónak a világ legversenyképesebb tudásalapú társadalmává kell válnia 2010-re. Ebben a gazdasági növekedést, a foglalkoztatottság növelését, a társadalmi integráció mélyítését sürgető akcióterv megvalósulásában jutott továbbra is kulcsszerep az információs és kommunikációs technológiáknak. Az eEurope megőrizte a korábbi korszak (1993–1999) legfontosabb gazdasági célkitűzéseit, miközben azokkal egyenrangúvá tette a társadalmi fejlődés elősegítését.

A célok elérése érdekében a következő konkrét feladatokat tűzték ki: 1) Valamennyi állampolgárt, otthont és iskolát, minden üzletet és hivatalt be kell vonni a digitális korszakba és a hálózatokba. 2) Digitálisan képzett Európát kell kialakítani, az új elképzelések finanszírozására és valóra váltására kész vállalkozói kultúrával alátámasztva. 3) Biztosítani kell, hogy a folyamat szociálisan befogadó jellegű legyen, erősítse a fogyasztói bizalmat és a szociális kohéziót.

Az eEurope információs politika végrehajtására az Európai Bizottság az eEurope Akciótervet *(eEurope Action Plan)*[52] dolgozta ki, amely a legfontosabb teendők áttekinthetőbbé és közérthetőbbé tétele érdekében átcsoportosította a tevékenységi irányokat, három fő csoportba sorolva a kismértékben módosított *eEurope* program célkitűzéseit: 1) Az internethez való hozzáférést mindenütt biztosító infrastrukturális háttér kiépítése (olcsó, gyors és biztonságos internethasználat). 2) Az emberek felkészítése az információs kihívásra. 3) Az internethasználat területeinek fejlesztése.

Már az *eEurope* program is célul tűzte ki az információs társadalom fejlesztésére irányuló törekvések kiterjesztését az újonnan csatlakozó országokra, ennek érdekében 2001. június végén az *eEurope* mintájára napvilágot látott az *eEurope+* program akcióterve *(eEurope+ 2003: A co-operative effort to implement the Information Society in Europe – Action Plan),* amely a tagjelölt és a csatlakozásban bízó országok számára jelölt ki fejlesztési irányvonalakat. Az egyik fő cél az egységes szabályozási keretfeltételek megteremtése volt az új gazdaságba való átmenethez. Az *eEurope+* program részleteinek kidolgozásakor a csatlakozásra váró országok túlnyomó része már rendelkezett saját nemzeti információs stratégiával (Magyarország például nem).

---

[51] eEurope, An Information Society For All, Communication on a Commission Initiative for the Special European Council of Lisbon, 23 and 24 March 2000.

[52] eEurope 2002 An Information Society For All Action Plan prepared by the Council and the European Commission for the Feira European Council, 19-20 June, 2000, Objective 3 b) Forrás: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0140:FIN:EN:PDF [2012-02-19]

Az összeegyeztetési folyamat problémáit az akcióterv készítői úgy látták megoldhatónak, ha változtatás nélkül átveszik az EU programjában megfogalmazott törekvéseket, de azok megvalósításához saját belső határidőket és ellenőrzési módszereket rendelnek. A tizenhárom csatlakozásra váró ország információs programja az alábbiakban felsorolt célokat tartotta elsőrendűnek: 1) Az információs társadalom megalapozása érdekében cél a megfizethető árú telekommunikációs szolgáltatások hozzáférhetővé tétele mindenki számára, és az információs társadalommal kapcsolatos részek átvétele a közös európai joganyagból. 2) Olcsó, gyors és biztonságos internet. 3) A befektetés tárgya: emberek és készségek. 4) Az internet használatának ösztönzése és az *online környezet védelme*. A program legfőbb célja az Európai Unión belül addig kevésbé jelentkező digitális megosztottság minimalizálása volt.

4.3. Az *eEurope2005* – a széles sávú internethasználat programja

Európa számára 2002-ben egyértelmű volt, hogy a jövő információs társadalmának szociálisan egységes társadalomnak kell lennie. Az *eEurope* és az *eEurope+* programok lezárulását követő időszakra kidolgozott *eEurope2005* program akciótervében ezért az „információs társadalom mindenkinek" jelszó már nem az infrastruktúrára és a hálózatok kiépítésére, hanem elsősorban az interneten elérhető tartalomra és az új szolgáltatásokra, a mennyiség helyett a minőségre vonatkozott. Az új akcióterv keretében a tagállamoknak ösztönözniük kellett a *biztonságos*, széles sávú internet-hozzáférés lehetőségének megteremtését mindenki számára. A program célja az e-kormányzat, az elektronikus oktatási és egészségügyi szolgáltatások, a dinamikus e-kereskedelmi környezet, az online közszolgáltatások, az informatikai rendszerek biztonságának megvalósítása volt.

4.4. Az *i2010* kezdeményezés

A szupranacionális szintű akciótervek implementációját tekintve 2005-ben Európa nemzetállamainak információs fejlettsége meglehetősen eltérő képet mutatott. A „*többsebességes Európa*" képe a nagyratörő stratégiák és akciótervek ellenére sem változott meg igazán, és továbbra sem jött létre olyan központi szervezet, amely kikényszeríthetné a szükséges lépések megtételét nemzetállami szinten.

Az „i2010: Európai információs társadalom a növekedéséért és foglalkoztatásért" kezdeményezés[53] 2005. június 1-jén nyilvánosságra hozott alapdokumentumában célként a „mediatizált információs társadalom" építését jelölte meg. Bár az új program már nem az *eEurope* programcsalád része, mégis megőrzött néhány elemet az *eEurope2005* célkitűzései közül: ilyen például a széles sávú internet népszerűsítése és a minőségi tartalom biztosítása a felhasználók számára.

Bár a lisszaboni célok eredetileg 2010-re kitűzött elérése megvalósíthatatlanná vált, az új feladatok meghatározása továbbra is a világ legversenyképesebb tudásalapú társadalmának és gazdaságának megteremtésének jegyében zajlott. Az Európai Tanács ennek értelmében a 2005-ben arra az álláspontra helyezkedett, hogy a fenntartható növekedés a tudás és az innováció függvénye, ehhez pedig elengedhetetlen az információs és kommunikációs technológiák alkalmazása a közszolgáltatásokban, a kis- és középvállalkozásoknál és a háztartásokban egyaránt, vagyis ki kell építeni a „befogadó" információs társadalmat.

[53] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions „i2010 – A European Information Society for growth and employment", SEC(2005) 717, Brussels, 1.6.2005, COM(2005) 229 final.

Az Európai Bizottság a fenti célok elérése érdekében az alábbi prioritásokat jelölte meg. *Az egységes európai információs tér létrehozása keretében* cél a széles sávú internet biztosítása és népszerűsítése, a biztonság garantálása és a szükséges jogi háttér megteremtése a minél színvonalasabb online tartalom előállítása érdekében, az interoperabilitás, azaz a különféle rendszerek, platformok és eszközök közötti átjárhatóság biztosítása, valamint a biztonság, azaz az illegális tartalom elleni küzdelem, a csalások visszaszorítása, a felhasználói bizalom elősegítése. *Az információs és kommunikációs technológiák kutatásával kapcsolatos befektetések és az innováció ösztönzése* keretében cél a világszínvonalú kutatás és innováció az IKT terén, felzárkózás Európa vezető versenytársaihoz. Cél továbbá a *befogadó európai információs társadalom létrehozása,* mivel a társadalmi, gazdasági és területi kohézió nélkülözhetetlen az Unió megfelelő működéséhez, és ennek megteremtéséhez feltétlenül szükség van az információs társadalom kiépítésére. Az Unió a társadalom elöregedése miatt ugyanakkor komoly demográfiai problémák elé néz, melyek leküzdésében – például az idősek részleges továbbfoglalkoztatásának, illetve a szabadidő tartalmas eltöltésének megkönnyítésével – szintén segíthetnek az információs és kommunikációs technológiák.

4.5. Az Európa 2020 program

A Bizottság 2010-ben *„Európa 2020”* néven új politikai stratégiát javasolt a foglalkoztatás, a termelékenység és a társadalmi kohézió növekedésének támogatása érdekében.[54] A stratégia keretében a Bizottság hét kiemelt kezdeményezést indított be, amelyek közül kiemelendő az *Innovatív Unió*, amely támogatja az innovatív termékek és szolgáltatások létrehozását, különösen az éghajlatváltozás, az energiahatékonyság, az egészségügy és a társadalom elöregedése terén, valamint az *Európai Digitális Menetrend*, amely kezdeményezés célja, hogy az információs és kommunikációs technológiák (IKT-k) alkalmazásának kulcsfontosságú szerepet jelöljön ki Európa 2020-ra kitűzött céljainak sikeres megvalósításában. A Digitális Menetrend[55] tehát az Európai Unió növekedésére vonatkozóan 2020-ig szóló célkitűzéseket meghatározó Európa2020 stratégia hét pillérének egyike, amely az információs és kommunikációs technológiákban rejlő lehetőségek hatékonyabb kiaknázását javasolja az innováció, a gazdasági növekedés és a haladás előmozdítása érdekében.

Az információs és kommunikációs technológiák ágazatának és infrastruktúráinak (a továbbiakban IKT) gazdasági és társadalmi jelentőségét több az innovációról és a gazdasági növekedésről a közelmúltban született beszámoló is kiemeli: mint például az i2010 félidős értékeléséről szóló közlemény[56], az Európai Unió éves gazdasági jelentései[57], vagy az OECD beszámolója.[58] Az IKT a társadalom valamennyi szegmense számára elengedhetetlenül fontos: a vállalkozások mind a közvetlen értékesítéshez, mind belső folyamataik hatékony lebonyolítására az IKT-ágazat által előállított termékeket használják, a termelékenység növekedésének 40 %-a az IKT-knak köszönhető.[59]

---

[54] Európa 2020 – Az intelligens, fenntartható és inklúzív növekedés stratégiája [COM(2010) 2020].
[55] A Bizottság közleménye (2010. május 19.) az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Az európai digitális menetrend [COM(2010) 245] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:HU:PDF [2012-04-15]
[56] COM(2008) 199.
[57] 2007. évi jelentés az EU gazdasági helyzetéről. Forrás: http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf [2012-04-15]
[58] http://www.oecd.org/dataoecd/1/29/40821707.pdf [2012-04-15]
[59] Lásd bővebben: http://epp.eurostat.ec.europa.eu [2012-04-15]

4.6. Az Európai Digitális Menetrend

A Digitális Menetrend hét kiemelt tevékenységi területre koncentrál, célkitűzései között szerepel az egységes digitális piac létrehozása, az interoperabilitás javítása, az internetbe vetett bizalom és az online biztonság előmozdítása, gyorsabb internet-hozzáférés, a kutatási és fejlesztési beruházások növelése, a digitális ismeretek elterjesztése, valamint az IKT alkalmazása olyan társadalmi kihívások megoldására, mint például a klímaváltozás.

1. Egy élénk egységes digitális piac kialakítása: E program keretében a cél, hogy a kereskedelmi és kulturális szolgáltatásokhoz az EU-ban országhatároktól függetlenül, a lehető legteljesebb mértékben lehessen hozzáférni. A dokumentum megállapította, hogy az EU online piaca még mindig megosztott, a jogi és jogvédelmi bizonytalanságok akadályozzák az európai távközlési és digitális szolgáltatásokhoz és tartalomhoz való hatékonyabb hozzáférést. Összehasonlításképpen hivatkozik az online zeneletöltés tekintetében az Amerikai Egyesült Államokra, ahol négyszer annyi zenét töltenek le, mint az EU-ban. A megoldás az egységes szerzői jogi szabályozás megteremtése és a jogkezelés és a határokon átnyúló engedélyezési eljárások leegyszerűsítése. Emellett a további intézkedések szükségesek például az elektronikus fizetések és számlázás, a határokon átnyúló internetes tranzakciók egyszerűsítése vagy a jogérvényesítés terén az online vitarendezés hatékonyabbá tétele érdekében.

2. Az interoperabilitás: Az IKT termékeknek nyitottaknak és együttműködésre képesnek kell lenniük, hogy lehetővé tegyék az összekapcsolásokat és az újítást, inspirálva az innovatív alkotó tevékenységet. Az internet nyílt architektúrája révén több milliárd felhasználó kapcsolódhat világszerte interoperábilis készülékekhez és alkalmazásokhoz, azonban az IKT előnyeinek teljes körű kihasználásához a szabványok optimálisabb meghatározásával, alkalmazásával tovább kell növelni a készülékek, alkalmazások, adattárolók, szolgáltatások és hálózatok átjárhatóságát.

3. A bizalom és a biztonság fokozása: Az eddig körvonalazott célkitűzések alapvető feltétele az információs és kommunikációs technológia biztonságába vetett hit erősítése, magának az IT biztonságnak a javítása az informatikai támadásokra adott, megfelelően koordinált európai válasz és a személyes adatokat védő szabályozás megerősítése. A számítástechnikai fenyegetések elhárítása és a védelem megerősítése a digitális társadalom közös felelőssége, melyből a részüket mind az egyéneknek, mind a magán- és állami szervezeteknek ki kell venniük. A szexuális kizsákmányolás, a káros tartalmak (pl.: gyermekpornográfia) elleni küzdelem érdekében országos és uniós figyelmeztető platformok létrehozása indokolt, kiegészítve a káros tartalmak eltávolítását vagy megtekintésének megakadályozását célzó intézkedésekkel. Szükséges továbbá kockázat-tudatosság erősítése különféle oktatási tevékenységek és a szélesebb közönségnek szóló figyelemfelkeltő kampányok révén. Az érintett ágazatokat önszabályozó rendszerek további kifejlesztésére és alkalmazására kell ösztönözni, különös tekintettel a szolgáltatásaikat igénybe vevő kiskorúak védelmére.

A fejezet kiemeli, hogy a kritikus informatikai infrastruktúrák védelméhez kapcsolódó cselekvési terv valamint a stockholmi program végrehajtásáról szóló cselekvési terv hatékony és gyors végrehajtásához az intézkedések széles spektrumára lesz szükség a hálózat- és adatbiztonság és a számítógépes bűnözés terén. A valós idejű reagálás érdekében például számítógépes szükséghelyzeteket kezelő csoportok jól működő, kiterjedt hálózatát kellene létrehozni Európában, beleértve egy európai intézményeket védő egységet is. Szükség van továbbá egy személyazonosság-kezelési stratégiára is,

mindenekelőtt a hatékony és biztonságos e-kormányzati szolgáltatások érdekében. Végül a biztonsági fenyegetések hatékony mérséklése és elhárítása céljából globális szintű együttműködést kell szervezni a releváns szereplők között. Operatív szinten a számítógépes bűnözés elleni küzdelemben nemzetközileg koordinált, célzott adatvédelmi intézkedésekre, valamint közös fellépésre van szükség a megújított Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) támogatásával.

4. A nagysebességű és szupergyors internethez való hozzáférés javítása: Egyértelmű, hogy a polgárok, a gazdasági élet szereplőinek vagy az állami szervek eljárásának az online területre történő terelése feltételezi az eddig elterjedtnél gyorsabb internet-hozzáférést. A negyedik célkitűzés alapján 2020-ra mindenki részére elérhetővé kell tenni a legalább 30 Mbps, a háztartások legalább felének pedig a legalább 100 Mbps sebességű internet-hozzáférést. A dokumentum e körben hivatkozik Európa lemaradását jelző adatokra, amely szerint az európaiaknak csupán 1 %-a rendelkezik nagysebességű üvegszálas internetkapcsolattal, szemben a japánok 12 %-ával és Észak-Korea 15 %-ával.

5. A kutatás és fejlesztés fellendítése az IKT területein: A menetrend részeként az EU-nak még több forrást és még több ösztönzést kell nyújtania a K+F projekteknek, hogy a legjobb ötletek piacra juthassanak, ezáltal tovább növelve a szektor gazdasági jelentőségét. A hivatkozott adatok szerint az EU-beruházások mértéke e téren az amerikainak kevesebb, mint fele.

6. A számítógépes ismeretek bővítése az online szolgáltatásokhoz való hozzáférés terén: a program célja a technológiától távolmaradók aktivizálása és bevonása az online felhasználások területén a digitális megosztottság csökkentése érdekében. A dokumentum megállapításai szerint az európaiaknak több mint fele (250 millióan) használja az internetet napi szinten, 30%-uk azonban még soha nem próbálta. Mivel a gazdasági élet, a közszolgáltatások, a szociális és egészségügyi szolgáltatások, az oktatás és a politikai élet egyre nagyobb mértékben áthelyeződnek a világhálóra, ezért szükséges a lehető legtöbb polgár „képzése”.

7. A hetedik programrészként az IKT lehetőségeinek felszabadítása révén a technológia ésszerű felhasználásába történő befektetések segíthetnek megtalálni a megoldást például olyan járulékos kérdésekre, mint az energiafogyasztás csökkentésére, az idős polgárok támogatására, a betegek érdembeli tájékoztatásának stb.

4.7. Az EU információs stratégiái összegezve

Az Eu információs társadalom stratégiáit összegezve a következők állapíthatók meg:

1. A fejlesztési programok részeként kiemelt fontosságú egy a nyilvános információ-feldolgozó és -szolgáltató létesítményekből álló információs infrastruktúra kiépítése, amelynek segítségével bárki, bárhol, bármikor képes lesz az általa igényelt bármilyen információhoz könnyen, gyorsan és olcsón hozzájutni.

2. Ugyancsak kiemelt fejlesztési terület a társadalom legfontosabb alrendszereinek informatizálása és ezzel párhuzamosan a polgárok tudásának bővítése.

3. Míg a harmadik szempontot az információs iparágak fejlesztési politikája jelenti, amelynek célja a húzóágazat kiemelt fejlesztése a gazdaság egészének informatizálása és ezzel növekedése érdekében.

Az említett irányvonalak mentén a cél egy egységes, szabad, határokon átívelő online gazdaság és társadalmi együttélés (quasi európai virtuális világ) kiépítése, amelynek mind több európai polgár az aktív tagja, és amely az európai gazdasági fejlődés alapja. A stratégiák keretében tehát az elérhető tartalmakhoz való hozzáférés biztosítása a biztonságos és gyors infrastruktúrán keresztül, valamint a tartalom előállításának ösztönzése, az e célok elérést biztosító kutatás-fejlesztés erősítésével az Eu aktív jogharmonizációs tevékenységét igényli.

A stratégiák célkitűzései jól érzékeltetik a mindennapi élet formálódó virtuális színtereit, az érintett társadalmi viszonyokat és azok változását, a fejlődés irányát és a felmerülő kockázatokat. A büntetőjogi szabályozást tehát a fent ismertetett társadalmi érdekek védelmében, azokra figyelemmel kell kialakítani.

5. A SZÁMÍTÓGÉPES FENYEGETÉSEK ÉRÉKELÉSE A STRATÉGIÁK KERETÉBEN

5.1. A számítógépes bűnözés elleni fellépés felé

Az ismertetett uniós stratégiák és jelentések alapján megállapítható, hogy az információs és kommunikációs technológiák, rendszerek, szolgáltatások, hálózatok és infrastruktúrák egy része létfontosságú az európai gazdaság és társadalom számára, mivel vagy alapvető termékek és szolgáltatások előállítására szolgálnak, vagy más kiemelt jelentőségű infrastruktúrák alapját képezik. Mivel az ilyen infrastruktúrák működésében bekövetkező zavar, azok megsemmisülése súlyos hatással lenne az alapvető társadalmi funkciók működésére nézve, ezért a létfontosságú informatikai infrastruktúrák (kiemelt) büntetőjogi védelme indokolt.

A Bizottság annak tudatában, hogy mihamarabb össze kell hangolni az elektronikus kommunikációban és szolgáltatásokban érdekeltek bizalmának növelésére tett erőfeszítéseket, az i2010 stratégia célkitűzéseire figyelemmel 2006-ban elfogadta a biztonságos információs társadalomra irányuló stratégiát *(A Strategy for a secure information society – Dialoge, partnership and empowerment).*[60] Az új program feladata volt, hogy a Bizottság korábbi javaslatába, a 2001-ben elfogadott a Hálózat- és Információbiztonság *(Network and Information Security: Proposal for a European Policy Approach of 2001. (NIS))*[61] új életet leheljen. Az új stratégia az információs társadalom és a biztonság aktuális állapotát és a lehetséges fenyegetéseket felmérve meghatározta, milyen további lépések megtételére van szükség, így például a kiemelt jelentőségű informatikai infrastruktúrák védelme *(critical information infrastructure protection)* érdekében.

Ezt követően a Bizottság 2007-ben közleményt fogadott el *„A számítógépes bűnözés elleni küzdelemre vonatkozó általános politika felé”* címmel.[62] A közlemény a számítógépes bűnözés három csoportkörét különbözteti meg. Az első kategóriába a bűncselekmények hagyományos formáit sorolja, úgymint csalás vagy hamisítás (az értekezés témáját illetően ide sorolható a zaklatás is). A második kategória az illegális tartalom elektronikus médián keresztüli közzétételére vonatkozik (pl. gyermekek szexuális kizsákmányolásával kapcsolatos anyagok, szerzői művek jogosulatlan felhasználása). A harmadik kategóriába az elektronikus hálózatokkal kapcsolatos bűncselekmények tartoznak, úgymint az információs rendszerekkel szembeni támadások, a hozzáférés megtagadása és a hackertevékenység. A közlemény szerint mindhárom bűncselekmény-kategória közös jellemzője, hogy az elkövetés terjedelme, valamint az adott bűncselekmény és hatásai közötti földrajzi távolság igen jelentős lehet, következésképpen az alkalmazott nyomozási módszerek technikai szempontjai gyakran ugyanazok.

A közlemény a következő tendenciákra hívta fel a figyelmet: a számítógépes bűncselekmények száma növekszik, és a bűnözés egyre kifinomultabbá és nemzetközibbé válik, a számítógépes bűnözésben egyre inkább részt vesznek a szervezett bűnözői csoportok, a határokon átnyúló bűnüldözési együttműködés alapján folytatott európai büntetőeljárások száma azonban nem növekszik. A felismert káros folyamatok ellen a közlemény szorgalmazta a tagállamok közötti mind szorosabb együttműködést egy koherens uniós politikai keret létrehozását és a számítógépes bűnözéssel kapcsolatos

[60] COM(2006) 251.
[61] COM(2001) 298.
[62] COM(2007) 267.

tudatosság erősítését, a bűnüldöző szervek állományának képzését. Az uniós fellépés leggyengébb pontjának a közlemény továbbra is a határokon átnyúló operatív együttműködés struktúráinak hiányát tartja.

5.2. A számítógépes bűnözés a digitális menetrendben

A digitális menetrend célkitűzéseinek megvalósítását számos akadály nehezíti, így természetesen a számítógépes bűnözés terjedése és a hálózatokkal szembeni bizalomvesztés kockázata. Az akadályok leküzdése érdekében tehát meg kell erősíteni a számítógépes bűnözés, az internetes pornográfia, valamint a magánélet és a személyes adatok védelmének megsértése elleni küzdelmet célzó politikát. A kitűzött célok elérése érdekében a Bizottság feladata a hálózat- és információbiztonsággal, valamint a számítógépes támadások elleni küzdelemmel kapcsolatos intézkedések kidolgozása, ezzel párhuzamosan a tagállamoknak gondoskodniuk kell jól működő nemzeti hálózatok kialakításáról, meg kell kezdeniük a nagyléptékű internetes támadások szimulációját, valamint az országos figyelmeztető platformjaikat az Europol számítógépes bűnözéssel kapcsolatos platformjához kell igazítaniuk. A digitális menetrend kiemeli, hogy az érdekelt feleknek össze kell fogniuk az IKT infrastruktúrák biztonságának és ellenálló képességének biztosításához, a megelőzésre, felkészültségre és tudatosságra koncentrálva, valamint a kibertámadások és kiberbűnözés új és egyre kifinomultabb formáira reagáló eredményes és koordinált mechanizmusok kidolgozásával. Ez a megközelítés biztosítja, hogy a kihívásnak mind a megelőzési, mind a reakcióval kapcsolatos dimenzióit is megfelelően figyelembe vegyék.

A közelmúltban a digitális menetrendben bejelentett alábbi intézkedéseket hozták meg: a Bizottság 2010 szeptemberében az információs rendszerek elleni támadásokról szóló *irányelvjavaslatot*[63] fogadott el. A javaslat célja a kiberbűnözés elleni küzdelem megerősítése a tagállamok büntetőjogi rendszerének közelítésével, valamint a bírósági és más illetékes hatóságok közötti együttműködés javításával, emellett további rendelkezések bevezetését szorgalmazza a kibertámadások új formái, különösen a botnetek elleni fellépés terén. Ezt kiegészítendő a Bizottság egy, az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) megerősítésére és modernizálására irányuló megbízásra vonatkozó javaslatot[64] nyújtott be a bizalom erősítése és a hálózatbiztonság javítása érdekében. Az ENISA megerősítése és korszerűsítése hozzájárulna ahhoz, hogy az EU, a tagállamok és a magánszektor szereplői felkészültebben és szakszerűbben tudják megelőzni és felderíteni a kiberbiztonsággal kapcsolatos kihívásokat, és hatékonyabb válaszlépéseket adhassanak azokra.

Végül, de nem utolsósorban az európai digitális menetrend, a stockholmi program[65] és az EU belső biztonsági stratégiájának[66] (ISS) megvalósítása is kihangsúlyozza a Bizottság elkötelezettségét egy olyan digitális környezet mellett, amelyben minden európai polgár teljes mértékben kibontakoztathatja gazdasági és társadalmi lehetőségeit.

5.3. A kritikus informatikai infrastruktúrák védelme

A Bizottság 2009-ben *„Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása”*

[63] COM(2010) 517 végleges.
[64] COM(2010) 521.
[65] COM(2010) 171.
[66] COM(2010) 673.

címmel közleményt[67] fogadott el a kritikus informatikai infrastruktúrák védelméről, amelyben körvonalazta a létfontosságú információs és kommunikációs technológiai infrastruktúra biztonságának és ellenálló képességének megerősítésére szolgáló tervet (CIIP cselekvési terv). A terv célja a felkészültség, biztonság és ellenálló képesség magas szintre fejlesztésének támogatása és ösztönzése nemzeti és európai szinten egyaránt. A CIIP cselekvési terv öt pilléren nyugszik: felkészültség és megelőzés, felderítés és reagálás, hatások enyhítése és helyreállítás, nemzetközi együttműködés és európai kritikus infrastruktúrákra vonatkozó követelmények az IKT-ágazat számára. A terv meghatározza az egyes pillérekre vonatkozóan a Bizottság, a tagállamok, illetve az ágazat által az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) támogatásával elvégzendő tevékenységet.

Az információs társadalom stratégiáiban sorolt célkitűzéseknek való megfelelés érdekében a Bizottság 2011-ben újabb közleményt adott ki a kritikus informatikai infrastruktúrák védelméről *„Eredmények és következő lépések: a globális kiberbiztonság felé”* címmel.[68] A közlemény áttekinti a CIIP cselekvési terv 2009-ben történt elfogadása óta elért eredményeket, minden tevékenység esetében leírja a következő, európai és nemzetközi szintű lépéseket, a kihívások globális dimenziójára koncentrálva kiemeli a tagállamok és a magánszféra között nemzeti, európai és nemzetközi szinten folytatott együttműködés fejlesztésének fontosságát a kölcsönös globális függőségek megfelelő kezelése érdekében. A CIIP cselekvési tervet kísérő hatásvizsgálat[69], valamint a magán- és állami szféra érdekelt felei által készített számos elemzés és jelentés nemcsak Európa társadalmi, politikai és gazdasági IKT-függőségét hangsúlyozza, hanem a – természet vagy emberi tevékenység által okozott – fenyegetések számának, kiterjedésének, kifinomultságának és potenciális hatásainak folyamatos növekedését is.

A közös fellépés elmélyítésének oka, hogy újszerű és technológiai szempontból kifinomultabb fenyegetések jelentek meg, amely fenyegetések globális szintű geopolitikai vonatkozásai is egyre egyértelműbbé váltak. Már nem csupán nemzetgazdasági megfontolások szerinti fejlesztésekről van szó, az információtechnológiai eszközök politikai és katonai erőfölény biztosítása érdekében történő felhasználásnak – beleértve az offenzív informatikai nyomásgyakorlás képességét a „kiberháború” és „kiberterrorizmus” életszerűsége miatt – nemzetbiztonsági szintű felértékelődésének folyamata is zajlik.

A megjelenő fenyegetéseket a Bizottság szerint a következő kategóriák szerint célszerű csoportosítani:[70]

- *haszonszerzés céljából elkövetett*, mint például a gazdasági és politikai kémkedésre használt „irányított állandó fenyegetések” (pl. a GhostNet[71]), személyazonosság-

[67] COM(2009) 149.
[68] COM(2011) 163.
[69] SEC(2009) 399.
[70] COM(2009) 149.
[71] A Bizottság által említett példa: az Information Warfare Monitor projekt jelentései: Tracking GhostNet: investigating a Cyber Espionage Network” [A GhostNet felgöngyölítése: nyomozás egy informatikai kémhálózat után] (2009) és „Shadows in the Cloud: Investigating Cyber Espionage 2.0” [Árnyékok a felhőben: nyomozás az informatikai kémkedés után 2.0] (2010).

lopás, a kibocsátás-kereskedelmi rendszer[72] vagy kormányzati informatikai rendszerek ellen irányuló támadások;

- *a szolgáltatás megzavarására irányuló*, mint például a megosztott szolgáltatás-megtagadással járó támadások, a botneteken keresztül történő kéretlen spamelés, azaz reklámlevél-küldés (pl. a 7 millió számítógépet összefogó Conficker hálózat és a spanyolországi, 12,7 millió gép fölött rendelkező Mariposa hálózat[73]), Stuxnet[74] és a kommunikációs csatornák megszakítása.

- *pusztító célú:* ez a forgatókönyv még nem valósult meg, de az IKT-nek a kritikus infrastruktúrák (pl. intelligens hálózatok és vízszolgáltatási rendszerek) terén történő egyre növekvő elterjedését tekintve nem zárható ki a jövőben.

Az információs társadalom globalizációs folyamatai miatt a kihívások nem csak az Európai Uniót érintik, és azokat az EU önerőből nyilvánvalóan nem tudja leküzdeni. Az IKT eszközök, az internet-használat elterjedése hatékonyabb, eredményesebb és gazdaságosabb kommunikációt, koordinációt és együttműködést tesz lehetővé az érdekelt felek között, és az élet minden területén élénk innovációs ökoszisztémát hozott létre, amelyben a fenyegetések a világ minden részéről származhatnak, és a rendszerek közötti globális szintű összeköttetések miatt a világ bármely részét érinthetik. Ezért a Bizottság hangsúlyozta, hogy egy tisztán európai megközelítés nem elégséges az előttünk álló kihívások kezeléséhez. Fontos a következetes és együttműködésen alapuló megközelítés kialakítása az Unión belül, de azt egy, a fő partnereket (adott országokat vagy vonatkozó nemzetközi szervezeteket) bevonó globális koordinációs stratégiába kell beágyazni.

---

72 http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=fr [2012-04-15]

73 A Bizottság által említett példa: a „Future Global Shocks” [Jövőbeni globális sokkhatások], „Reducing systemic cyber-security risks” [A rendszerben rejlő informatikai biztonsági kockázatok csökkentése] 2011 január 14-i OECD/IFP projektet a következő címen: http://www.oecd.org/dataoecd/3/42/46894657.pdf [2012-04-15]

74 Lásd: http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis [2012-04-15]

6. SZABÁLYOZÁSI KÉRDÉSEK II.: A MAGYAR INFORMÁCIÓS STRATÉGIA

6.1. A kezdetek: NIS, eMagyarország

Az információs társadalom fejlesztésének uniós bemutatását követőn a következőkben a magyar viszonyok rövid ismertetésére kerül sor.[75] Egy nemzeti információs stratégia elkészítésének az igénye döntően szakmai kezdeményezésre a gazdasági és civil szféra összefogásával már az 1990-es évek közepén megjelent, amelynek első testet öltött dokumentuma a Nemzeti Informatikai Stratégia (NIS)[76] volt, amely egyfajta stratégia-előkészítő anyagként a tudatos kormányzati szerepvállalást sürgette az Európai Unió Bangemann-jelentéséből kiindulva. Azonban az elkészült szakanyag végül nem került elfogadásra. Ettől függetlenül az egyes területek informatizálása megindult – pl. a Sulinet program az iskolák hálózatba kapcsolásának érdekében – ám hiányzott a programokat egy irányba rendező nemzeti információs társadalom stratégia.

Bár hivatalosan elfogadott információs társadalom stratégia a 2001-ben meghirdetett Széchenyi-tervet és a Nemzeti Információs Társadalom Stratégiát (NITS) megelőzően nem született, néhány dokumentum már az 1990-es évek második felében bemutatta az információs kihívásokat. Ilyen volt például az *eMagyarország*, amely az eEurope első változatának a mintájára készült el 1999 decemberében, de gyakorlatilag a magyar fejlesztésektől függetlenül kezelte az EU irányadó célkitűzéseit. Az eMagyarország nem volt hivatalos dokumentum, civil kezdeményezésre készült el az eredeti dokumentum magyar fordításaként. A *Magyar válasz az információs társadalom kihívásaira* című szakmai vitaanyag a Miniszterelnöki Hivatalon belüli szakanyagként állt elő, és szintúgy nem követte stratégia megírása, csupán egy stratégia-előkészítő szövegnek volt tekinthető. Említésre méltó, de nem hivatalos, nem kormányzati szereplők által készített dokumentum volt a *Magyar Informatikai Charta (MIC)* volt, amelyet 2000 áprilisában mutatott be az INFORUM (Informatikai Érdekegyeztető Fórum). Az anyag elkészítésének hátterét az a meggyőződés adta, hogy az informatika a gazdasági növekedés kulcsfontosságú szektora. Összességében az mondható el, hogy 1994-2000 között el nem ismert prioritásként az információs társadalom témája teljesen háttérbe szorult az általános politikai programokban, valamint tervezésben.

6.2. NITS 1.0

A nemzetközi fejleményeket ellenére az információs társadalom csak jelentős fáziskéséssel, az ezredforduló táján jelent meg hangsúlyosan a kormányzati fejlesztési politikában, amely az Informatikai Kormánybiztosság (IKB) Miniszterelnöki Hivatalon belüli megalakulásával öltött alakot. A politikai tudatosság első jeleként először 2001-ben a Széchényi Terv Információs Társadalom- és Gazdaságfejlesztési Program foglalkozott részletesen az információs társadalommal, amely akkoriban a kormányzat hivatalos nemzeti fejlesztési terveként deklaráltan a tudásgazdaság igényeiből és az információra épülő gazdaság térhódításaiból indult ki, és amely többek között a következő fontosabb irányokat jelölte ki: a kormányzat-közigazgatás fejlesztésében, az eszközellátottság és hozzáférés javításában, az e-gazdasági folyamatok megalapozásában, az információs kultúra és a megfelelő tartalom kiépítésében, illetve az életminőség és tudatosság növelésében. 2001 májusára elkészült az első saját információs társadalom stratégia, a

[75] A cím az ITTK Magyar Információs társadalom jelentés 1998-2008. alapján készült. Forrás: http://www.ekonyvkereso.net/file/05600/05681/05681.pdf [2012-02-19]
[76] http://www.iif.hu/dokumentumok/nis/ [2012-02-19]

Nemzeti Információs Társadalom Stratégia (NITS). Emlékeztetőül, az Európai Unióban ekkoriban, 2000 első félévében dolgozták ki az *eEurope* programot, amely központi prioritásként fogalmazta meg minden területen az információs változások végrehajtását. Míg a Széchenyi-terv informatikai fejezete csupán egy szűken definiált, ad hoc projekt-csoportot rögzített, addig a NITS egy átfogó koncepciót fogalmazott meg az információs társadalom kiépítésére és alapvetően három fő terület – ember, eszköz és tartalom – fejlesztését irányozta elő. Az így létrejött stratégia egyben akcióterv is volt: mindegyik feladathoz rendelt megoldási javaslatokat és határidőket. Az akcióterv csak két évre tervezett, a stratégiát és a hozzá rendelt akciótervet a terület gyors fejlődése miatt évente tervezték felülvizsgálni (ezért kapta a 2001 májusában megjelent stratégia hivatalosan is az 1.0-s verzió megjelölést). A NITS végrehajtása a szabályozás-infrastruktúra, gazdaság, kultúra, oktatás, társadalom, e-kormányzás és intelligens régió illetve elektronikus önkormányzat témaköreire terjedt ki.

6.3. MITS

2002 nyarán az információs kihívások kezelésére a kormány önálló Informatikai és Hírközlési Minisztériumot hozott létre az Informatikai Kormánybiztosság jogutódjaként, illetve ezzel párhuzamosan a Miniszterelnöki Hivatalon belül felállította a Kormányzati Informatika és Társadalmi Kapcsolatok Hivatalát (KITKH, 2004-től Elektronikus Kormányzati Központ). Előbbi az információs társadalom általános építéséért, utóbbi az elektronikus kormányzati fejlesztésekért lett felelős. Az információs fejlettség növelése érdekében az információs jártasságok/tudás („skill") – hozzáférés – és tartalom kérdésköreit kívánták kiemelten kezelni.

Ezt követően 2002-ben elkészült a Magyar Információs Társadalom Stratégiát (MITS) előkészítő tanulmány, hogy rá egy évre a kormányzat határozatot fogadjon el az időközben a tárcák és szakértők bevonásával elkészült MITS végrehajtásáról (1126/2003. [XII.12.] kormányhatározat). Az újabb stratégia hátterében részben a digitális szakadék problémarendszere állt, amely azzal fenyegetett, egyes társadalmi rétegek tartósan kizáródnak a fejlődésből. Az információs társadalom szempontjából kiemelt területeket kezelő minisztériumok önálló ágazati stratégiákat készítettek, amelyek az IHM koordinálása mellett 2003 október végén épültek be a kormány által is elfogadott új stratégiába. A Magyar Információs Társadalom Stratégia (MITS) egy viszonylag hosszú, 10-15 éves időtávra jelölte ki a stratégiai célkitűzéseket, ezzel szemben az egyes központi kiemelt programok általában középtávra, a 2004-2006 közötti időszakra szóltak. A MITS modellje a fejlesztések két alapvető pillérét a *folyamatok korszerűsítésében* és a *szolgáltatások modernizálásában* jelölte meg. Mindkét pillér esetén az érintett területek a következők voltak:

- *Tartalom és szolgáltatások:* ide tartozik a gazdaság (munka, üzlet, közlekedés és agrárium), a közigazgatás (e-kormányzat, e-önkormányzat), a kultúra (Nemzeti Digitális Archívum), az oktatás, az egészségügy és a környezetvédelem.

- *Infrastruktúra:* ide tartozik a szélessávú hálózatok kiépítése (Közháló, NIIF), a hozzáférés/elérés fejlesztése (eMagyarország Pontok), a közcélú, közhasznú adatok, szabványok és szoftver eszközök biztosítása.

- *Tudás és ismeret:* ide tartozik a digitális írástudás megteremtése.

- *Jogi és társadalmi környezet:* ide tartozik a bizalom és biztonságérzet megerősítése és az elektronikus demokrácia kiépítése.

- *Kutatás-fejlesztés:* ide tartozik az információs társadalomhoz köthető kutatási és fejlesztési feladatok rendszerezése.

- *Esélyegyenlőség:* ide tartozik az eInclusion elősegítése, egy e-ernyő kiépítése.

A MITS célkitűzései és programjai illeszkedtek az Európai Unió akkoriban érvényben lévő eEurope stratégiájához, ami lehetőséget adott Magyarország számára, hogy kapcsolódjon a közösségnek az eEurope-ot támogató programjaihoz (pl. IST, eContent, eSafety, IDA stb.), és szintén lehetővé tette, hogy az EU strukturális alapját forrásként felhasználhassák az információs társadalom építéséhez.

6.4. Digitális Magyarország Program és a kritikus infrastruktúrák védelme

2006. után az informatikai tárca beolvadt a Gazdasági és Közlekedési Minisztériumba, ettől kezdve további átfogó modernizációs keret nem készült, a kormányzat az információs társadalom ügyét csupán infrastrukturális kérdésként kezelte. Kiemelt stratégiaként csak 2010-ben jelent meg újra az információs társadalom fejlesztésére irányuló átfogó koncepció a kormányprogram részeként, kezdetben „Digitális Magyarország program 2010-2014." vitairat néven. A dokumentum célja volt, hogy felhívja a figyelmet az infokommunikáció eszközkészletének mozgósítása a Kormányprogramban meghatározott célok elérése, a gazdasági versenyképesség növelése, egy modern európai digitális nemzet megteremtése és a fogyasztói jólét növelése érdekében. A tervezet végrehajtására a Digitális Megújulás Cselekvési Terv szolgált, amely már jól illeszkedett az Europe2020 programhoz.

A Digitális Megújulás Cselekvési Terv részeként kiemelt jelentőséghez jutott a „kritikus információs infrastruktúra védelme" is, amelyet a Terv a következőképpen definiál. Az információs infrastruktúrákon belül különböző rendeltetésű és típusú infrastruktúrahalmazok különböztethetők meg. Felhasználás (alkalmazás) szerint megkülönböztethetünk: a) globális információs infrastruktúrát, b) nemzeti információs infrastruktúrát, és pl. ezen belül védelmi célú információs infrastruktúrát. Rendeltetése szerint az információs infrastruktúrákat két csoportba oszthatjuk, funkcionális és támogató információs infrastruktúrákra. Ha az infrastruktúrákat nemzetbiztonsági szempontból vizsgáljuk, akkor kritikus és sebezhető infrastruktúrákat különböztethetünk meg, melyek működése alapvető fontosságú és nélkülözhetetlen a társadalom működtetéséhez. Amennyiben ezek valamilyen beavatkozás következtében működésképtelenné válnak, az beláthatatlan következményekkel járhat az ország gazdaságára és védelmére, azaz maga az ország biztonsága kerülhet veszélybe. A nemzeti információs infrastruktúra magában foglalja: a) a közszolgálati, kormányzati és magán célú, nagysebességű hálózatokat; b) az információ továbbítására szolgáló műholdas-, földi vezeték nélküli- és vezetékes rendszereket; c) számítógépeket, televíziókat, rádiókat és egyéb eszközöket, melyek segítségével az emberek képesek kihasználni az infrastruktúra adta lehetőségeket, valamint d) az embereket, akik létrehozzák, felhasználják és hasznosítják az információt. Egy ország biztonsága szempontjából kulcsszerepet játszanak a védelmi információs infrastruktúrák, amelyek felölelik a védelmi célú információk továbbítására, feldolgozására, az információ és adat tárolására, kezelésére, visszakeresésére és megjelenítésére szolgáló eszközöket. A nemzeti védelmi infrastruktúra természetesen részét képezi a nemzeti információs

infrastruktúra rendszerének, ezen túlmenően pedig szervesen kapcsolódik a szövetséges védelmi információs közműhöz is.

A dokumentum kiemeli, hogy az elmúlt időszak különböző infrastruktúrák elleni támadásai csak a fizikai dimenzióban realizálódtak, és így az országhatárok bizonyos védelmet jelentettek, addig napjainkban korlátozott erőforrások is elegendőek az infokommunikációs rendszerekre alapozott kritikus infrastruktúráink elleni támadások megtervezésére és kivitelezésére. A különböző egyéni aktivisták, jogosulatlan felhasználók és terroristák aszimmetrikus fenyegetései részben kibővítették, részben pedig felváltották a jól ismert háborús fenyegetettségeket, ezért a katonai és polgári természetű fenyegetések közötti hagyományos határvonal egyre inkább elmosódik.

Természetesen egy-egy infrastruktúrának nem minden eleme tekinthető kritikusnak, még abban az esetben sem, ha kritikus infrastruktúráról beszélünk. Ezért a dokumentum szerint szükség lehet azonosítani és meghatározni azokat az elemeket, amelyek a legkritikusabbak, azaz amelyek támadásával, és amelyek kiesésével, részleges, időleges, vagy teljes működésképtelenségével a legjelentősebb mértékben okozhatók komoly humán (emberi élet) vagy anyagi (gazdasági) kár. Az infrastruktúrák méretének és összetettségének mérése lehetőséget teremthet beazonosítani ezeket a kritikus elemeket.

A kritikus információs infrastruktúrák védelmét gyakran leegyszerűsítik, és egyenlőnek tekintik az informatikai biztonsággal. Azonban ahogy az a kritikus szektorok felsorolásából, valamint az előzőekben felvázolt veszélyekből, illetve támadási formákból is látszik, az informatikai biztonság megteremtése csak egy – bár egy nagyon fontos – eleme a védelmi megoldásoknak. Mivel egy-egy infrastruktúra több másik rendszerrel is kapcsolatban van, ezért azkra is komoly hatással van, ennek analógiáján a védelem megteremtése terén is hasonló komplexitás elérése a cél. Tehát a kritikus infrastruktúráink védelmének egy olyan, átfogó és komplex megoldásnak kell lennie, amely a fizikai védelemtől kezdődően a hálózati biztonságon keresztül számos területre kiterjed. A kritikus infrastruktúrák védelmének kidolgozása, sőt maga a védelem is jórészt állami feladat, még abban az esetben is, ha ezek egyes fő elemei nincsenek állami kézben. Ebben a körben az állam feladata, hogy kijelölje nemzeti kritikus infrastruktúra, valamint az európai kritikus infrastruktúra elemeit, illetve folyamatosan felülvizsgálja.

6.5. A magyar viszonyok számokban

Magyarországi viszonylatban adott egy minden eddigi változásnál intenzívebb, lendületesebb technológiai haladás, és az e mentén kettészakadó társadalom az ismeretekkel és technikával rendelkezőkre, illetőleg mindezeket hatékonyan felhasználókra és a távolmaradókra bontva.

A Központi Statisztikai Hivatal adatai szerint a magyarországi internet-előfizetések száma 2003. évtől 2011 harmadik negyedévéig közel meghatszorozódott, a szám 2011. harmadik negyedévben valamivel kevesebb, mint 4 millióra volt tehető.[77] A mobiltelefon-előfizetések száma a KSH adatai alapján 2011. harmadik negyedévére kb. 11,67 millió.[78] További érdekes adat, hogy a mobilhálózatokban a tárgyidőszak folyamán 2010 III. negyedévéhez viszonyítva 1%-kal több hívást kezdeményeztek, 4%-kal nőtt a mobiltelefonálással töltött összes percidő (egy előfizetésre átlagosan 391 percnyi

[77] Forrás: KSH http://portal.ksh.hu/pls/ksh/docs/hun/xstadat/xstadat_evkozi/e_oni001.html [2012-04-15]
[78] Forrás: KSH http://portal.ksh.hu/pls/ksh/docs/hun/xstadat/xstadat_evkozi/e_onp001.html [2012-04-15]

beszélgetés jutott), és az „okostelefonok” valamint a mobilinternet terjedését jelzi, hogy egy év alatt közel ötödével bővült a mobilhálózatban bonyolított adatforgalom, mialatt az SMS-ek és MMS-ek száma csak 4, illetve 7%-kal növekedett.[79] A KSH 2011. december 8. napján kiadott további adatai alapján elmondható, hogy az internet-előfizetéseken belül a vezeték nélküli szegmens egy év alatt 54%-kal bővült, amely nagymértékű változáshoz erőteljesen hozzájárult az egyre inkább megfizethető mobilinternet. Az összes internet-előfizetés 47%-a a mobilkategóriába tartozott, részaránya egy év alatt közel 10 százalékponttal lett nagyobb.

Az internethasználati szokások tekintetében az Információs Társadalom és Trendkutató Központ (ITTK) Magyar információs társadalom jelentés 1998-2008. című kiadmánya szerint míg 2001-ben a 14 év feletti korosztály 30%-a használt rendszeresen számítógépet, és mintegy 18%-a internetet, addig a 2007-es adatok szerint ugyanezen korosztálynak 52%-a használ rendszeresen vagy alkalmanként számítógépet és 45%-uk internetet.[80] Az ITTK kutatása szerint a magyar kultúra az internethasználat tekintetben kettészakadóban van, azaz míg az online haladásban csak az ország kisebb része vesz részt, az állampolgárok jelentős része egyelőre kimarad e változásokból, amely változások a lemaradóknak egyfajta kulturális „sokkot” fog okozni.[81]

6.6. A számítógépes fenyegetésekre adott magyar válaszok

A Büntető Törvénykönyvről szóló 1978. évi IV. törvénybe viszonylag korán, már 1994. évben bekerült „számítógépes csalás” címmel egy számítógépes érintettségű deliktum. Az 1994. évi IX. törvény a 300/C. §-szal egészítette ki a Btk-t, amely jogszabályhely azóta is a számítástechnikai bűncselekményeket szankcionálja. A törvény indokolása szerint a jogalkotó felismerve a számítógépes technika fejlődésével egyre gyakoribbá váló tulajdont károsító számítógépes manipulációk terjedését és a vagyon elleni bűncselekmények dogmatikájának alkalmazhatatlanságát, szükségesnek tartotta új tényállás kialakítását, amelynek középpontjában a számítógépes adatfeldolgozás eredményének kárt okozó, haszonszerzés céljából történő befolyásolása volt. A számítógépes bűncselekmények magyar büntetőjogi kezdete – hasonlóan a korszak gazdasági indíttatású szabályozási mintáihoz, programjaihoz – kizárólag a vagyoni viszonyokat támadó cselekmények szankcionálására korlátozódott.

A tényállást később a 2001. évi CXXI. törvény módosította – figyelemmel a későbbiekben részletesen elemzett Cyber-crime Egyezmény rendelkezéseire – amely így már magába foglalta a „hacking”-et szankcionáló jogosulatlan belépést számítástechnika rendszerbe, valamint a nem haszonszerzési célú, számítástechnikai adatfeldolgozás manipulálását, továbbá egy újabb, sui generis tényállást iktatott be a 300/E. §-ban a számítástechnikai rendszer védelmét biztosító technikai intézkedések kijátszásának szankcionálása céljából. A 300/C. § tényállásának a támadható jogi tárgyak differenciálására figyelemmel történt módosítása, kiegészítése már jól tükrözi azt a szemléletváltást, amely a számítástechnika és a bűncselekmények kapcsolatának megítélésében végbement. A módosítás óta eltelt tíz év azonban joggal veti fel a kérdést, időszerű volna-e a tényállást revideálni, korszerűsíteni a jelen kor kihívásainak való megfelelése érdekében.

---

[79] KSH Gyorstájékoztató 2011. december 8. Forrás: http://portal.ksh.hu/pls/ksh/docs/hun/xftp/gyor/tav/tav21109.pdf [2012-04-15]

[80] Információs Társadalom és Trendkutató Központ (ITTK) - Magyar információs társadalom jelentés 1998-2008. pp. 39-40.

[81] Információs Társadalom és Trendkutató Központ (ITTK) - Magyar Információs társadalom – éves jelentés 2006. p. 62. http://www.ittk.hu/web/docs/ITTK_MITJ_2006.pdf [2012-04-15]

A számítástechnikai érintettségű bűnelkövetés mind gyakoribbá válása miatt a jogalkotó a fentieken túlmenően további új tényállásokat alkotott (pl.: a bankkártya-csalásokra reagálva), és egyes korábbi tényállások elkövetési magatartásait is bővítette (pl.: magántitok jogosulatlan megismerése, levéltitok megsértése).

Az anyagi jogi jogközelítés fontossága mellett a Bizottság 2009-ben, a kritikus informatikai infrastruktúrák védelméről kiadott közleményében kiemelte, hogy Európa korai figyelmeztető és reagáló képességének megerősítéséhez kormányzati ellenőrzés alatt álló, jól működő számítástechnikai katasztrófaelhárító csoportok (CERT) szükségesek, amelyek működése közös alapképességeken nyugszik. A nemzeti CERT-ek feladata, hogy tagállami szinten serkenteniük kell az érdekeltek motivációját és képességét, hogy részt vegyenek a közpolitikai tevékenységekben a határokon átnyúló együttműködésben és információcserében. E feladat ellátása érdekében az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendelet rendelkezett a kormányzati CERT tevékenységért felelős Nemzeti Hálózatbiztonsági Központ felállításáról. A kormányrendelet 2. § f) pontja olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózataként definiálja a kritikus infrastruktúrát, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak, érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában, és ezért meg kell felelniük az alapvető biztonsági, nemzetbiztonsági követelményeknek. Az értelmező rendelkezés érzékletesen mutat rá az IKT társadalomban betöltött szerepére, és a hozzájuk fűződő biztonsági érdekekre.

7. SZABÁLYOZÁSI KÉRDÉSEK III.: AZ INFORMÁCIÓS TÁRSADALOM BŰNÖZÉSE A NEMZETKÖZI JOGFORRÁSOKBAN

7.1. A kezdeti regionális törekvések

Amint említettem, a számítógépes bűnözés könnyen válik nemzetközivé, hiszen a kárt okozó cselekmények elkövetésének közege illetve eszköze az országokat összekapcsoló nemzetközi hálózat, amely körülmény természetes folyománya, hogy az ellene való harc is csak nemzetközi fellépéssel kecsegtethet a siker esélyével.[82]

A nemzetközi összefogás terén az első jelentős kezdeményezés az OECD (Gazdasági Együttműködési és Fejlesztési Szervezet) által életre keltett ad hoc bizottság felállítása volt, amely 1983. és 1985. között az európai államok számítástechnikai téren kialakult joggyakorlata területén végzett felmérésein alapuló tapasztalatát összegezve közzétette a büntetőjogi reformokat sürgető jelentését *Computer-Related Crime: Analysis of Legal Policy* (Számítógépes bűncselekmények: jogpolitikai elemzés) címmel 1986-ban.

A következő nagyobb volumenű lépésként az Európa Tanács – szakértő bizottságának jelentését alapul véve – 1989-ben kibocsátott egy ajánlást[83] a tagországok számára, mely egy minimális, illetve egy fakultatív listát tartalmazott a számítógépes környezetben elkövethető és szankcionálandó cselekményekről. Az ajánlás a minimális listán szereplő magatartások feltétlen szankcionálását javasolta az egyes államoknak, míg a fakultatív listán szereplő magatartások büntethetőségének előírását az egyes államok belátására bízta.[84] Az OECD minimum listája újabb típusú visszaélésekkel bővült, valamint olyan kérdések is felmerültek, mint a személyes adatok védelme, a sértetti közrehatás, a megelőzés lehetősége, illetve a nemzetek közötti eljárásjogi különbségek orvoslása a nyomozás és a bűnvádi eljárás terén. 1992-ben az OECD irányelveket állított fel az informatikai rendszerek biztonságára nézve, amely egyúttal alapot jelentett egy keretrendszer kidolgozására az államok és a magánszektor között, az Európa Tanács pedig hozzákezdett egy tanulmány elkészítéséhez, amely az eljárásjog és a nemzetközi együttműködés által felvetett új keletű problémák megoldására koncentrál a számítógépes bűncselekmények és az információtechnológia területén. Ennek eredménye egy újabb tanácsi ajánlás lett a büntető eljárásjogi kérdésekről (1995).[85]

Az ENSZ 1994-ben megjelent informatikai bűnözéssel foglalkozó tanulmánya[86] felismerte, hogy a regionális szinten megtett lépések nem elegendőek az informatikai bűnözés megállításához, hiszen a bűncselekmények potenciális kiterjedtsége a nemzetközi telekommunikációs rendszerek egészét átfogja.

A G8 (Group of 8) 1995-ben megalapította az országhatárokon átnyúló bűnözéssel foglalkozó csoportot, a Lyon Group-ot, melynek egyik alcsoportja a számítástechnikai

---

[82] BALOGH, Zs., Az infokommunikációs jogról, *Infokommunikáció és Jog* 2004/2. pp. 45-49.
[83] R (89) 9. számú Ajánlás a számítógépekkel kapcsolatos bűncselekményekről
[84] *A minimum lista tartalma:* számítógéppel kapcsolatos csalás, számítógépes hamisítás, számítógépes adatok károsítása, számítógépes programok rongálása, számítógépes szabotázs, jogosulatlan hozzáférés, távközlés jogosulatlan vétele (lehallgatás), védett számítógépes program jogtalan sokszorosítása, félvezető topográfiák jogtalan sokszorosítása. A *fakultatív lista tartalma*: számítógépes adatok programok megváltoztatása, számítógépes kémkedés, számítógép jogosulatlan használata, védett számítógépes program jogosulatlan használata.
[85] R (95) 13. számú Ajánlás az információs technológiával összefüggő büntető eljárásjogi problémákról.
[86] UN Manual on the Prevention and Control of Computer-Related Crime (ENSZ-tanulmány a számítógépes bűnözés megelőzéséről és szabályozásáról)

deliktumokra specializálódott. A G8-ak állítottak fel először egy olyan éjjel-nappal működő hálózatot a tagállamok között, amelynek célja a hatékony transznacionális nyomozás elősegítése, s amelynek igénye – mint később látni fogjuk – a Cyber-crime Egyezményben is felmerül. A G8 által kezdeményezett felügyeleti hálózathoz 2001-re 19 ország csatlakozott, s működtetése immáron az Interpol feladata.

Az Európa Tanács 1999. január 1-ei hatállyal egy négy évre szóló akciótervet fogadott el az Internet biztonságos használatának elősegítéséről, melyet később meghosszabbított két évvel, így az 2004. december 31-ig volt hatályban. A terv az internetes tartalomszabályozás megvalósítását többek között önszabályozó és tartalom-ellenőrző mechanizmusok felállításában, illetve olyan tartalom-szűrő és -osztályozó rendszerek alkalmazásában látja, amellyel a szülők és a tanárok könnyedén alakíthatják az elérhető internetes tartalmat, honlapokat a gyermekek érdekeinek megfelelően.

Az Egyesült Nemzetek Szervezetének ez időszakban megszülető tanulmányai a 2000 áprilisában megrendezett 10. Bécsi Kongresszus[87] határozatán alapulnak. A Bécsi Egyezményként[88] emlegetett megállapodás 18-as pontja foglalkozik az informatikai bűncselekményekkel: „[A tagországok döntése értelmében] tett-központú politikai ajánlásokat fogunk kidolgozni a számítógépes bűncselekmények megelőzése és szabályozása terén, és felszólítjuk a Bűnözésmegelőzés és Bűnügyi Igazság Bizottságát, hogy e tekintetben vállalja fel a munkát, figyelembe véve a más fórumokon folytatott tevékenységeket is. Ezen kívül elkötelezzük magunkat, hogy megerősítjük képességeinket a számítógépekhez és a csúcstechnológiához kapcsolódó bűncselekmények megelőzése, nyomozása és vádemelése terén.”.

A fenti bekezdés alapján születettek egy évvel később – a Bűnözésmegelőzés és Bűnügyi Igazság Bizottságának 10. ülésszakára – a Bécsi Egyezmény 2001-2005-ig szóló Akciótervének ide vonatkozó rendelkezései *(92-101.)*, illetve az a tanulmány, amely a legújabb technikai vívmányok figyelembevételével készült a számítógépekkel és a csúcstechnológiai eszközökkel elkövethető deliktumok szabályozásáról és megelőzéséről. A dokumentum kiemeli az informatikai bűncselekmények teljesen különálló cselekménytípusként való kezelésének a fontosságát, szorgalmazza a fejlődő országok támogatását, illetve a nemzetközi, a nemzeti és a magánszektor által tett intézkedések, lépések figyelembevételét és egybevetését.

7.2. A Cyber-crime Egyezmény *(Convection on Cyber-crime)*

Az Egyezmény megszületésének folyamatában az európai igazságügy-miniszterek az addigi nemzetközi együttműködés eredményeire, ösztönző hatásaira tekintettel határozatukban felvázolták a szükséges feladatokat. 1997. június 10-11-i, XXI. Prágai Konferenciáján az európai igazságügy-miniszterek által elfogadott 1. számú határozat a Miniszteri Bizottság számára javasolta, hogy támogassa a Büntetőjogi Kérdésekkel Foglalkozó Európai Bizottság (CDPC) számítástechnikai bűnözéssel kapcsolatos tevékenységét a nemzeti büntető jogalkotás közelítése és a számítástechnikai bűncselekményekkel szembeni hatékony nyomozati eszközök felhasználása érdekében. A 2000. június 8-9-i, XXIII. Konferencián elfogadott 3. számú határozat felismerte a számítástechnikai bűnözés elleni harc sajátos követelményeit figyelembe vevő, gyors és

[87] ENSZ 10. Kongresszusa a Bűnözés Megelőzéséről és az Elkövetőkkel Kapcsolatos Bánásmódról: „Bűnözés és igazság, találkozás a 21. század kihívásaival”; 2000. április 10-17.
[88] Bécsi Egyezmény a Bűnözésről és az Igazságról: Találkozás a 21. század kihívásaival; 2000. április 15. Közgyűlés által jóváhagyva: 2000. december 4.

hatékony nemzetközi együttműködés eszközei megteremtésének szükségességét. Az Egyezmény kidolgozásakor szintén figyelembe vették az új információs technológiák fejlődésével kapcsolatban az Európa Tanács értékein és normáin alapuló közös megoldások kidolgozására vonatkozó, az Európa Tanács állam- és kormányfőinek az 1997. október 10-11. között Strasbourgban megtartott Második Találkozóján elfogadott akcióprogramot.

A Büntetőjogi Kérdésekkel Foglalkozó Európai Bizottság (CDPC) keretében létrehozott Számítógépes Bűnözéssel Foglalkozó Szakértői Bizottság (PC-CY) által kidolgozott Egyezmény végleges tervezetét több tanulmány is megelőzte, ezek közül az egyik az ún. Sieber-féle jelentés. Ulrich Sieber német professzor három fő követelményt támaszt a jogi szabályozással szemben egy 1998-as, az Európai Bizottság számára készített tanulmányában.[89] Az egyik a *nemzetköziség*, hiszen az információ szabad áramlásának nemzeti szabályozása és megszorítása kudarcra lenne ítélve azáltal, hogy a nemzetközi számítógépes hálózatokon átfutó adatok mennyisége tartalmi ellenőrzésüket egyrészt lehetetlenné, másrészt társadalmilag nemkívánatossá teszik. A másik az *átfogó megoldások* kidolgozása: a felmerülő problémák nem jogi eszközökkel történő orvoslása – mint a technológia, az oktatás és a gazdaság önszabályozása – gyakran sokkal hatásosabbak lehetnek, mint a büntetőjogi rendelkezések szigorítása, amely – főleg az eljárásjog területén – alkalmas lehet a polgári szabadságjogok megsértésére. Sieber kiemeli továbbá, hogy minden megoldásnak *specifikusnak* kell lennie, tekintettel a materiális és szellemi javak közötti különbségre. Ez különösen fontos a jogi beavatkozásoknál: az információ egy olyan új, jól elhatárolható érték, melynek védelme megvalósíthatatlan a fizikai tárgyak védelmének analógiájára. Sieber összességében négy fő területen látja és ajánlja az Európai Unió számára a számítógépes bűncselekmények elleni harc megvalósíthatóságát, ezek a technológia, az oktatás, a gazdaság és a jog.

Ilyen előzmények után az Európa Tanács 2001-ben fogadta el a Számítástechnikai Bűnözésről Szóló Egyezményét (*Convection on Cyber-crime*, a továbbiakban: Cyber-crime Egyezmény).[90] A Budapesti Egyezmény néven is ismert megállapodást 2001. november 23-án írta alá Budapesten mintegy harminc ország. Az Egyezmény több lényeges szempontból meghaladja az elődjeit, mivel definíciókat ad a számítástechnikai rendszer elemeire vonatkozóan, az anyagi jogi, eljárásjogi és a nemzetközi jogi összefüggéseket együtt tárgyalja, így magába építi az anyagi jogi kérdésekkel foglalkozó (89) 9. ET ajánlást, és az eljárásjogi kérdéseket tárgyaló (95) 13. ET ajánlást. További előremutató újdonsága az Egyezménynek, hogy abban a számítástechnikai rendszer és adatok elleni bűncselekmények mellett[91] megjelentek a hálózatokon elkövethető „tartalom-bűncselekmények" is, úgymint a gyermekpornográfia és a szerzői jogi bűncselekmények, és mindezek mellett igyekezett választ adni az olyan elterjedten jelentkező problémákra is, mint az illegális fájlcserélő rendszerek alkalmazása, a kéretlen kereskedelmi levelek küldözgetése, vagy az adathalászat.[92] Az Egyezmény egyik célja volt a bűnügyi együttműködés eredményességéhez elengedhetetlenül szükséges közös jogi alap megteremtése, hiszen az 1959-es strasbourgi, kölcsönös bűnügyi jogsegélyről szóló

[89] SIEBER, U., *Legal Aspects of Computer-Related Crime in the Information Society*, 1998. (A számítógépes bűncselekmények jogi aspektusai az információs társadalomban) Forrás: http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf [2012-04-15]

[90] Magyarország az Egyezményt a 2004. LXXIX. törvénnyel hirdette ki, hatályos 2004. július hó 1. napjától.

[91] Ezek: jogtalan belépés, jogtalan kifürkészés, adatok és rendszer elleni cselekmény, visszaélés eszközzel, számítástechnikai csalás és hamisítás.

[92] NAGY, Z., A számítógépes környezetben elkövetett bűncselekmények kriminológiai aspektusairól. In. Gál, I. & Nagy, Z. (ed.) *Informatika és büntetőjog*, Pécs, 2006. pp. 150-151.

egyezmény szerint a jogsegély kérésének és nyújtásának az a feltétele, hogy az adott cselekmény az érintett országokban büntethető legyen. Az Egyezmény úgy próbál közös büntetőjogi politikát kialakítani az aláíró országokban, hogy közben a büntetőjogi kényszerintézkedésekhez fűződő érdek és az alapvető emberi jogok védelme közötti megfelelő egyensúly fennmaradjon.

7.3. Az Európai Unió számítógépes bűnözésre vonatkozó jogforrásai

Az EU működését jelentősen átszabó Lisszaboni Szerződés előtt az Európai Unió jogalkotása szempontjából a Maastrichti Szerződés által létrehozott és az Amszterdami Szerződés által módosított harmadik pillérébe tartozott a tagállamok közötti bűnügyi együttműködés irányítása. Az Európai Unió Bizottsága több közleményben és megrendelt tanulmányban hangsúlyozta és hangsúlyozza a szupranacionális fellépés szükségességét, kiemelve azt a körülményt, amely szerint az információs rendszerek elleni támadás komolyan veszélyezteti a biztonságosabb információs társadalom, valamint a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség megvalósítását, ezért az Európai Unió szintjén kell fellépni ellene.[93]

A *2005/222/IB számú kerethatározat*.[94] A Tanács a fentiekre figyelemmel rövid időn belül, 2005. február 24. napján megalkotta a még jelenleg is hatályos 2005/222/IB számú kerethatározatot, amely ha nem is szó szerint, de lényegét tekintve közel azonos megfogalmazással átvette a Cyber-crime Egyezmény számítástechnikai bűncselekményekre vonatkozó tényállásait. Mivel a kerethatározat uniós jogforrás, ezért kötelező az unió valamennyi tagállamára nézve, ezzel máris jelentősebb lépés az informatikai bűncselekmények elleni nemzetközi együttműködésben, mint az ihletadó Cyber-crime Egyezmény. Az egyes tényállásokkal részletesebben a számítástechnikai rendszerek elleni támadásokkal foglalkozó fejezet foglalkozik.

További kerethatározatok és irányelvek. Természetesen nem kizárólag az említett uniós kerethatározat érinti a számítástechnikai vonatkozású bűncselekményeket, hanem egy-egy gazdasági, szűkebben pénzforgalmi biztonság vagy a hálózatokon hozzáférhetővé tett tartalmak érdekeltjei által megkövetelt uniós fellépés is életre hívott ilyen jellegű dokumentumokat, amelyek közül egyesek egy-egy bűncselekménytípusra koncentrálnak, míg a többi az EU ismertetett információs politikájának szellemében a célzott szakterület biztonságát erősíti. Ilyen jogforrások például:

- a 2001/413/IB. számú kerethatározat a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről;

- a 2004/68/IB. számú kerethatározat a gyermekek szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről;

[93] Példának említhető a Bizottság Európai Parlamentnek, Tanácsnak és a Régiók Bizottságának intézett 2001-ben megjelent COM(2000)890. számú közleménye. Az egyik legújabb ilyen dokumentum a COM(2007)267-es, a számítógépes bűnözés elleni közdelemre vonatkozó általános politika felé című közleményben foglalt megállapítások többségét is egy 2006-ban elrendelt tanulmányból vették át (szerződésszáma: JLS/2006/A1/003.)

[94] Az Európai Tanács 2005/222/IB kerethatározata (2005. február 24.) az információs rendszerek elleni támadásokról, OJ. L. 069, 16/03/2005 p. 0067-0071. Elérhető: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:HU:HTML [2012-04-15]

- a 2002/58/EK elektronikus hírközlési adatvédelmi irányelv arra kötelezi a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtóit, hogy biztosítsák szolgáltatásaik biztonságát. Az irányelv rendelkezéseket tartalmaz a kéretlen levelek és a kémprogramok ellen is.

Az információs stratégiák szellemében az internethasználat biztonságosabbá tétele érdekében a hálózat- és információbiztonsági politikát azóta számos fellépéssel fejlesztették tovább, például:

- a biztonságos információs társadalomra irányuló stratégiáról szóló közleménnyel (COM(2006) 251.) – amely megújított stratégiát dolgoz ki és keretet nyújt a hálózat- és információbiztonsággal kapcsolatos koherens megközelítés folytatására és finomítására –, valamint

- a kéretlen levelek, a kémprogramok és a rosszindulatú szoftverek elleni küzdelemről szóló közleménnyel (COM(2006) 688) és

- a 460/2004/EK rendelet az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról (ENISA).

A 2005/222/IB tanácsi kerethatározat továbbfejlesztése. Az EU Igazságügyi Tanácsa a 2011. április 12. napján tartott ülésén a kiberbűnözés elleni új irányelv-tervezet vitáját folytatta le. Az „Európai Parlament és Tanács irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat hatályon kívül helyezéséről” című javaslat célja, hogy korszerűsítse a korábbi, 2005-ös kerethatározatot többek között a „botnet”-alapú elkövetések büntethetőségének megalapozásával, és az úgynevezett személyazonosság lopás *(identity theft)* bűncselekménnyé nyilvánításával. A javaslat az információs rendszerek elleni támadásokról szóló, 2005. február 24-i 2005/222/IB tanácsi kerethatározat felváltására irányul, amely kerethatározat célkitűzése a preambulum szerint a tagállamok igazságügyi és egyéb hatóságai – beleértve a rendőrséget és egyéb bűnüldöző szakszolgálatokat – közötti együttműködés javítása a tagállamok büntetőjogszabályainak az információs rendszerek elleni támadások területén történő további közelítése révén. Ezen új irányelv tervezete meghatározza a bűncselekményi tényállásokat az informatikai rendszerek elleni támadások területén, létrehozza az ilyen bűncselekményekre vonatkozó büntetési tételekhez kapcsolódó szabályozási minimumokat. További célja, hogy külön rendelkezéseket vezessen be ezen a területen az említett támadások megelőzése, az európai büntetőjogi együttműködés javítása érdekében.

A nemzetközi bűnügyi együttműködés fejlesztése. A nemzetközi bűnügyi együttműködés kiépítése érdekében számos nemzetközi egyezmény született és megannyi nemzetközi szervezet jött már eddig is létre, sokuk egy-egy bűncselekmény-csoport hatékonyabb üldözésére. Ilyen általános, a részes tagállamok bűnügyi hatóságai között egyfajta koordinációs tevékenységet folytató, jogsegélyeket és információcserét bonyolító, együttműködést segítő szervezetnek tekinthető például az Interpol, az Europol, az Eurojust. Ezen szervezetek mindegyike a határon átnyúló valamennyi bűnözési forma visszaszorítása jött létre, így ebben a tekintetben, többek között a számítógépes bűnözést érintő együttműködésre is kiterjed tevékenységük, azonban kifejezetten a számítógépes bűnözésre vonatkozó specialitással nem rendelkeznek, így velük a továbbiakban szükségtelen foglalkozni.

Európai szinten – a shengeni együttműködés részletes szabályainak ismertetését mellőzve – a bűnügyi együttműködés egyszerűsítésére a Tanács *2006/960/IB kerethatározata* is tett már lépéseket a pontos és naprakész információkhoz, köztük a bűnüldözési operatív információkhoz való gyors hozzáférés biztosítására törekedve. Az említett kerethatározat 1. Cikk (4) bekezdése azonban még mindig határozottan védi a tagállamok szuverenitását, amikor a következőképpen rendelkezik. A kerethatározat a tagállamokat semmiféle módon nem kötelezi arra, hogy az igazságügyi hatóságok előtt bizonyítékként felhasználható információt és bűnüldözési operatív információt szolgáltassanak, és nem jogosít fel az ilyen információ vagy bűnüldözési operatív információ e célra történő felhasználására. Amennyiben valamely tagállam az e kerethatározatnak megfelelően beszerzett információt vagy bűnüldözési operatív információt bíróság előtt bizonyítékként fel kívánja használni, be kell szereznie az információt vagy bűnüldözési operatív információt szolgáltató tagállam beleegyezését, szükség esetén az információt vagy bűnüldözési operatív információt szolgáltató tagállam nemzeti joga szerint, a tagállamok között hatályban lévő, az igazságügyi együttműködésre vonatkozó eszközök alkalmazása útján. E beleegyezés beszerzése nem szükséges, amennyiben a megkeresett tagállam az információ vagy bűnüldözési operatív információ átadásakor beleegyezését adta annak bizonyítékként történő felhasználásához.

Az EU bel-és igazságügyi politikájának a 2011-2015. közötti időszakára vonatkozó programja *(Stockholmi Program)*[95] előirányozza az európai bizonyítékgyűjtési rendszer kidolgozását, tehát e területen jelentős javulásra lehet számítani. A program számítástechnikai bűnözéssel foglalkozó 4.4.4. pontjának tervei szerint a tagállamoknak mielőbb meg kell erősíteniük az Európa Tanács számítástechnikai bűnözésről szóló, 2001. évi egyezményét. Ez az egyezmény szolgálhatna globális szinten a számítástechnikai bűnözés elleni küzdelem jogi referenciakeretéül, míg az Europol pedig az európai forrásközpont szerepét tölthetné be azáltal, hogy az észlelt bűncselekmények jelzésére szolgáló európai fórumot hoz létre, amely segíti a tagállamok nemzeti figyelmeztető platformjait a legjobb gyakorlatok cseréjében.

A Tanács 2007. február 12-i *2007/126/IB határozata* az „Alapvető jogok és jogérvényesülés" általános program keretében létrehozta a 2007-2013-as időszakra a büntetőjogi jogérvényesülés egyedi programját. A határozat 3. cikkében meghatározott konkrét célkitűzések között szerepel a bűnügyi nyilvántartásokból származó információk cseréjének javítása számítógépes rendszerek használata révén.

A Tanács 2009. április 6-i *2009/316/IB határozata* pedig döntött az Európai Bűnügyi Nyilvántartási Információs Rendszer (ECRIS) létrehozásáról.

Az Unió tehát mind anyagi jogi, mind a bűnügyi együttműködésre vonatkozó eljárásjogi kérdésekben törekszik a számítógéppel érintett bűncselekmények visszaszorítására irányuló tagállami jogalkotást egy mederbe terelni. Az egyes konkrét előírások ismertetésére azonban már nem ebben a fejezetben, hanem az értekezés különös részében kerül majd sor.

[95] Európai Tanács: A Stockholmi Program – A polgárokat szolgáló és védő, nyitott és biztonságos Európa EU HL (2010/C 115/01).

8. AZ INFORMÁCIÓS TÁRSADALOM EMBERKÉPE

Az infokommunikációs forradalom változásokat generál az élet szinte valamennyi területén, így az emberek magánéletében is. Melyek ezek a változások, mi jellemzi az új élethelyzeteket?

Balogh Gábor szerint[96] az információs társadalom többek között olyan hálózati jellegű társadalomként jellemezhető, amelyben az egyént különböző szinteken és erővel integráló csoportok közötti erőeltolódás figyelhető meg, és amely biztosítja az infokommunikációs korszak polgárának, a *„homo informaticus”*-ként jelölt embereinek identitását. Balogh Gábor megközelítésében a hálózat egyrészt olyan technikai-technológiai eszköz, amely csomópontokból és az azokat összekötő utakból, kapcsolatokból áll, másrészt topologikus alakzat, amely integrációba foglalja a rajta tevékenykedőket. A hálózat alapvető jellemzője a kapcsolat, topologikus alakzatként pedig az infokommunikáció biztosítása, fenntartása és lebonyolítása.

A hálózati lét „helyszíneként” legtöbbször azonosított internet *Ropolyi László* szerint[97] nem csupán a számítógépek hálózatba kapcsolt rendszere és nem kizárólag médium, hanem sajátosan formálható közeg, a legtágabb értelemben vett kultúra, amelyben a legkülönfélébb emberi törekvések, szándékok, értékek, tervek és termékek formát ölthetnek. Ropolyi értelmezésében az internet olyan univerzális médium is, a mindenség egyik különálló szférája, ahol az ember a számára korábban hozzáférhető természeti és társadalmi közeg után új világra lelhet, ahol új lehetőségeket próbálhat ki, illetve ahol saját természetének, megszokott értékeinek és tevékenységének új aspektusait valósíthatja meg. Az internet létezésének egyik célja a késő modern ember kiszabadítása az univerzális elvont értékekre épített modern világból, valamint egy új posztmodern értékekre alapozott, szabadnak hitt, virtuális és nyitott emberi létszféra kialakítása és fenntartása. Az internet e felfogásban a különválasztott emberek között mesterségesen kialakított közösség, amely céljait tekintve szabad, valamiért valóban szabad, és amelyben az individuumok identitása értékvilága nyitott, virtuálisan bárkivé válhatnak, számukra bármi értékké válhat. Az internet tehát a társadalmi viszonyokat átértékelő, az emberi lényeget a társadalmi szférából a hálólét viszonyai közé transzformálni kívánó hálópolgár rendelkezésére álló eszköz.

Milyen hatással van tehát a hálózat a polgárára? Az infokommunikációs eszközök által meghatározott környezetben azonosíthatóságunk elvesztésének lehetősége miatt a hálózati lét eredményeképpen megváltozik a tudat és az identitás szerepe, függetlenítheti őket interakcióink közvetítettsége, mediatizálódása. Az interneten teremthető kapcsolatok az emberi kiteljesedés, az önmegvalósítás vagy éppen az addigi személyiségtől való elszakadás eddigi legteljesebb lehetőségeit biztosítja, sokszor többet, mint a fizikai világ, hiszen a kommunikáció formái olyan mértékben alakíthatók, befolyásolhatók, hogy az egyén a valóságtól teljesen elszakadva személyesítheti meg magát akár többféleképpen is.[98]

---

[96] BALOGH, G., Az információs társadalom olvasatai. In: Balogh, G. (ed.), *Az információs társadalom dimenziói*, Gondolat-INFONIA, Budapest 2006. pp. 11-22.

[97] ROPOLYI L., Internethasználat és hálólét-konstrukció, *Információs társadalom: társadalomtudományi folyóirat*, 2006. (6. évf.) 4. sz. pp. 39-46.

[98] JEWKINS, Y. & SHARP, K., Crime, deviance and the disembodied self: transcending the dangers of corporeality. In. JEWKINS, Y. (ed.), *Dot.cons-Crime, deviance and identity on the Internet*, Willan Publishing 2003. Portland, Oregon USA. pp. 2-3.

De nem csupán a kísérletezés lehetősége, hanem az előző bekezdéssel ellentétben olyan alapvető emberi tulajdonságok is szerepet játszanak a felhasználók online viselkedésében, mint az őszinte kitárulkozás vágya, a valós személyiség megélése, az az igény, hogy az egyén a mindennapi élet feszültségeit valaki olyannal ossza meg, aki megérti, aki hasonló problémákkal küszködik anélkül, hogy mindez bármiféle komoly, negatív következményekkel járna.[99] A technológia közvetítette kommunikációkban a felhasználó sok esetben érzi magát biztonságban, hiszen a másik féltől fizikailag is távol van, ekként a nem kívánt interakciókat egyszerűbben kizárhatja, megszüntetheti anélkül, hogy figyelemmel volna a szemtől-szemben folytatott beszélgetések társadalmi konvencióira.[100] Általános felismerés az is, hogy sokszor könnyebben beszéljük el problémáinkat idegeneknek, mint közeli hozzátartozóinknak. Ez, a pszichológusok által „idegennel a vonaton" -nak *(stranger on the train)* nevezett magatartás is jelentős mértékben befolyásolhatja az egyén online életét. A kitárulkozás nem csak belülről fakadhat, lehet elvárás is egy csoporthoz tartozás legitimálásához, vagy a kölcsönös bizalom kialakításához, de legyen szó bármelyik esetről is, könnyebben vállalható az egyébként stigmatizált tulajdonság bevallása anonim módon. [101]

Miben rejlik ennek a veszélye? Az infokommunikációs eszközökkel jellemzett környezetben a fenti új lehetőségek miatt egyrészt megváltozik a résztvevők magánszférára vonatkozó felfogása, a felhasználók könnyebben megnyitják magánszférájukat és mások magánéleti történéseinek megismerésére is nagyobb igénnyel lépnek fel. Másrészt az infokommunikációs eszközök olyan nem monopolizált tömegtermékek, amikhez bármely polgár hozzáférhet, a felgyorsult társadalmi interakciók olyan létszükségletei, amelyek egyre inkább létfeltételei a modern embernek. Konfliktus akkor keletkezik, amikor a személy az infokommunikációs környezetből kilépve a valós, közvetlen világ eseményeit, helyzeteit képtelen azonosítani.

Bár a továbbiakban is kiemelt szerephez jut majd a XXI. század új kultikus helye, a kibertér, természetesen a problémakör nem szűkíthető le kizárólag erre a szektorra, viszont szembetűnő módon mutat olyan anómiás jegyeket, amelyekkel jellemezhetjük társadalmunk negatív változásait. Arra a kérdésre tehát, hogy miben rejlik a mediatizált kommunikáció csábításának veszélye, és miért kell annak a személyiségre gyakorolt torzító hatásairól beszélnünk, a válasz egyszerűnek tűnik: a kibertérben folyó interakciók hatásai továbbgyűrűznek a társadalom „valós, közvetlen" életterében is. A felhasználók mind jelentősebb része képtelen egymástól elhatárolni a két területen folyó interakcióit, szerepjátékait, személyiségének egyszer rejtett, majd titkon kiélt devianciáit.

M. Poster és *S. P. Wilbur* szerint a kibertér kedvez az egyén „labilis énné" válásának, kedvez olyan egyéniséggé alakulásának, aki rabjává válik annak a folyamatnak, amelyben sokféle személyiséget alakíthat ki magának.[102] Meghatározó az élmény, amely lehetővé teszi az embereknek, hogy kimozduljanak tér- és időbeli helyükről, hogy személyiségük olyan oldalaival kísérletezzenek, amelyeket eltitkolnak a valós földrajzi térben. Az

[99] MCKENNA, K. Y. A., Through The Internet looking glass – Expressing and validating the true self. In. Joinson, A., McKenna, K., Postmes, T. & Reips, U-D. (ed.), *The Oxford Handbook of Internet Psychology,* Oxford University Press, 2007. pp. 205-221.

[100] GREEN, Melanie C.: Trust and social interaction on the Internet. In. Joinson, A., McKenna, K., Postmes, T. & Reips, U-D. (ed.), *The Oxford Handbook of Internet Psychology,* Oxford University Press, 2007. p. 43.

[101] WHITTY, M. T. & JOINSON, A. N., *Truth, Lies and Trust on the Internet,* Routledge, 2009. 27 Madison Avenue, New York USA. pp. 9-11.

[102] MÉSZÁROS, R., A kibertér társadalomföldrajzi megközelítése. In: Balogh, G. (ed.), *Az információs társadalom dimenziói*, Gondolat-INFONIA, Budapest 2006. (a továbbiakban Mészáros, 2006.) p. 216.

anonimitás és a képzelet szabad megvalósíthatóságának ajánlatával a kibertér lehetővé teszi a társadalmilag elvárt célok, a siker látszólagos megvalósítását is.

Ami a társadalmi kapcsolatokra gyakorolt hatását illeti, *Mészáros Rezső* szerint jellemzője, hogy a földrajzi határokat eltüntetve a felhasználók közös érdeklődési körére épül, tehát ezzel gyengíti a földrajzi közösségeket, a fanatikus felhasználók visszaszorulnak a kibertérbe, kilépnek a „való világbeli" társadalomból.[103] A kibertér kulturális hatásai jelentősek, a jelenlegi világtrendnek megfelelően félő, hogy az amerikanizálódó világ és a globalizáció erősödését könnyíti, alternatív teret kínál, amelyben az „én" határozatlan körvonalú és testetlen.[104]

Az információs társadalom emberképének vizsgálatához további adalékul szolgál az egyének magánszférához való viszonyulásának változása is. *Szabó Máté* az információs társadalom változásainak a magánszférára vonatkozó hatásait, problémáit a következőképpen magyarázza.[105] Az információs társadalomra jellemző, hogy a magánszféra egyre nyitottabbá válik. Az online életben az egyént egyre inkább jellemzői, a róla elmondott és elmondható információk határozzák meg, nem pedig fordítva. Az egyén egyre több olyan kapcsolatot tart fenn, amelyekben a másik oldalon nem jelenik meg fizikai lény, egy ember a maga testi valójában, hanem ott csupán az információknak valamilyen halmaza található, azaz az egyén a külvilág számára virtualizálódik. A konfliktus ott kezdődik, hogy az egyén csak a külvilág számára válik virtuálissá, önmaga fizikailag továbbra is létező ember marad. A külvilág azonban nehezen fogadja el, hogy a számára virtuális lénynek is van igénye a magánszférára. A jogi védelem a magánéletnek mindig más és más aspektusát kiemelve jelent meg a magyar jogrendszerben is, és éppen az aktuális társadalmi igényeknek megfelelően változott, ezért az online magánszféra problémájának megértéséhez a fogalom gyökereihez kell nyúlni. Szabó Máté a magánszféra fogalmának megértéséhez a következők szempontokat tekinti meghatározónak. A privacy védelmével kapcsolatos gondolkodás hagyományosan az ember mint társadalomalkotó lény kétféle életszférája közötti különbségtételből: a magánélet és az azon kívül álló világ elválasztásából indul ki.

A privacy a magyar jogirodalomban az önrendelkezés szabadságához kapcsolódik, tehát az egyén joga ahhoz, hogy magáról döntsön, arról, hogy mi lesz a maga sorsa, mit tesz magával, a testével és a rá vonatkozó ismertekkel. Másként fogalmazva az önrendelkezési jog részben az egyén arra vonatkozó döntési jogát jelenti, hogy hol húzza meg a határt önmaga és a külvilág között, azaz meddig engedi be a külvilágot a személyes szférájába. Az online közösségi portálok, a személyes blogok használatára vonatkoztatva egyértelmű, hogy a felhasználó az önmagáról közzétett információkkal jeleníti meg, határozza meg önmagát a külvilág számára (pl.: fényképek, videók, szabadidőszokások), azonban a megadott információkkal egyben ki is jelöli a magánszféra határait, ha nem is objektíven, de félreértésre okot adóan.

Amennyiben tehát a felhasználó önmagáról intim információkat oszt meg, az egyben azt is jelenti, hogy a külvilág számára az intim szféra hasonló tekintetben, azonos mértékig hozzáférhető, azaz nem az intim kapcsolat létesítésére jogosít, hanem például a megnyitott információk véleményezésére, értékelésére, következtetések levonására és azok alapján

[103] Természetesen ezzel szemben is hozhatók fel érvek, az értekezés azonban – célja okán – csupán a negatív hatások lehetőségeinek ismertetésére szorítkozik.
[104] MÉSZÁROS, 2006. pp. 218-219.
[105] SZABÓ, M. D., Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival. *Információs Társadalom: társadalomtudományi folyóirat* 2005. (5. évf.) 2. sz. pp. 44–54.

további cselekmények megtételére. A jogilag – büntetőjogilag – nehezen értékelhető helyzet ezen további cselekmények megítélésében áll. A magánszféra határait illetően megtévesztésre okot adó információk közzététele és azoknak a másik oldalon tévedéssel történő értékelése viszont nehezen róható fel az annak alapján cselekvő jogsértőnek. Egy másik oldalról megközelítve a kérdést a magánszférát illetően úgy is fogalmazhatunk, hogy az egyénnek egyfelől ahhoz van joga, hogy önmagát a külvilágtól megkülönböztesse, másfelől joga van ahhoz, hogy a külvilágot saját magától elhatárolja. Amennyiben az egyén ezen utóbbi jogával láthatóan nem él (vagy félreérthetően él), úgy mindennek a magánszférába belépő másik felhasználónak való felrovása is aggályos lehet bizonyos tekintetben. Mindezen helyzetek helyes megítélésére természetesen kizárólag konkrét esetek vizsgálata esetén kerülhet sor. A magánszféra megítélésének változására vonatkozóan az információs társadalom devianciáival foglalkozó fejezet szolgál további információkkal.

9. A FEJEZET MEGÁLLAPÍTÁSAI

9.1. Az információs társadalommal kapcsolatban

Az információs társadalom egyik meghatározó jellemzője, hogy az információ előállítása, terjesztése, elosztása és felhasználása alapvető gazdasági, politikai és kulturális tevékenységként jelenik meg. A közgazdaságtanban ezzel a megközelítéssel összhangban áll a tudásgazdaság fogalma, melynek lényege, hogy az értelem, mint az emberi erőforrás gazdasági hasznosításán keresztül nemcsak szellemi, de anyagi értelemben is kifejezhető érték jön létre. Az információs társadalom lényegi elemei így a következőképpen is összegezhetők: az információ mint vagyoni érték elsődleges szerephez jut a gazdaságban, az elektronikus kereskedelemben, amely immár virtuális aktusokra is épül, szemben a hagyományos gazdaság működési mechanizmusaival, továbbá az információ alapvető része a politikai hatalomgyakorlásnak is, hiszen utóbbit megszerezni és birtokolni csak az képes, aki az információt előállítja és elosztja.[106]

Az információs társadalom lényegi alapeleme a technológia, amely az információ hatékony megszerzését és feldolgozását lehetővé teszi. A technológia fejlődése jelentősen növelte a társadalom reakciójának gyorsaságát az új életviszonyokkal szemben, mivel az információk mind nagyobb arányú áramlása fokozatosan csökkentette a naprakész tudás elsajátításának tartamát, míg ezzel párhuzamosan a folyamatos tanulás alapvető követelménnyé vált. Mindezen folyamatoknak egy másik gazdasági vetülete, hogy a termelő tevékenységet végző foglalkoztatottak egyre nagyobb része az információ megszerzésével és feldolgozásával összefüggő munkakörben dolgozik.[107]

Pintér Róbert összegzése[108] alapján az információs társadalom tehát az emberi együttélés olyan új módja, amelyben az információ szervezett előállítása, tárolása, előhívása és felhasználása játssza a fő szerepet, és új strukturális elemek, hálózatok segítségével kialakul egyfajta „hálózati társadalom" a maga új intézményeivel együtt, amelyek nagyobbrészt a már ismert társadalmi intézmények átalakult formái. Ebben a rendszerben formálódik újjá makroszinten a politika, a gazdaság és a kultúra, míg mikroszinten a családok és az egyéni identitások.

9.2. A büntetőjogi szempontokkal kapcsolatban

A büntetőjog jogrendszerben betöltött, végső soron igénybevett szerepéből kiindulva önálló információs társadalom-képpel nem rendelkezhet, lévén hogy feladata a fennálló társadalmi rend, értékek védelme akkor, amikor a többi jogág védelme már nem elegendő, vagy a jogtalan cselekedettel okozott sérelem oly mértékű, hogy a legszigorúbb, alkotmányos alapjogokat is komolyabban korlátozó beavatkozásra van szükség. Máshogy fogalmazva a büntetőjog számára a társadalom, legyen az posztindusztriális, információs vagy tudásalapú, jobbára mindig statikusnak tekinthető, eszközként közvetlenül nem, csak közvetve fejleszti a társadalmi viszonyokat, nem előmozdítja, hanem védi a társadalmi-gazdasági rendet és fejlődést. Azonban nem vonhatja ki magát a társadalmi változások alól olyan tekintetben, hogy az általa használt, dogmatikailag letisztult jogintézmények alkalmazásának környezete átalakult, új társadalmi értékek, viszonyok, jogtárgyak jelentek meg, a bűncselekményeket új eszközökkel lehet elkövetni, vagy éppen felderíteni. Anélkül,

[106] SUM, Sz., A szellemi alkotások jogának információtechnológiai vonatkozásairól. In: Takács, T., (ed.) *Az informatikai jog nagy kézikönyve,* Complex Kiadó Budapest, 2009. pp. 212-213.
[107] SUM, 2009. p. 212.
[108] PINTÉR, 2007b. p. 13.

hogy az információs társadalmat kizárólag az új technológiai eszközök által meghatározottnak tekinteném, a bűnözés és bűnüldözés szempontjából az információs társadalom technológiai megközelítése volt indokolt a következő fenntartással. A büntetőjogi felelősség alapja a bűnösség fogalmi elemeiben megjelenő szabad akarat. Ekként a technológiai elem megítélése során el kell fogadnunk annak semleges voltát, azaz az infokommunikációs technológia eszközei nyújtotta lehetőségek nem feltételezik azok szükségszerűen bűncselekményekre történő hasznosítását, de funkcióik, az általuk biztosított lehetőségek ösztönzői lehetnek egyes devianciák kialakulásának, és létük egyes bűncselekmények dogmatikájának újraértelmezését teszik szükségessé.

Milyen büntetőjogi vonatkozásai vannak a technológiai fejlődésnek? A közműszerű információtechnológiai szolgáltatás terjedése, a cloud computing például felveti a személyes és más információk tárolásának és használatának az egyes nemzeti törvényekben megmutatkozó különböző szabályozását. A virtualizáció olyan ma még magától értetődő fogalmak jelentésének alkalmazhatatlanságát vetíti előre, mint az adatok helye, célja, vagy a szerverek üzemeltetője. Átértékelődnek a stratégiai fontosságú infrastruktúrák védelmének szempontjai, így például a különböző érzékenységű adatokra vonatkozó jogszabályi előírások alapján bizonyos információkat nem lehet a felhasználó anyaországán kívüli adatközpontokban tárolni, másrészt a cloud computing működésének elve alapján az adatok konkrét helye szintén nehezen határozható meg. Probléma például a szerverek „megfoghatatlansága", hiszen amint képesek leszünk egy számítógépes feldolgozás során a teljes állapotot egyik helyről a másikra áthelyezni a feldolgozás igényei szerint, anélkül hogy közben bármit is elvesztenénk, lehetségessé válik a jogi keretek kijátszása, például tiltott szerencsejáték szervezése esetén a regisztrációs folyamatot az USA-ban, a banki műveleteket Svájcban, míg a szerencsejáték algoritmusait a Bahamákon futtatni.[109]

A fejezet elején meghatározott vizsgálati szempontok alapján a következők állapíthatók meg. Az információs társadalom számítástechnikai vonatkozású deliktumainak szabályozási környezetét – jelentősebb mértékben anyagi jogi, kisebb részben eljárásjogi tekintetben – az információs stratégiák részeként alapvetően meghatározza az európai uniós joganyag, valamint a nemzetközi viszonylatban etalonnak számító Cyber-crime Egyezmény. A magyar büntetőjogi tényállások elemzése során éppen ezért nem vonatkoztathatunk el az Alaptörvény mellett az említett jogforrásoknak való megfeleléstől.

Az egyének élethelyzetének változásait tekintve megállapítható, hogy a természeti és társadalmi létszféra mellett az egyre több társadalmi viszony informatizálása révén kiépül egyfajta „hálólét szféra"-ként értelmezhető életviszony is, azaz az ember a hálóvilág polgára is egyben, pontosabban az emberi élet centruma mind jobban elmozdul a hálólét felé. Az egyes szférákhoz való hozzáférés szabadsága a létszférák egymáshoz való viszonya még beláthatatlan módon alakul, ebből fakadóan a jogi szabályozás számára az átalakulás számos, még nyitott kérdést teremt. Az információs társadalom új, jogilag értékelhető és védendő társadalmi viszonyokat termelt ki, valamint a már létező társadalmi érdekeket is tovább differenciálta. A materiális jogellenesség vizsgálatakor, a majd elemzett bűncselekmények társadalomra veszélyességének megítélése során nem hagyható figyelmen kívül a korábbi fejezetekben részletezett technológiai környezet és annak az egyének szokásaira gyakorolt hatása.

[109] DÖMÖLKI et al. 2008. p. 380.

II. FEJEZET: AZ INFORMÁCIÓS TÁRSADALOM DEVIANCIÁI

1. A DEVIANCIA FOGALMA ÉS ALAPJA

Az információs társadalom narratíváinak bemutatását követően e fejezetben az információs társadalom új devianciáinak, azok okainak, egyes konkrét megnyilvánulási formáinak érintőleges elemzésére kerül sor.

A „deviancia" kifejezés valamely normák által szabályozott közösség együttélésének alapvető szabályait sértő magatartást jelöl. E meghatározásból érződik egyfajta szubjektivitás, azaz az elítélt magatartás közösségenként és korszakonként változhat. A deviancia jelentésrétegei leginkább egy tölcsérhez hasonlíthatók: legtágabb értelemben olyan érzés, hogy valami talán rossz, furcsa, különös, míg legszűkebb értelemben ítélet, hogy valami a legteljesebb mértékben rossz, valahol e két szélsőség között válik a deviáns viselkedés bűncselekményt megvalósító magatartássá.[110]

Az információs társadalom új, eddig nem ismert devianciáinak egyik lehetséges oka az új életviszonyok okozta „anómia". Az anómia a szó szoros értelmében normahiányos állapotot jelent, tágabban olyan állapot, amikor bizonyos (általában új, ismeretlen) élethelyzetekre nincs régi, eligazító norma, vagy egy kialakult társadalmi gyakorlat eltér a társadalom által vallott normáktól.[111] Megint másként fogalmazva az anómia a társadalmi rend felbomlása az értékek és a normák elvesztése következtében.[112] *Durkheim* az anómia fogalmát az öngyilkosságok számának korszakonkénti változásával illusztrálta, és okát kutatásai során több jelenségre vezette vissza: az öngyilkossági ráta többek között a nagyobb szabású és gyors gazdasági változások idején nőtt jelentősen, azon oknál fogva, hogy az emberek a megszokott életviszonyokból hirtelen új, ismeretlen helyzetbe kerültek, amelynek törvényeihez hirtelen alkalmazkodniuk kellett.[113] Durkheim a XIX. század ipari forradalmát elemezve jutott arra a következtetésre, hogy a felszabadult társadalmi erők nem kerültek egyensúlyba, egymáshoz viszonyítva értékük nincs meghatározva, emiatt egy ideig nem működik a szabályozás. Az emberek nem tudják, hogy mit lehet és mit nem, mi igazságos és mi igazságtalan, mi az, amit jogosan követelhetnek, mi az, ami túllépi a mértéket, ennek következtében nincs semmi, amire ne tarthatnának igényt.[114]

Robert Merton szerint az anómia oka nem a társadalmi változás, hanem az olyan társadalmi szerkezet, amely minden tagja elé azonos célokat tűz, ám nem biztosít azok eléréséhez azonos eszközöket, azaz feszültség van kultúránk követelményei és társadalmi szerkezetünk között.[115] E feszültség egyik eredménye a deviancia. Az „amerikai álomként" ismert kifejezésünk jól tükrözi társadalmunknak a francia forradalom egyenlőség-eszméjének megerősödése óta elfogadott szemléletét: célunk egyenlőként, egyenlő eséllyel törekedni a sikerre, a jólétre. Az alkalmazkodás a kor céljaihoz és eszközeihez ötféleképpen történhet: konformizmus esetén mindkettő elfogadása történik, újítás esetén a célokat elfogadjuk, de saját eszközökkel érjük el, a ritualizmusnál feladjuk céljainkat, de továbbra is megengedett eszközökkel élünk, visszahúzódás esetén mindkettőt feladjuk,

[110] ADLER, F., MUELLER, G. O. W. & LAUFER, W. S., *Kriminológia,* Osiris Kiadó Budapest, 2002. pp. 34-35.
[111] GÖNCZÖL K., KEREZSI K., KORINEK L. & LÉVAY M. (ed.), *Kriminológia – Szakkriminológia* CompLex Kiadó Budapest, 2006. p. 104.
[112] ADLER et al. 2002. p. 157.
[113] DURKHEIM, É., *Az öngyilkosság,* Budapest, KJK, 1982. pp. 227-161.
[114] DURKHEIM, É., *Az öngyilkosság: szociológiai tanulmány,* Osiris kiadó, Budapest. 2000. pp. 274-275.
[115] ADLER et al. 2002. p. 159.

lázadás esetén pedig mind a célokat, mind az eszközöket tagadva, azokat saját céljainkkal és eszközeinkkel helyettesítjük, új társadalmi szerkezetet alkotva.

Természetesen a fenti szempontok a számos deviancia-elmélet közül erősen kiragadottnak tűnnek, feltehető azonban, hogy az információs társadalom fejlődése – hasonlóan a korábbi kulturális és technológiai forradalmakhoz – olyan új társadalmi viszonyokat hozott létre, amelyekben még nincsenek meg az eligazító normák. Elfogadva tehát, hogy a devianciák kialakulásában a jelentősebb társadalmi változások szerepet játszanak, és ha az információs társadalom új formája a közösségi együttélésnek, akkor következésképpen olyan új élethelyzetek is megjelennek, amelyek morális megítélését illetően a társadalom egyes rétegei között nincs egyetértés, ennek okán a korábbiaktól merőben eltérő konfliktusok és devianciák születhetnek.

2. A DEVIANCIÁK ÖSZTÖNZŐI

Mi lehet az oka annak, hogy egy ilyen fiatal technológia ily hamar képes volt magához láncolni felhasználóinak tömegét?

Katelyn McKenna szerint az infokommunikációs eszközök segítségével folytatott interakciókban négy olyan fő rizikófaktor van jelen, amelyek nagymértékben meghatározzák e környezet pszichológiai hátterét. Ezek: az anonimitás, a fizikai jelenlét szükségességének csökkenése, az interakciók ideje és menete feletti erősebb kontrol, és a hasonló gondolkodásúak könnyebb találkozása.[116]

A látszólagos anonimitás mellett egy másik rizikófaktor az enyhének tűnő közösségi szankció, mivel a deviáns viselkedésnek a virtuális térben legtöbbször csupán annyi következménye lehet, hogy a másoknak nem tetszőn viselkedőt kizárják a csoportból, ellentétben a közvetlen élethelyzetekkel, ahol sokkal súlyosabb következményei is lehetnek egy normaszegésnek.[117]

Természetesen a hasonlóan deviánsan viselkedőknek is adott a lehetőség, hogy megalkossák a maguk közösségét, melyben ezután maguk határozzák meg a követendő szabályokat, éppen ezért a deviáns magatartásokat ma még a domináns csoport értékrendszeréhez viszonyítva ítéljük meg. Akkor lenne nehezebben feloldható a probléma, ha a ma még deviánsnak tekintett felhasználók és az „átlag" felhasználók száma között egyensúly jönne létre. A hasonló gondolkodású és érdeklődési körrel rendelkező felhasználók és a belőlük felépülő közösségek sajátos szubkultúrát hoznak létre, mely megnyilvánulhat a kommunikációs eszközök használatában, az újonnan csatlakozni kívánók tesztelésében, melynek célja természetesen a közösség erősítése, az idegenek kizárása.

Egyes kutatások alapján a 16 éves és az ennél fiatalabb személyek követik el a legtöbb számítógéppel kapcsolatos deviáns magatartást.[118] A fiatalok erőteljes jelenlétét támasztja

[116] AMICHAI-HAMBURGER, Y., Personality, individual differences and Internet use. In. Joinson, A., McKenna, K., Postmes, T. & Reips, U-D. (ed.), *The Oxford Handbook of Internet Psychology*, Oxford University Press, 2007. pp. 187-188.

[117] PARTI K., Devianciák a virtuális valóságban, avagy a virtuális közösségek személyiségformáló ereje. *Infokommunikáció és jog* 2007/2. p. 61.

[118] ROGERS, M. K.: A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory Study. UMI Dissertation Services. 57-58. Ismerteti: PARTI K., Devianciák a virtuális valóságban, avagy a virtuális közösségek személyiségformáló ereje. *Infokommunikáció és jog* 2007/2. p. 62.

alá egy, a látens fiatalkori devianciákról készített önbevalláson alapuló hazai felmérés is, amelynek eredményeképpen megállapítható, hogy a film- és zenefájlok internetes letöltése az egyik legenyhébbnek tekintett deviancia: a megkérdezett fiatalok 50,9 %-a életében már töltött le ilyen tartalmakat, a letöltők 41,8 %-a kezdte tevékenységét 12 éves vagy fiatalabb korában.[119]

A kibertéri közösségek enyhe szankciói mellett a való világbeli társadalom szintén enyhe értékelése is erősíti ezeket a devianciákat. Az el nem ítélés oka részben az, hogy a kibervilág „nem valós", „nem fizikai" dolgaira még nem terjedt ki a társadalom többségi tagjaiban az az abszolút, kizáró birtokviszony-rendszer szellemisége, amely a kibervilág megjelenése előtt évezredekkel a többi „dologra" már kialakult. További oka, hogy a számítástechnikai rendszereket érő támadások túlnyomó része nem kap nyilvánosságot. A vagyoni célzatú támadások legtöbbször nem érintik az egyéni felhasználókat, „csak" azokat a nagyvállalatokat, amelyekkel szemben a társadalom többsége gyakran szimpatizál a magukat Robin Hood-ként beállító ellenállókkal. Mivel az emberek védve érzik magukat a számítógépes támadásokkal szemben, ezért a számítástechnikai jellegű bűncselekmények erkölcsileg inkább illeszkednek a mai társadalom értékrendjébe, így az elkövetőkben a morális feloldozáshoz nincs szükség túlzott erőfeszítésre.[120] A Sonda Ipsos egy korábban közzétett felmérése szerint a közvélemény például az illegális szoftverhasználatot kisebb vétségnek tekinti, mint ha valaki nem adja át helyét az idősebbeknek a buszon, az illegális cd- és dvd-másolást pedig a bliccelésnél is enyhébb kihágásnak számít.[121]

Az anonim online élet egyfajta kettős morál kialakulásához vezet, ami az offline társadalmi normák lazább értelmezését jelenti, azaz a felhasználók nagy része hagyományosan normakövető marad, de az internetes kommunikációja során már elérő szabályok szerint él.[122]

3. A KOCKÁZATOT JELENTŐ FELHASZNÁLÓK

Az információs társadalom devianciáival érintettek jellemzéséhez nyújt egyfajta módszert a profilozó, viselkedéskutató megközelítés. A számítógéppel összefüggésbe hozható devianciák közül egyes bűncselekmények tetteseit vizsgálva Saw, Ruby és Post felállították a CITI *(critical information technology insiders)*, azaz a kockázatot jelentő felhasználók kategóriáját, akik változó indítékok alapján, de valamennyien veszélyt jelenthetnek például a számítástechnikai rendszerelemekre nézve.[123] A kiemelten veszélyes felhasználók mindegyikére jellemző az introvertált viselkedés, azaz a hétköznapi problémákat nehezen kezelik, nehezen alakítanak ki közvetlen kapcsolatot az egyes akadályok leküzdésére. Tipikusan olyan emberek, akik inkább e-mailben közlik aggályaikat, mint szemtől-szemben.

A kutatások hat magas kockázatú jellemvonást mutatta ki: személyes és közösségi kudarcélmény (frusztráció), számítógép-függőség (kóros internethasználat), erkölcsi

[119] PARTI K., Számítástechnikai devianciák. In. Kerezsi K. & Parti K. (ed.), *Látens fiatalkori devianciák – Fiatalkori devianciák egy önbevalláson alapuló felmérés tükrében – „ISRD-2"*. ELTE Állam- és Jogtudományi Kar Kriminológiai Tanszék és az Országos Kriminológiai Intézet Budapest 2008. pp. 127-159.
[120] PARTI K., Devianciák a virtuális valóságban, avagy a virtuális közösségek személyiségformáló ereje. *Infokommunikáció és jog* 2007/2. p. 63.
[121] Forrás: http://www.ipsos.hu/site/s-lyos-b-ntett-a-sz-m-t-g-pes-adatlop-s/ [2012-02-05]
[122] PARTI K. & VIRÁG Gy., A szájbergyerek és a bicikli – A kelet-európai gyerekek nethasználatának specifikumai. In: *Kriminológiai Tanulmányok* 2011. 48. kötet. p. 42.
[123] CASEY, E., Criminal Behavior on the Internet. In. Turvey, B. E. (ed.) *Criminal Profiling – an introduction to behavioral evidence analysis*, Elsenier Inc. 84. Theobald's Road, London 2008. pp. 675-676.

rugalmasság, csökkent kitartás-hűség, öntudatosság, együttérzés hiánya. Ezek a személyiségjegyek társulnak olyan tulajdonságokkal, mint hatalomvágy, bosszúvágy, önzőség, nyereségvágy. A vizsgált alanyok indítékai alapján a) a felfedezőket (explorers) a tudásvágy, a kíváncsiság vezérli, b) az irgalmas szamaritánusokat (good samaritans) a másokon való segítés, a dolgok megjavítása mozgatja, c) a hackert az ártó szándék nélküli önkifejezés és bizonyítási vágy, d) a machiavellistát a személyes célok elérése figyelmen kívül hagyva a környezetet, más személyt, e) a kivételeseket egyedülállónak vélt kvalitásuk elismertetése, f) a megtorlókat (avengers) sérelmeik, g) a karrieristákat a haszonlesés, h) a vakondokat (moles) is a nyereségvágy, de azzal a különbséggel, hogy cselekményükkel kárt is okoznak.

4. AZ EGYES ÚJ DEVIANCIÁK

Kérdés, hogy a jelenlegi többség által elfogadott normák és az új szokások közötti konfliktusról van-e szó, vagy a túlzott mobiltelefon-használat, az öncélú felszínes csevegés, csetelés, a virtuális játék- és internetfüggőség valóban devianciák-e. Annak megválaszolása, hogy egy egyébként is demoralizálódó társadalomban élünk, vagy az egyes erkölcsi törvények feloldódása az infokommunikációs eszközök generálta változásoknak tudható be, már igen összetett szociálpszichológiai kutatás eredményeképpen történhetne, ezért ennek eldöntésére nem is vállalkozhatom, azonban a problémák létét igazolja a következő devianciák jellemzése.

Az elmélet után tehát lássunk egy-két jellemző, az információs társadalom megjelenésével együtt felbukkanó deviáns magatartást. Ilyenek tekinthető a cyberszex, internet-mobil telekommunikáció- és számítógép függőség, a számítógép és számítástechnikai rendszer bűncselekmények elkövetési eszközeiként valamint azok célpontjaiként való megjelenése.

4.1. A cyberszex

A pornográf oldalak gyakori látogatása vagy a csetelés ilyen témában a felhasználók hálózaton kívüli életét is jelentősen befolyásolhatja, mégpedig magától értetődő módon akként, hogy az érintettek egyre kevesebb időt töltenek hús-vér szeretteikkel, kollégáikkal, de abban nem minden kutató értett egyet, hogy ez a befolyásolás milyen mértékű.[124] További vizsgált szempont ebben az újszerű problémában, hogy a társadalom még mindig nem tisztázta, hogy a párkapcsolatban élők esetében mi is számít a párkapcsolati hűség megszegésének. Whitty kutatásai szerint például egyes online interakciók, úgymint az erotikus tartalmú beszélgetés, a flörtölés, vagy éppen az ennek során történő kielégülés az általa vizsgált személyek válaszai alapján testi kontaktus hiányában is hűtlenségnek számít a társadalmi értékítélet szerint.[125]

Az internet ugyanakkor megváltoztatja a társadalom és az egyes felhasználók hozzáállását a szexualitáshoz, a szexuális kíváncsiság következmények nélküli kielégítésével valamint a kísérletezés lehetőségével a heteroszexuális viselkedés normálisnak tekintett attitűdje is új tartalmat nyerhet, azaz változik a szexuális kategorizálás értelmezése is.[126] Ennek formái a

[124] WHITTY, M. T. & JOINSON, A. N., *Truth, Lies and Trust on the Internet,* Routledge, 2009. 27 Madison Avenue, New York USA. pp. 86-87.
[125] WHITTY, M. T., *Pushing the wrong buttons: Men's and women's attitude towards online and offline infidelity*. CyberPsychology and Behavior, 6. pp. 569-579.
[126] DIMARCO, H., The elektronic cloak: secret sexual deviance in cybersociety. In. JEWKINS, Y. (ed.), *Dot.cons - Crime, deviance and identity on the Internet*, Willan Publishing 2003. Portland, Oregon USA. pp. 54-55.

megannyi strukturált és kategorizált társkeresőoldal, a felhasználók szavazatai alapján minősített, rangsorolt prostituáltakat és masszőröket hirdető weboldalak, de ide tartoznak az egyre népszerűbb online szerepjátékok, amelyekben a felhasználó a kedvére formált „avatar"-ral játszhat szexuális helyzetekben.[127] A hasonló érdeklődés alapján szerveződő online közösségek kialakításával a felhasználók tapasztalatokat cserélhetnek, bátrabban ismertetik egymás előtt aggályaikat, felfedik egymás előtt addig rejtett devianciáikat és a technológia nyújtotta titkosítás segítségével könnyebben oszthatják meg egymással tiltottnak minősített pornográf felvételeiket.

4.2. Az internetfüggőség, kóros internet-használat

Az internetfüggőség megítélését, önálló betegségként való elfogadását illetően nincs egyetértés a szakterület képviselői között, de megnevezését illetően sincs egységes gyakorlat *(internet addiction, internet dependency, internet abuse)*. Egy dologban e terület kutatói azonban egyetértenek, mégpedig abban, hogy a túlzott internet-használatnak markáns hatásai lehetnek a mindennapi életre vonatkozóan.[128] Internetfüggőség esetén az internet, a világhálón elérhető tartalmak mennyisége és változatossága, maga a böngészés, az információk keresése öncélú örömforrássá válhat. A kérdés az, hogy beszélhetünk-e önmagában való internetfüggőségről, vagy játék-, szex- és információfüggő betegek léteznek, akik csak a választott örömforrás tekintetében különböznek, és az internet csupán eszköz számukra.

Más függőségi viszonyok korábban is ismertek voltak, azonban a különböző fórumokat látogató cset-függők kizárólag az interneten élhetik ki vágyaikat. A kóros internethasználókra általában jellemző a kielégítetlen társas igény, ami kórossá attól válik, hogy a rendszeres kommunikáció ellenére fel sem merül a személyes találkozás lehetősége a kommunikációs partnerekkel. Az érintettek nagy része identifikációs zavarokkal is küzd, ezért az interneten hamis névvel, életkorral vagy akár más nemi szerepben jelennek meg. A kórházba felvett betegeknél általában nem internetfüggőséget diagnosztizálnak, hanem depressziót, szorongást, zavart személyiséget, erre a fajta függőségre csak később, mintegy mellékbetegségként derül fény. Produkálhat elvonási tüneteket, ideges reakciókat, feszültséget válthat ki, ha az illető nem ülhet a monitor elé.[129]

Az ITTK egyik 2002-es kutatása szerint:[130] a tipikus kóros internethasználó férfi, 20 év alatti, az internet nem feltétlenül szükséges a munkájához vagy a tanuláshoz, otthon is internetezik, naponta 6 óránál többet tölt a világhálón, magasan reprezentáltak az általános iskolát végzettek, ami a serdülő korosztályra irányítja a figyelmet, az internethasználat

[127] SHARP, K. & EARLE, S., Cyberpunters and cyberwhores: prostitution on the Internet. In. JEWKINS, Y. (ed.), *Dot.cons - Crime, deviance and identity on the Internet*, Willan Publishing 2003. Portland, Oregon USA. pp. 36-52.

[128] MORAHAN-MARTIN, J., Internet use and abuse and psychological problems. In. Joinson, A., McKenna, K., Postmes, T. & Reips, U-D. (ed.), *The Oxford Handbook of Internet Psychology,* Oxford University Press, 2007. pp. 331-343.

[129] ROMHÁNYI T., A világháló foglyai. Beszélgetés dr. Vincze Gáborral, a gyulai Pándy Kálmán Kórház pszichiátriai osztályának osztályvezető főorvosával. Forrás: http://nol.hu/cikk/333242/ [2012-02-05]

[130] A kutatás résztvevői: Ritter Andrea, Dr. Fábián Zsolt, Hoyer Mária, Pillók Péter. A csoport kisebb módosításokkal a Kimberly Young amerikai pszichológus által alkalmazott kérdőívet használta, adaptálva azt a magyarországi viszonyoknak megfelelően. A kérdőív 2 részből állt: 11 demográfiai és 20, a káros internethasználatot mérő kérdést tartalmazott. A vizsgálat ideje alatt a kérdőívet tartalmazó honlapot 1714-en töltötték ki (válaszadási ráta 70,8%). Az elemzésbe 1529 érvényes adatlap került bele (csak azok, amelyekben minden kérdésre válaszoltak). Forrás: http://archive.infinit.hu/2002/0307/index.html [2011-07-31]

kezdetének ideje pedig nem szignifikáns a függőség kialakulására nézve. A kutatók szerint a célszerűbb a „kóros internethasználat" fogalmát használat, az érintettek ugyanis a kapott eredmények alapján három, egymástól gyakran nehezen elkülöníthető csoportba sorolhatók, így megkülönböztették az addiktológiai modellbe, a szekunder internetezők táborába és az impulzuskontroll zavarokkal rendelkezők csoportjába tartozó kóros internetezőket.

Az addiktológiai modellbe tartoznak azok, akik megfelelnek az internet-addikció kritériumainak, arányuk 6%. A férfiak lényegesen többen vannak, mint a többi csoportban (81%). Ez a legfiatalabb csoport, a 20 év alattiak 46%-ot tesznek ki közülük. A szekunder internetezők elsősorban azért neteznek sokat, mert bizonyos pszichés szükségleteket könnyebben ki tudnak elégíteni online, mint a valós életben, olyan felhasználók, akik kapcsolati hálójuk elégtelensége miatt mintegy másodlagos örömforrásként használják az internetet, arányuk 11%. Az impulzuskontroll zavara a 21-30 éves korosztályra jellemző, arányuk 12%. Az egészségeseknek tekinthető felhasználók aránya 71%. A függőknek és a szekunder internetezőknek ritkábban van szükségük munkájukhoz, vagy a tanuláshoz internetre, jellemző rájuk, hogy leginkább otthon használják. Mindhárom problémás csoportnál megfigyelhető a napi 3 óránál hosszabb internethasználati idő, a függők 46%-a napi 6 óránál többet ül a képernyő előtt.

A problémás csoportokba tartozók általában nem információszerzés vagy levelezés céljából neteznek, hanem egyéb tevékenységeket végeznek: a függőkre jellemző a csevegés és kimagasló értékkel a játék, az impulzuskontroll-zavarokkal küszködőkre a játék és a multimédiás csevegés, a szekunder csoportra a csevegés, és kimagasló értékkel a multimédiás cset jellemző. Mindhárom problémás csoportban gyakori a pszichológus segítségét igénylő panasz.[131]

4.3. A cyberbullying, sexting

A közösségi oldalak (pl. Facebook, Iwiw) fiatalok közötti általános és mindennapi használatának számos adatvédelmi kockázata ismert, emellett azonban több, eddig ismeretlen és negatív trend erősödése is megfigyelhető. A közösségi oldalak kockázataival uniós szinten részletesen foglalkoznak például az ENISA jelentései[132], vagy az Európai Gazdasági és Szociális Bizottság saját kezdeményezésű véleménye.[133] A 2008-as Biztonságosabb Internetért Fórum[134] keretében az Európai Bizottság nyilvános konzultációra bocsátott egy kérdőívet a közösségi hálózatokról.[135] A beérkezett válaszok

[131] A kutatás eredményei szerint más, addikcióval kapcsolatos problémája elsősorban a függőknek, kisebb mértékben az impulzuskontroll-zavarosoknak volt. Az impulzuskontroll-zavarban szenvedők csoportjának elkülönülése arra utal, hogy a kóros internethasználók nem képeznek homogén csoportot. A kutatók szerint az eddigi eredmények alapján úgy tűnik, érdemesebb egy kevésbé specifikus diagnosztikai kategóriában gondolkozni, ami akár kóros internet-használatnak is nevezhető. Valószínűnek látszik ugyanis, hogy ez nem képez majd egy homogén csoportot, hanem olyan alcsoportok mentén szerveződik, amelyeknek a pszichopatológiája, terápiája és prognózisa különböző.

[132] ENISA Security Issues and Recommendations for Online Social Networks, Forrás: www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf. [2012-02-19]

[133] 2010/C 128/12

[134] http://ec.europa.eu/information_society/activities/sip/events/forum/forum_sepet_2008/index_en.htm [2012-02-19]

[135] http://ec.europa.eu/information_society/activities/sip/policy/consultations/ageverif_sns/index_en.htm [2012-02-19]

alapján[136] az az általános nézet, hogy a közösségi oldalak használatakor a kiskorúakat leginkább az internetes zaklatás *(cyberbullying)*, a magánélet megsértése és a szexuális célú megkörnyékezés *(grooming)* veszélye fenyegeti. Érdemes tehát az említett trendek közül kettővel részletesebben foglalkozni.

A cyberbullying olyan, infokommunikációs eszközök segítségével elkövetett támadó jellegű cselekmény, amely ismétlődő jelleggel irányul egy meghatározott áldozat ellen, amelytől az nem tudja önmagát megvédeni.[137] A cyberbullying tehát olyan durva tréfa, ugratás, amely során jellemzően a 13-17 éves fiatal korosztályok tagjai különböző platformokon lejáratják egymást. Kamerával felszerelt mobiltelefon birtokában egy bárhol megtörtént balesetet, vagy kellemetlen jelenetet már aznap este tömegek nézhetnek valamelyik közkedvelt közösségi oldalon. A zaklatáshoz *(stalking)* közel álló jelenség lényegében egy személy magánszférája elleni támadás.[138]

A sexting olyan tevékenységként definiálható, amely során a felhasználók mobiltelefonon önmagukról készített, már-már pornográf, erotikus, vagy ahhoz közelálló felvételeket és szexuális töltetű üzeneteket küldenek egymásnak.[139] Ehhez hasonló magatartás, amikor a fent említett képeket internetes közösségi oldalakon teszik közzé. A jelenségről néhány számadat tükrében lehet állást foglalni. Egy 2008-ban, az Amerikai Egyesült Államokban, a fiatalkori és nem tervezett terhességek megelőzése érdekében folytatott nemzeti kampány során készített kutatás eredményei alapján a tizenhárom és tizenkilenc évesek közötti korosztály 20%-a küldött már önmagáról meztelen vagy félmeztelen képet.[140] Egy további érdekes adat, hogy a lányok 25%-a, míg a fiúk 3%-a válaszolt igennel arra a kérdésre, hogy kapott-e már olyan erotikus képet, amit eredetileg nem kívántak megosztani velük. A tizenévesek 39%-a küldözget szexuális töltetű üzeneteket, 48%-uk kapott már ilyen üzenetet. Egy újabb kutatás eredményei alapján ezen arányok növekedtek, a 13-19 éves korosztály 65,5%-a sextingelt már.[141] A legtöbb, egyáltalán „felderített" sexting eset során az erotikus jellegű felvételeket az érintettek önmagukról vagy közös megegyezéssel másról készítették, amely felvételek sorsa a későbbiekben már tőlük függetlenül alakult.

A nyilvánvaló körülmény, amely visszaélésekre adhat lehetőséget az, hogy a többszörözött képek minden további engedély és egyéb korlát nélkül továbbíthatók. A felelőtlenség mellett egy másik motivációt a bosszúvágy jelenti, általában azokban az esetekben, amikor egy párkapcsolat megszakadása után az egyik fél – legtöbbször a fiú, férfi – a párjáról készített felvételeket hozza nyilvánosságra.[142] Egyesek szerint a jelenség oka pusztán az,

---

136 http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/summaryreport.pdf [2012-02-19]

137 SMITH, P. et al: Cyberbullying: Its nature and impact in secondary school pupils. *Jurnal of Child Psychology and Psychiatry* 2008. 49. p. 376.

138 KIFT, S., CAMPBELL, M. & BUTLER, D., Cyberbullying in Social Networking Sites and Blogs: Legal Issues for Young People and Schools. *Journal of Law, Information and Science*, Vol. 20(2) 2009/2010.

139 MCDONALD, J., Sexting and Excessive Texting: Symptoms of Teen Dating Violence? *Children's Legal Rights Journal* 2010. Vol. 30. No. 4. p. 19.

140 ARCABASCIO, C., Sexting and Teenagers: OMG R U Going 2 Jail??? *Richmond Journal of Law & Technology*, Volume XVI, Issue 3. p. 2.
A forrás hivatkozása: The National Campaign to Prevent Teen and Unplanned Pregnancy http://www.thenationalcampaign.org/sextech/PDF/SexTech_Summary.pdf [2011-07-31]

141 LIPKINS, S., LEVY, J. & JERABKOVA, B., Sex Offenders Statistics by a Voice of Reason, Sexting Part II.: Results and Recommendations of Sexting Study 2009. Forrás: http://sexoffender-statistics.blogspot.com/search/label/Sexting [2012-02-05]

142 RICHARDS, R. & CLAVERT, C., *When Sex and Cell Phones Collide: Inside the Prosecutin of a Teen Sexting Case*, 32 Hastings Comm. & Ent. L.J. 1, 8. 2009. pp. 3-5.

hogy a mai tinédzserek egyszerűen szexuálisan túlfűtöttek, és csak szórakozásból küldözgetik az erotikus üzeneteket.[143] Mások szerint mindez csak a fiatalok kísérletező magatartása, amelynek során egyszerűen csak rossz döntéseket hoznak.[144] Azonban a témakörrel foglalkozók abban már egyetértenek, hogy az erotikus felvételek haragból vagy bosszúból történő terjesztése további létező, emocionális visszaélésekkel és erőszakkal jellemezhető, fiatalkori párkapcsolati magatartásminták része is lehet.[145] Hiba volna azt feltételezni, hogy csak a fiatal generációkra jellemző ez az attitűd, azonban technikai lehetőségek birtokában a tizenévesek emocionális élete, alapvetően impulzív viselkedése az oka annak, hogy nem mérlegelik a hosszú távú következményeket.[146]

A sexting új jelenségének etikai megítélése nem tárgya a dolgozatnak, az viszont megemlítendő, hogy milyen jogellenes cselekményeket vethet fel. Nyilvánvalóan felmerül a tiltott pornográf felvétellel visszaélés lehetősége, de emellett – az életkori eltérések esetén – a személyes adattal visszaélés vétsége is, azonban a probléma okának meghatározása és kezelése tekintetében, a cselekmény felfogását illetően még az Egyesült Államokban sincs egységes koncepció.[147] Egyedüli problémát azon körülmény megítélése okozza, hogy a felvételeket sok esetben az érintettek önmaguk készítik és továbbítják, azaz a bűncselekményi tényállások megalkotásának elsődleges céljára figyelemmel a sexting erodálja a felelősségre vonás egyes, védendő jogi tárgyra vonatkozó elveit.

Ami viszont az értekezés jelen fejezete szempontjából jelentőséggel bír, az a felhasználók magánszférához, a privacy-hoz való viszonyának átértékelődése. Mindkét trend annak tanújele, hogy a privacy-hoz viszonyulás negatív irányban változott, hiszen amíg a cyberbullying más magánszférájának a semmibevétele, addig a sexting a felhasználó saját magánszférájának a teljes megnyitását jelenti. Ezek az új trendek érzékletesen jellemzik nemcsak a morál változásait, de az érintett szereplők egyes védett társadalmi értékekhez való viszonyát is.

4.4. Az e-bűncselekmények

A társadalmi és jogi normákkal szembeszegülő és a társadalmi együttélést leginkább támadó magatartások a bűncselekmények. A számítógép már nemcsak a büntetendő cselekmények elkövetésének eszköze, hanem egyre inkább az őket összefogó informatikai rendszerek, illetőleg a bennük tárolt, vagyoni vagy személyes értéket megtestesítő adatok válnak a cselekmények célpontjává. Az informatikai bűncselekmények elemzése több okból is nehézségekbe ütközik. Szemben a „hagyományosnak" tekinthető bűncselekményekkel kevés a rendelkezésünkre álló statisztikai adat, a különleges infrastruktúra miatt magas a látencia, speciális az elkövetési hely, idő, eszköz, az elkövetésez speciális szakismeret szükséges, kevés adat van az elkövetők személyéről, speciális a jogi tárgy valamint az elkövetési tárgy. A címben szereplő „e-bűncselekmények" fordulatot olyan semleges kifejezésként alkalmazom, amely egyaránt

[143] DURHAM, M. G., *The Lolita Effect: The Media Sexualization of Young Girls and What We Can Do About It,* The Overlook Press, Peter Mayer Publishers, Inc. Woodstock and New York, 2008.
[144] Például: RICHARDS és CLAVERT.
[145] MCDONALD, J., Sexting and Excessive Texting: Symptoms of Teen Dating Violence? *Children's Legal Rights Journal* 2010. Vol. 30. No. 4. p. 21.
[146] MCLAUGHLIN, J. H., Crime and Punishent: Teen Sexting in Context. *Penn State Law Review* Vol. 115:1 2010. p. 145.
[147] BAUMLER, K., Sexting: Is it Teenagers Being Teenagers? Or Is It Child Porn? *Children's Legal Rights Journal,* Vol. 30. No. 4. 2010.

utal a számítástechnika alkalmazásával, az eszközök ellen, és az interneten elkövetett hagyományos deliktumokra.

Az információ nemcsak gazdasági, vagyoni érdekek hordozója lehet, hanem társadalmi közérdek vagy magánérdek megtestesítőjeként is értékkel bírhat, tehát az információs társadalom új bűncselekményei többfajta jogi tárgyat sértő vagy veszélyeztető bűncselekmények. Elnevezésüket, csoportosításukat illetően nincs egyetértés a témakörrel foglakozók között, ezért gyakran találkozhatunk a – sokszor ugyanazon bűncselekményeket felölelő – következő gyűjtőnevekkel: informatikai bűncselekmények, számítógépes-, számítástechnikai bűncselekmények, vagy számítógéppel érintett bűncselekmények *(computer-crime, cumputer-related crime, cyber-crime).*

A dolgozatban számítástechnikai bűncselekményeknek a számítástechnikai rendszer és adatok elleni bűncselekményeket tekintem, tehát a számítástechnikai rendszer zavartalan működését, a benne tárolt adatok megbízhatóságához, hitelességéhez, titokban maradásához valamint mindezekhez fűződő gazdasági érdekeket sértő vagy veszélyeztető bűncselekményeket (Btk. 300/C. §, 300/E. §), míg informatikai bűncselekmények alatt értem az egyes szerzői joggal kapcsolatos bűncselekményeket (Btk. 329/A. §, 329/B. §) és az infokommunikációs eszközökkel elkövetett zaklatást (Btk. 176/A. §, cyber-stalking), de ide tartoznak az egyre inkább csak számítógéppel támogatott adatfeldolgozó rendszerek miatt az adatvédelmi bűncselekmények és a tiltott pornográf felvétellel visszaélés vagy a készpénz-helyettesítő fizetési eszközzel visszaélés egyes tényállásai is.

5. A FEJEZET ÖSSZEFOGLALÁSA

Az információs társadalom devianciái olyan létező, új jelenségek, amelyek pontos oka ha nem is ismert, azonban az kétséget kizáró módon megállapítható, hogy jelenlétük nagymértékben az infokommunikációs technika elterjedt használatához köthető. A devianciák kialakulása kapcsolatba hozható azokkal a korábban részleteiben is elemzett társadalmi változásokkal, amelyekben a technológiának meghatározó szerepe van. A devianciák maguk a társadalmi értékrendek, szokások változására mutatnak rá, amelyektől a jog, azon belül is a büntetőjog nem függetlenítheti magát. Az információs társadalom és devianciáinak a büntetőjogi vizsgálatok szempontjából is lényegesnek tekinthető elemei a következő pontokba foglalhatók össze.

1) A fiatal generációk meghatározó jelenléte. Az érintett felhasználók, a fiatalabb generációk tömegének jelenléte az infokommunikációs eszközök által biztosított interakciókban azt jelenti, hogy az általuk képviselt értékrend, szemlélet, szabályrendszer válik domináns, meghatározó elemmé a változás gyorsasága, intenzitása miatt. Emellett hiányzik a generációk által közvetített átmenet, amely az új környezet normáinak elsajátítását, tanítását biztosítaná. A fiatalok a számítástechnikai devianciák elkövetéséhez kedvező morális attitűddel rendelkeznek, hiszen viselkedésükben még nem rögzültek a társadalmi erkölcsök, ezért azokat könnyebben helyettesíthetik a népszerűbbnek ítélt online viselkedési kultúra normái.[148]

2) Az enyhe közösségi szankciók. A társadalom még mindig nem rendezte, tisztázta, hogyan kezelje, egyáltalán miként tekintsen az egyes új élethelyzetekre. Amíg egy-egy új trend, magatartás nem rendelkezik egységes – vagy legalábbis általánosan osztott –

[148] PARTI K., Számítástechnikai devianciák. In. Kerezsi K. & Parti K. (ed.), *Látens fiatalkori devianciák – Fiatalkori devianciák egy önbevalláson alapuló felmérés tükrében – „ISRD-2”.* ELTE Állam- és Jogtudományi Kar Kriminológiai Tanszék és az Országos Kriminológiai Intézet Budapest 2008. p. 127.

társadalmi megítéléssel, addig az arra vonatkozó büntetőjogi válasz sem bír megfelelő erejű morális háttérrel.

3) Új társadalmi viszonyok megjelenése. Az előző ponthoz kapcsolódóan megállapítható, hogy az infokommunikációs eszközök nyújtotta közösségszervező és formáló lehetőségek olyan új élethelyzeteket és társadalmi viszonyokat alakítottak ki, amelyekben az együttélés még formálódó szabályainak megsértésére a társadalmi értékítélet megnyilvánulásaként adott válaszok közül a büntetőjog helye nem eleve adott, nem egyértelmű.

4) Az infokommunikációs eszközök segítségével elkövetett bűncselekmények népszerűségének egyik további oka, hogy az eszközök könnyen elérhetők, a fiatal generációk nagyobb része birtokolja, és napi rendszerességgel használja őket.

A kérdés az, hogy abban a környezetben, amelyben az egyénekre a korábbi fejezetekben leírt hatással van az ismertetett technológia, hol húzódik a társadalmi önszabályozás, a jogrendszer enyhébb szankciórendszerével operáló jogágainak a területe, mit jelentene az állam megelőzést elősegítő oktatási kötelezettsége, és honnan kezdődik a büntetőjog uralma. A jogalkotónak – legfőképpen a büntetőjogi szabályozás politikájának meghatározásakor – mindezen szempontokat figyelembe kell vennie, amikor egy alakuló, formálódó társadalmi kapcsolatrendszerben a büntetőjog belépésének határvonalát kívánja meghúzni.

Ebben vezérfonalként majd az alkotmányos büntetőjog elveinek kell utat mutatniuk, amelyekhez viszonyítva, amelyeknek megfeleltetve kell továbbra is megalkotni, majd alkalmazni és értelmezni a szükséges bűncselekményi tényállásokat, és a büntetőeljárási szabályokat. Előbb azonban – annak okán, hogy a dolgozat technológiai vonala ne szakadjon meg – a számítástechnikai környezetre és a számítástechnikai bűncselekményekre vonatkozó fogalmi rendszerezéssel indokolt továbbhaladni.

III. FEJEZET: ALAPFOGALMAK A NEMZETKÖZI JOGFORRÁSOK ALAPJÁN

Az előző fejezetekben sor került az információs társadalom büntetőjogi vonatkozásainak bemutatására. Az újabb kérdés az, hogy melyek azok a bűncselekmények, amelyek a további vizsgálat körébe vonhatók, és milyen szempontok szerint szükséges őket elemezni, illetve milyen fogalmi környezet veszi őket körbe. Informatikai-, számítógépes-, számítástechnikai, internetes bűncselekmény vagy csúcstechnológiai-bűnözés? Már e kifejezések sora is jól mutatja, hogy a klasszikus bűncselekmények mellett pár évtizeddel ezelőtt – büntetőjogi léptékkel mérve nem is oly régen – megjelent a tilalmazott magatartásoknak egy olyan új köre, amelyet valamely jellemvonása – legtöbbször az elkövetés eszköze – alapján az előbb felsorolt megnevezések egyikével illethetünk.

A számítógéppel kapcsolatos deliktumok egy részére az jellemző, hogy a támadás céljai már maguk a számítógépek, a kommunikációs berendezések, adatátviteli hálózatok, és az adatok, ugyanakkor az elkövetők szándéka irányulhat ezen eszközök felhasználásával más, hagyományos értékekre is.[149] Az információs társadalom új típusú bűncselekményeinek alapvető jellemzője tehát az, hogy az információ maga – mint vagyoni értéket megtestesítő dolog –, és annak környezete válik a bűncselekmények tárgyává.[150] Ugyanakkor az információs társadalomról szóló fejezet megállapításai alapján nem szabad megfeledkezni arról sem, hogy az információvédelemnek nem csupán az információk tulajdonosainak vagy hordozóinak gazdasági érdekeit kell figyelembe vennie, hanem azokét is, akiket az információk tartalma érint. Az információnak ebből az aspektusából származnak a privacy, szűkebb értelmében a személyiségi jog védelmével kapcsolatos követelmények, elsősorban az elektronikus úton történő adatfeldolgozás miatt.[151] Az információ tehát nemcsak gazdasági, vagyoni érdekek hordozója lehet, hanem közérdek vagy számos magánérdek megtestesítőjeként is értékkel bírhat. De miként is ölthetnek testet az eddig ismertetett szempontok egy-egy büntetőjogi tényállásban?

Nagy Zoltán szerint a számítógéppel elkövetett bűncselekmények jogi minősítésének nehézsége abban ragadható meg, hogy az elektromágneses impulzus, az adat – mint testetlen, kézzel nem fogható dolog – értelmezhető-e a büntetőjog tradicionális kategóriáival vagy sem.[152] Ennek okán a tényállások megfogalmazásakor olyan terminológiával kell operálnia a jogalkotónak, amely megfelel mind az informatika mind a jogtudomány elvárásainak és figyelemmel kell lennie a várható technológiai fejlődés jelentette kihívásokra is.

1. FOGALMI ALAPOK

Az információkra vonatkozó jogi szabályokat nem lehet analógia útján levezetni a testi dolgokról szóló rendelkezésekből, hanem a maguk önálló alapjából kell kidolgozni őket. Ezért mindenekelőtt az értekezés egységes fogalomhasználatának megalapozására, másrészt az információk környezetének megértéséhez nélkülözhetetlen az alábbi fogalmak érintőleges tárgyalása.

---

[149] SZATHMÁRY B., *Jogi Informatika. Tanulmányi segédlet a jogi informatika oktatáshoz*, Debreceni Egyetem Állam-és Jogtudományi Kar. én. p. 89.
[150] VILLÁNYI J., Az Európa Tanács Informatikai bűnözéssel kapcsolatos egyezményéről, *Magyar Jog* 2001/8. p. 464.
[151] SIEBER, U., A számítógépes bűnözés és más bűncselekmények az információtechnika területén, *Magyar jog*, 1993/1. p. 46.
[152] NAGY Z., Konferencia az információtechnikai bűnözésről, *Magyar Jog*, 1993/2. p. 102.

1.1. A számítástechnikai rendszer és az adat mint elkövetési tárgyak

A büntetőjogi tényállások elemzése előtt – az interdiszciplináris jogterületre figyelemmel – először az tisztázandó, hogy a számítógépes bűncselekmények esetében az adat mely fogalmával kell dolgozni. Az ISO 27000 szabványcsalád adatfogalmára építve a Cyber-crime Egyezmény és az EU kerethatározat megfogalmazása szerint a számítástechnikai adat tényeknek, információknak, illetőleg fogalmaknak minden olyan formában való megjelenése, mely számítástechnikai feldolgozásra alkalmas, ideértve azon programot is, mely valamely funkciónak a számítástechnikai rendszer által való végrehajtását biztosítja.[153] Az adat legfontosabb ismérve tehát az, hogy számítástechnikai feldolgozásra alkalmas legyen, de az Egyezmény ide sorolja a feldolgozásához szükséges programot is. Ez tehát meglehetősen széles kört ölel fel. Az adatok és az azokat kezelni képes rendszerek tágabb körű megfogalmazásának forrása és így a számítástechnikai bűncselekmények jogi és elkövetési tárgyának alapja tehát az információ- illetve adatbiztonság fogalomrendszere köré épül.

Az adatbiztonság vonatkozásában a legáltalánosabb értelmében minden testet öltött információt, kódolt közleményt adatnak tekintünk. Az adat az információ megjelenési formája, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája.[154] Az adat esszenciája tehát az általa megtestesített információ, amelyhez – a teljesség igénye nélkül – gazdasági, össztársadalmi és személyes érdekek egyaránt fűződhetnek. A támadás alapvetően az információt hordozó adatot érheti, veszélyeztetheti az adat bizalmasságát, sérthetetlenségét, hitelességét, de értünk a támadás alatt minden olyan fenyegetést, amely a rendszer működését, az adatok rendelkezésre állását, a funkcionális követelményeknek megfelelő felhasználásukat veszélyezteti.[155] Az adat megvédése érdekében minden esetben céltudatos, tervszerű emberi magatartás szükséges, amely a kívánt emberi magatartásokat előírások (jogszabályok, szabályzatok, szabványok stb.) formájában rögzíti.[156] Ebben az értelemben a biztonság az információs- és informatikai rendszerekben olyan előírások betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.[157] Az adatot tehát az így körülírt minőségében kell büntetőjogi védelemben részesíteni.

Ezt követően azt a környezetet kell jellemeznünk, amelyben az adat elhelyezkedik. Az adatra irányuló támadások az adatokat ugyanis rendszerint nem közvetlenül, hanem az adatot körülvevő rendszerelemeken keresztül érik. Ilyenek: a rendszer fizikai környezete és infrastruktúrája, hardver rendszer, szoftver rendszer, kommunikációs, hálózati rendszerek, adathordozók, dokumentumok és dokumentáció, személyi környezet. Az Egyezmény és a kerethatározat szerint számítástechnikai rendszer bármely olyan önálló eszköz illetve egymással kapcsolatban lévő vagy összekötött eszközök összessége, amelyek, illetőleg amelyeknek egy vagy több eleme program végrehajtásával adatok automatikus

[153] Cyber-crime Egyezmény 1 Cikk, b) pont.

[154] Ha értelmezzük, már információvá válik, ami az adat esszenciájaként értéket képviselhet birtokosa számára.

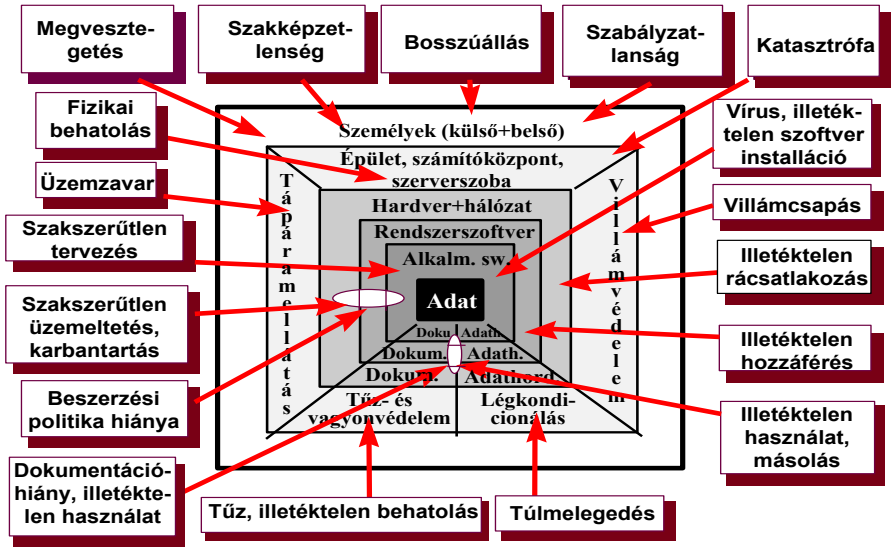
[155] A támadás eredendően emberi magatartást feltételez, mégpedig szándékos emberi magatartást, tudjuk azonban, hogy az adat sérülését eredményezheti emberi gondatlanság, de az embertől független körülmény, pl. természeti jelenség, mint pl. a villámcsapás is.

[156] Az ISO (International Standards Organisation) az ISO 27000-es szabványcsaládot tartja fenn az információvédelemmel összefüggő szabványok részére.

[157] CSUKA D., GASPAREZT A., TARJÁN G. & DÓSA I., Szabványos információbiztonság, ISO 27001-nek való megfelelés – Információvédelmi fogalmak: In. Takács T. (ed.), *Az informatikai jog nagy kézikönyve*, Complex Kiadó, Budapest, 2009. p. 688. Lásd egy korábbi forrásban részletesebben: az Informatikai Tárcaközi Bizottság 12. számú ajánlása az informatikai rendszerek biztonsági követelményeiről.

feldolgozását biztosítja. A hazai szabályozás ezt a fogalmat vette át kismértékben módosítva: számítástechnikai rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés vagy egymással kapcsolatban lévő ilyen berendezések összessége.[158] Látható, hogy mindkét meghatározás tágabban igyekszik definiálni a számítástechnikai rendszer fogalmát.[159] A rendszerelem a rendszer olyan jól elkülöníthető egysége, amely annak bevezetéséhez, kiépítéséhez szükséges, amelyet a fenyegető tényezők érintenek. A rendszerelemek tárgyalása azért lényeges, mivel az adatok, rendszerek támadása nem közvetlenül, hanem az egyes rendszerelemeken keresztül történik. Ebben a körben szorul értelmezésre a szenzorok működésének befolyásolása, hiszen azok olyan rendszerelemeknek mondható eszközöknek tekinthetők, amik a környezetből származó ingereket érzékelik és azokat számítástechnikai adatokba átalakítva továbbítják. A későbbi probléma a következő: a környezet és a szenzor közötti fizikai közeg megzavarása viszont kívül esik a rendszeren, a rendszer működését nem akadályozza, az ilyen cselekmény egyszerűen értelmezhetetlen adattal látja el a rendszert, vagy az adatoktól megfosztja. Mindez azonban a rendszernek mint meghatározott célra alkotott berendezésnek a meghatározott – adott esetben védett – jogi érdeket megtestesítő funkcionalitását sérti.

Az adat maga tehát közvetlenül nem elérhető, ebből következően a védelmi rendszereknek is az adatot körülvevő rendszerelemekhez kell kapcsolódniuk. A struktúra vázlatát a következő ábra jól szemlélteti:[160]



Az ábra elemzése alapján arra a következtetésre juthatunk, hogy az adatot fenyegető veszélyek sokfélesége folytán teljes biztonságot soha el nem érhetünk, a cél zárt, teljes körű, folyamatos és a kockázatokkal arányos védelem megtervezése, kiépítése, működtetése lehet csak. Az adatbiztonság megvalósítása védelmi tevékenységek sorozatát

[158] Btk. 300/F. § (3) bekezdés.

[159] A meghatározás felöleli a számítógépes rendszeren túl a kommunikációs rendszert is, illetve minden, akár fizikai eszközök, akár elektronikus vagy rádióhullámok útján összekapcsolt, információáramlást, adatkezelést lehetővé tevő rendszert. Lényeg, hogy ezen definíciók ismérvei alapján az informatikai rendszer fogalma kiterjeszthető az úgynevezett nagyszámítógépekre, irodai rendszerekre, munkahelyi számítógépekre (pc-k, laptopok, munkaállomások), mikroszámítógépekre (ilyen lehet a mobiltelefonok chipkártyája), kommunikációs rendszerekre, számítógép-hálózatokra.

[160] Forrása az Informatikai Tárcaközi Bizottság 12. számú ajánlása az informatikai rendszerek biztonsági követelményeiről. Bár a forrás meglehetősen idejétmúltnak tűnhet, az ábra szemléletesen mutatja be a lehetséges problémák mibenlétét.

jelenti, így indokolt lenne adatvédelemről beszélni, ez a fogalom azonban már foglalt.[161] Az adatvédelem az adatok egy szűkebb körére, a személyes adatokra vonatkozó jogi védelmet biztosító szabályozást, míg az itt tárgyalt fogalomkör valamennyi adat biztonsága érdekében kifejtendő emberi magatartást és ennek technikai feltételeit, az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszerét jelenti.

A hatékony adatbiztonság olyan előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és megbízhatóságát érintik, és amelyeket az informatikai rendszerekben vagy komponenseikben, valamint az informatikai rendszerek vagy komponenseik alkalmazása során megelőző biztonsági intézkedésekkel lehet elérni. Az ISO 27001 szabvány fogalomkörében a bizalmasság az információ azon tulajdonsága, hogy jogosulatlan személyek, entitások vagy folyamatok számára nem hozzáférhető. A sértetlenség az információ azon tulajdonsága, hogy az eredeti állapotának megfelel és teljes, míg a rendelkezésre állás jelentése szerint az információ azon tulajdonsága, hogy elérhető a feljogosított személyek, entitások és folyamatok számára a szükséges időpontban.[162]

Más, tágabb értelmű megfogalmazásban az informatikai biztonság alatt valamely informatikai rendszer azon állapota értendő, amelyben a kockázatokat, amelyek ezen informatikai rendszer bevezetésekor a fenyegető tényezők alapján adottak, elfogadható intézkedésekkel elviselhető mértékűre csökkentettük.

Az informatikai biztonság két alapterületet foglal magába: az információvédelem, amely az adatok által hordozott információk sértetlenségének, hitelességének és bizalmasságának elvesztését hivatott megakadályozni és a rendszer megbízható működése területét, amely az adatok rendelkezésre állását és a hozzájuk kapcsolódó alkalmazói rendszerek funkcionalitását hivatott biztosítani. Az informatikai rendszerben működő alkalmazások és a hozzájuk kapcsolódó adatok fenyegetettségét a legszélesebb körben a következőkkel lehet jellemezni: az adatra vonatkozóan a bizalmasság elvesztése, a sértetlenség elvesztése, a hitelesség elvesztése, míg az adatot körülvevő rendszerre vonatkozóan a rendelkezésre állás elvesztése, a funkcionalitás elvesztése. Ezeket a fogalmakat alapfenyegetettségeknek nevezzük. A megbízható működés fogalma a rendelkezésre állás és a funkcionalitás biztosítását jelenti.

Mindezek alapján a számítástechnikai bűncselekmények jogi tárgyai a következők: *a számítástechnikai rendszerek zavartalan működése, a bennük kezelt adatok megbízhatóságához, hitelességéhez, titokban maradásához fűződő érdek, és mögöttesen az ezekhez fűződő érdekek.* A jogi tárgy tehát e tekintetben mindig kettős.

[161] Megemlítendő, hogy ez az éles elhatárolás az adatvédelem és adatbiztonság fogalmát illetően nem tekint hosszú múltra vissza. Korábban, az ELTE Jogi informatika jegyzetében Gödöny József az adatvédelmet a számítógépen tárolt és kezelt adatok jogosulatlan emberi beavatkozás (kiolvasás, megváltoztatás, megsemmisítés, jogosulatlan felhasználás) elleni védelemként definiálta, az adatbiztonságot pedig a számítógépen tárolt és kezelt adatok véletlen (nem szándékos emberi beavatkozás eredményeként bekövetkező) esemény (szoftver vagy hardver hibás működése, elöregedés, külső behatás, stb.) által okozott rongálódás, megváltozás, megsemmisülés elleni védelmeként. Kovacsicsné Nagy K., (ed.) Jogi informatika, ELTE egyetemi jegyzete 1996. p. 79.

[162] CSUKA et al. 2009. p. 688.

1.2. További adat-meghatározások

A fenti adat-fogalom mellett büntetőjogi szempontból – főképp a bizonyítási kérdésekben – kiemelt jelentőséggel bírnak az Egyezmény következő meghatározásai. A forgalmi adat *(traffic data)* minden olyan, a számítástechnikai rendszeren átmenő és a számítástechnikai rendszer mint kommunikációs lánc egyik eleme által létrehozott kommunikációra vonatkozó adat, amely jelzi a kommunikáció származási és rendeltetési helyét, útvonalát, időpontját, időtartamát, terjedelmét vagy a szolgáltatás típusát.[163] Ezen adatfogalomnak feleltethető meg a 180/2004. (V. 26.) Kormányrendelet 2. § e) pontjában meghatározott kísérő adat fogalma. Kísérő adat az elektronikus hírközlési szolgáltató hálózatában és azzal összefüggő informatikai rendszereiben az adott kommunikációval összefüggésben az adott szolgáltatás teljesítésével kapcsolatban keletkező, illetve az elektronikus hírközlési szolgáltató hálózatában rendelkezésre álló adat.

A tartalomra vonatkozó adatok *(content data)* a kommunikáció információtartalmát jelölik. Az előfizetőkre vonatkozó adatok *(subscriber data)* az adott szolgáltató által birtokolt, az előfizetőkkel kapcsolatos, a tartalomra vagy a forgalomra vonatkozó adatoktól eltérő információ, amely lehetővé teszi az előfizető által használt kommunikációs szolgáltatás típusát, a szolgáltatás időszakát, az előfizető személyazonosságának azonosítását.

Miért van szükség ezen adatok meghatározására és megkülönböztetésére? Ezen adatkörök eltérő szenzitivitásúak, ekként a büntetőeljárás, a bizonyítás, a felderítés során a magánszférát érintő hatósági beavatkozások lehetőségét is differenciálni kell a szerint, hogy melyik adat megismerésére és meddig jogosult az eljáró hatóság.[164]

Ebben a körben jut jelentőséghez a hírközlési hálózatokban keletkezett adatok tárolásáról szóló 2006/24/EK európai parlamenti és tanácsi irányelve (adatvisszatartási irányelv), amely a bűnügyi együttműködés hatékonyabbá tétele érdekében részletesen szabályozza az internetszolgáltatók adatrögzítési és közlési kötelezettségét. Mindezzel azonban a dolgozat a büntetőeljárási kérdésekről szóló utolsó fejezete foglalkozik részletesen.

2. AZ INFORMATIKAI BŰNCSELEKMÉNYEK RENDSZEREZÉSE

Figyelemmel a fenti meghatározásokra informatikai bűncselekményeknek nevezhetjük azon bűncselekményeket, amelyek elkövetésével jellemzően valamely adatot, vagy az adatkezelés, adatfeldolgozás folyamatát és az ezekhez fűződő érdeket sért vagy veszélyeztet az elkövető. A bűncselekmények jogi tárgyai alapján az informatikai bűncselekmények tovább csoportosíthatók, mivel a különböző védett társadalmi viszonyok különböző jogi, szűkebben különböző büntetőjogi szabályozást igényelnek. Ezért az informatikai bűncselekményekhez sorolhatjuk az adatvédelmi, a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének bűncselekményeit, a tiltott pornográf felvétellel visszaélést és a számítástechnikai bűncselekményeket.

2.1. Adatvédelmi bűncselekmények

Az egyre inkább kizárólag számítógéppel történő adatfeldolgozás miatt az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény szerinti,

[163] A 2001. évi CXXI. törvény miniszteri indokolása.
[164] SZABÓ I., A számítástechnikai adat mint elektronikus bizonyíték – A magyar szabályozás elemzése az Európai Tanács számítástechnikai bűnözésről szóló egyezménye alapján. *Kriminológiai tanulmányok,* 2011. (48. kötet) p. 16.

de számítástechnikai feldolgozásra alkalmas formában megjelenő adat és az ahhoz kapcsolódó személyiségi jogok védelmében a büntetőjogi tényállások jelentik az egyik legkomolyabb szabályozási elemet az adatvédelem összetett rendszerében. Információs alapjog az információszabadság és az adatvédelem. Az információszabadság a közérdekű adatok nyilvánosságához, megismerhetőségéhez való jog, míg az információs önrendelkezési jog,[165] ismertebb megnevezése szerint az adatvédelem a magánszféra adatainak védelméhez való jog. A magánszféra védelme informatikai jogi szempontból a személyes adatok védelmét jelenti, a cél azonban a személyes adat által leírt, tárgyiasult emberi személyiség szabadságának, méltóságának, pontosabban a magánszférának (privacy) védelme, nem pedig magának az adatnak a védelme. Fokozza a személyiség alávetettségét, hogy az informatikai eszközök segítségével könnyen, gyorsan előállítható olyan személyiségprofil, mellyel feltérképezhető az egyén teljes magánélete, így családi állapota, jelen, múltja, következtetni lehet terveire, jövőére, sértve ezzel szabad akaratát, méltóságát, komoly visszaélésekre adva ezzel alapot.[166] Éppen ezért a személyes adatok védelmét garantálni kell minden olyan társadalmi viszonyban, amibe a természetes személy kerülhet, és amely viszonyban a személyére vonatkozó adatok kezelésének lehetősége felmerül.[167] Maga az adatvédelem tehát az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségére vonatkozik.[168] E komplex jogvédelemnek a büntetőjog tehát csak egy kis területét felügyeli, a Btk. 177/A. és 177/B. szakaszaiban büntetendővé tett magatartások speciálisak, kifejezetten a 2011. évi CXII. törvény rendelkezéseinek, előírásainak megsértését rendeli büntetni, ahol a védett jogi tárgy nem az adat és az azt körülvevő rendszer, hanem a Btk-beli elhelyezkedéséből következően a személyi szabadság.

2.2. A szerzői jogot vagy ahhoz kapcsolódó jogot sértő bűncselekmények

A konvergencia hatásaként és kiterjedt elérhetősége miatt az interneten megszerezhető és szerzői jogi oltalom alá eső tartalmakhoz, információkhoz való hozzáférés, a művel felhasználása is számítástechnikai eszközzel történik. E technológiai-társadalmi változások miatt az informatikai bűncselekmények nagyobb körét teszik ki a szerzői jogot vagy ahhoz kapcsolódó jogokat sértő bűncselekmények. A szerzői jogot sértő cselekmények körüli problémahalmaz tárgyalására a következő fejezetekben részletesebben kerül sor.

2.3. Tiltott pornográf felvétellel visszaélés

A tiltott pornográf felvétellel visszaélés külön csoportot képez, figyelemmel arra, hogy a kiskorú személyről készült pornográf felvétel számítástechnikai feldolgozásra alkalmas személyes adatnak minősül ugyan, büntetőjogi tilalmazásánál azonban nem adatvédelmi, mint inkább a kiskorú egészséges szexuális, testi, lelki, erkölcsi fejlődése biztosításának megfontolásai játszottak szerepet. Az internet nyújtotta – vélt – anonimitásnak és a lebukás esélyét minimálisra csökkentő egyéb technikai lehetőségek miatt e bűncselekményi kör is

[165] A kifejezést és az általa jelölt alapjogot a 15/1991. AB határozat vezette be a jogi nyelvbe és vezette le lényegét.
[166] GALÁNTAI Z., E-privacy olvasókönyv. Forrás: http://mek.oszk.hu/04100/04134 [2012-02-19]
[167] BALOGH Zs. Gy., Az információs alapjogokkal kapcsolatos számítógépes bűncselekmények. In. GÁL I. L. & NAGY Z. A. (ed.) *Informatika és büntetőjog*, Pécs, 2006. p. 7.
[168] FARAGÓNÉ HATÓ K., *Adatbiztonság, adatvédelem*, főiskolai jegyzet, Gábor Dénes Főiskola 1999/2000. p. 10.

mindinkább számítástechnikai úton valósul meg, a hagyományos papír- vagy mágnesszalagos (Vhs) adathordozó alapján történő elkövetés régen visszaszorult.

2.4. A számítástechnikai bűncselekmények

Ezek a tényállások és értelmező rendelkezéseik a Btk. gazdasági bűncselekményekről szóló fejezetében találhatóak, mégpedig a 300/C. és 300/E. §-ban. A számítástechnikai bűncselekmények fogalmának meghatározásához olyan közös ismérvet kell találnunk, amely megkülönbözteti őket a többi bűncselekménytől. Első pontként közös sajátosság lehet az elkövetett bűncselekmény tárgya, célja: az informatikai rendszer, a tárolt adat, maga az információ, az információt továbbító kommunikációs rendszer. Másodszor közös lehet a bűncselekmény elkövetési eszköze: a számítógép, illetve az elkövetéshez szükséges speciális ismeretek megléte. Megfelelő gyűjtőfogalom hiányában a nézetek különbözősége abból adódik, hogy egyes szerzők – helyesen – csak a második pontban meghatározott eseteket sorolják a számítógéppel kapcsolatba hozható bűncselekmények közé, míg mások bármelyik csoportnak való megfelelés esetén használják a fogalmat.[169] Ennek alapján már eddig is számos definíció született: Parker, Nycum és Aura megfogalmazása szerint számítógépes bűncselekmény minden olyan törvénysértő cselekedet, amelynek elkövetéséhez, nyomozásához és bírósági vizsgálatához elengedhetetlen a számítástechnika speciális ismerete.[170] Az Amerikai Egyesült Államok igazságügyi kormányzatának *(US Department of Justice)* közel azonos meghatározása szerint számítógépes bűncselekmény *(computer crime)* minden olyan bűncselekmény, amelynek elkövetéséhez nyomozásához és elbírálásához a számítástechnika ismerete szükséges.[171] Ezek a meghatározások bizonyítási-eljárási oldalról közelít tárgyához, azt kell mondanunk, hogy nagyon találóan, bár számos bűncselekmény-típus üldözéséhez kell a jogalkalmazónak speciális ismeretekkel rendelkeznie. A Centre de Droit International Pénal (CDIP) fogalma szerint: informatikai bűncselekmény minden olyan tevékenység vagy mulasztás, amely számítógépes rendszerekbe történő közvetlen vagy közvetett behatolással anyagi vagy szellemi javakban kárt okoz.[172]

A fent soroltakon kívül számos más csoportosítás ismert, azonban célszerűbb a Btk. szerkezetéből kiindulni és a védendő jogi tárgy alapján a számítástechnikai bűncselekmények fogalmát meghatározni. Tekintettel arra, hogy a büntetőjog bűncselekmény-fogalma maga a büntető törvénykönyv tárgyi hatálya, a számítástechnikai bűncselekmény genus proximuma kizárólag a mindenkori bűncselekmény-fogalom lehet. A számítástechnikai bűncselekmények fogalmát a fentebb írtakra figyelemmel nem aszerint kell meghatározni, hogy az adott cselekmények esetében a számítógép eszköz-e vagy cél, illetve az elkövetéshez szükségesek-e speciális ismeretek, hanem a védett jogi tárgyak oldaláról kell kiindulnunk. Emellett szól az is, hogy a Cyber-crime Egyezmény, és az Európai Tanács 2005/222/IB számú kerethatározata is a büntetendővé nyilvánítandó cselekmények által támadott adat és rendszer alapján csoportosítja előírásait és határoz meg alapfogalmakat. A korábbi fejezetben írt elkövetési tárgyra, a számítástechnikai rendszer és adatok alapfenyegetettségeire alapozva a számítástechnikai bűncselekmény fogalma a következő: *az a bűncselekmény, mely a számítástechnikai rendszerek zavartalan működését, a bennük kezelt adatok megbízhatóságához, hitelességéhez, titokban*

[169] GELÁNYI A., A számítógépes bűnözés szabályozásának összehasonlítása a magyar és a svájci jogban. In. GÁL I. L. & NAGY Z. A. (ed.) *Informatika és büntetőjog*, Pécs, 2006. p. 49.
[170] BALOGH Zs., *Jogi informatika*, Dialóg Campus Kiadó Budapest-Pécs, 1998. p. 260.
[171] National Institute of Justice, DOJ, Computer Crime: Criminal Justice Resorurce Manual 2. (1989.)
[172] BALOGH Zs., *Jogi informatika*, Dialóg Campus Kiadó Budapest-Pécs, 1998. p. 260.

maradásához fűződő, illetőleg az ezekhez fűződő egyéb (nemzetbiztonsági, államigazgatási, gazdasági vagy személyes érdeket) sért, vagy veszélyeztet.

2.5. Számítógéppel érintett bűncselekmények *(computer-related crimes)*

E csoportba lehet sorolni valamennyi olyan egyéb bűncselekményt, amelynek megvalósulása jellemzően számítástechnikai eszközök igénybevételével történik – például: az internetes rágalmazás, becsületsértés, vagy a zaklatás egyes elkövetési magatartásai –, de olyan önállósult törvényi tényállások is ide tartozhatnak, mint a „bankkártya-csalás", azaz a készpénz-helyettesítő fizetési eszközzel visszaélés.

IV. FEJEZET: AZ ALKOTMÁNYOS BÜNTETŐJOG

Az „alkotmányos büntetőjog" kifejezést *Szabó András* alkotmánybíró alkotta, tartalmát pedig az Alkotmánybíróság büntetőjogi vonatkozású határozatai töltik ki, ekként az alkotmányos büntetőjog a láthatatlan alkotmány egyik alapelemének tekinthető.[173] Szabó András megállapítása szerint a büntetőjognak alkotmányos büntetőjognak kell lennie. A büntetőjognak az alkotmányból, az alkotmányos értékekből kell kiindulnia, de ezen értékeket nem csak védenie kell, hanem – ahogyan azt a 11/1992. (III. 5.) AB határozatban kifejtette – maga is értékhordozó.

Ádám Antal hangsúlyozza emellett, hogy a társadalmi és egyéb körülmények – mai is tapasztalható – változásai az eszmeáramlatok átalakulásával, az értékek újrarendeződésével járnak, a jogi normákba foglalt értékeknek, a jogrendszert alkotó jogi normáknak azonban ellentmondásmentes értékrendszert kell alkotniuk.[174] *Wiener A. Imre* szerint az alkotmányos büntetőjog koncepciója a jogállamiságból, mint alapértékből eredő, az állami büntetőhatalom gyakorlására háramló következmények rendszere, ezen belül a büntető jogalkotás számára adódó tartalmi korlátok és formai követelmények.[175]

A továbbiakban vizsgálandó kérdésként merül fel, hogy az egyébként kőbe vésett alapokat kereső büntetőjog számára e láthatatlanság mennyire oszlatható el, azaz melyek az alkotmányos büntetőjog Alkotmányból levezetett, de abban nem egyértelműen jelenlévő szilárd bástyái?

A vizsgálódás időszerűségével szemben ésszerű kételyek támaszthatók ugyan, amennyiben a 2011. április 12. napján elfogadott új Alaptörvény 2012. január hó 1. napjával történő hatálybalépése miatt a jövőben egyes alkotmánybírósági határozatok felülvizsgálatára kerülne sor, továbbá azon okból kifolyólag, hogy a jelenleg hatályos Alkotmány alapvető jogokra vonatkozó rendelkezései – jóllehet azonos tartalom mellett – megváltozott fogalmazásban öltenek testet. Ennek ellenére az értekezés célkitűzése aggálytalanul, stabil alapokról érhető el, hiszen a büntetőjog alkotmányos alapelvei expressis verbis sem a hatályos, sem az azt követő Alaptörvényben nem szerepelnek teljes terjedelemben, ha úgy tetszik a „láthatatlan alkotmány" részei jelenleg, és azok lesznek sajnálatos módon a jövőben is. Ugyanakkor, legyen a dolgozatban felhívott alkotmánybírósági határozatok sorsa mégoly bizonytalan is, az alkotmányos büntetőjog alaptételei egy jogállamban nem változhatnak, nem fognak változni. Az alkotmánybírósági határozatokra történő hivatkozás miatt a továbbiakban a volt alkotmány és a hatályos Alaptörvény rendelkezéseit egymással párhuzamosan történő alkalmazása szükséges.

1. A JOGBIZTONSÁG, NORMAVILÁGOSSÁG

A vonatkozó alkotmány-rendelkezések közül elsőként említhetjük a korábbi alkotmány 2. §-t, amely kinyilvánította, hogy a „Magyar Köztársaság független, demokratikus

[173] SZABÓ András többnyire előadó bíróként közreműködve alkotta meg az alkotmányos büntetőjog rendszerét az egyes alkotmánybírósági határozatok meghozatalának vitájában. Álláspontját jelenítik meg a megszületett Ab határozatok indokolásai, az azokhoz írt párhuzamos véleményei, így ezek maradéktalan felsorolása nélkül hivatkozom személyére. A kérdésben született tanulmányai (pl.: Jogállami Forradalom és a büntetőjog alkotmányos legitimitása. Belügyi Szemle 1999/10., Alkotmány és büntetőjog. Jogtudományi Közlöny 1999/4.) ismertetésére terjedelmi okok miatt nem vállalkozom, elfogadva az alkotmányos büntetőjog fogalmának Szabó Andráshoz kötődését.
[174] ÁDÁM A., *Alkotmányi értékek és Alkotmánybíráskodás.* Osiris Kiadó Budapest, 1998. p. 32.
[175] WIENER A. I., Alkotmány és büntetőjog. *Állam és Jogtudomány.* 1995. (37. évf.) 1-2 szám. p. 104.

jogállam". A hatályos Alaptörvény B) cikk (1) bekezdésének rendelkezése szerint „Magyarország független, demokratikus jogállam", így ebben a tekintetben értékelhető változás nem történt. A jogállamiság részeként a jogbiztonság – azon belül is a kiszámíthatóság és az előreláthatóság – elve számos szigorú elvárást támaszt és követel meg a jogalkotótól, amikor az egyes életviszonyok szabályozásának szándékával lép fel.

A 30/1992. (V. 26.) AB határozat alapján az alkotmányos büntetőjog követelményei szerint a büntetőjogi szankció kilátásba helyezésével tilalmazott magatartást leíró diszpozíciónak határozottnak, körülhatároltnak, világosan megfogalmazottnak kell lennie. Alkotmányossági követelmény a védett jogtárgyra és az elkövetési magatartásra vonatkozó törvényhozói akarat világos kifejezésre juttatása, amelynek egyértelmű üzenetet kell tartalmaznia arra vonatkozóan, hogy az egyén mikor követ el büntetőjogilag szankcionált jogsértést, ugyanakkor korlátoznia kell az önkényes jogértelmezés lehetőségét a jogalkalmazók részéről. E körben vizsgálni kell, hogy a Btk. 329/A. § tényállása a büntetendő magatartások körét egyértelműen, határozottan, előre láthatóan jelöli-e ki, amely biztosíték a jogalkalmazói önkénnyel szemben.

A 26/1992. (IV. 30.) AB határozat szerint a világos, érthető és megfelelően értelmezhető normatartalom a normaszöveggel szemben alkotmányos követelmény. A jogbiztonság megköveteli, hogy a jogszabály szövege értelmes és világos, a jogalkalmazás során felismerhető normatartalmat hordozzon.

2. AZ ALAPVETŐ JOGOK KORLÁTOZÁSA

Az alapvető jogok korlátozásának mércéi közül a legszigorúbb próbát az Alkotmánybíróság a 30/1992. (V. 26.) számú határozatában dolgozta ki, amikor a korábbi alkotmány 8. §-ának értelmezése kapcsán hangsúlyozta, hogy az állam akkor nyúlhat az alapjog korlátozásának eszközéhez, ha másik alapvető jog és szabadság védelme vagy érvényesülése, illetve egyéb alkotmányos érték védelme más módon nem érhető el. Az Alaptörvény I. cikkének (3) bekezdése alapján alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható. Az alapjog korlátozásának alkotmányosságához tehát önmagában nem elegendő, hogy az másik alapjog vagy szabadság védelme vagy egyéb alkotmányos cél érdekében történik, hanem szükséges, hogy megfeleljen az arányosság követelményeinek: az elérni kívánt cél fontossága és az ennek érdekében okozott alapjogsérelem súlya megfelelő arányban legyen egymással. A törvényhozó a korlátozás során köteles az adott cél elérésére alkalmas legenyhébb eszközt alkalmazni. Alkotmányellenes a jog tartalmának korlátozása, ha az kényszerítő ok nélkül, önkényesen történik, vagy ha a korlátozás súlya az elérni kívánt célhoz képest aránytalan.

A szükségesség-arányosság teszt elemei[176] közül az első a legitim jogalkotói cél. Az alkotmányosan elfogadható korlátozási indok, illetve a cél és az eszköz logikai kapcsolatának vizsgálatát az Alkotmánybíróság általában a szükségességi elem keretein belül teszi meg. A második elem, a szükségesség nem jelent mást, mint a korlátozás elkerülhetetlenségét, a kényszerítő ok fennállását. Míg a harmadik lépcső az arányosság, amelynél az Alkotmánybíróság a korlátozás és a korlátozással elérni kívánt cél

[176] GÁRDOS-OROSZ F., Alapjogok korlátozása. In: JAKAB A. (ed.), *Az Alkotmány kommentárja I.* Századvég Kiadó Budapest, 2009. pp. 416-427.

fontosságának viszonyát vizsgálja.[177] Az arányosság jelentése szerint az alapjogot a szabályozás kevésbe korlátozza, mint amennyivel növeli egy másik alapjog vagy alkotmányos érték védelmét a jogalkotó.[178] A felsorolt elemek egyenértékűsége okán bármely lépcsőfokon elbukó jogszabály alkotmányellenesnek tekinthető.

Az alapjogok korlátozására vonatkozó vizsgálati mérce főbb vonalai ugyan hamar kialakultak, a részleteket tekintve azonban a mai napig nincs következetes alkotmánybírósági gyakorlat, mivel a teszteket az Alkotmánybíróság kisebb módosításokkal, a különböző alapvető jogok tekintetében koncepcionálisan eltérő szigorúsággal alkalmazza.[179] A korlátozási indokok nem egyenrangúak, mivel minél kevésbé kapcsolódik konkrét alanyi jogok védelméhez a korlátozást megvalósító szabály, annál inkább szorul bizonyításra a szabályozás megalapozottsága.

Az 56/1995. (IX. 15.) AB határozat szerint az arányosságot nem önmagához kell mérni, mércéje mindig a másik alapjog érvényre juttatásához elkerülhetetlenül szükséges korlátozás mértéke, a korlátozás súlyának kell arányosnak lennie a korlátozással elérni kívánt céllal. Az AB mindezt mérlegeléssel tudja eldönteni, amely alkalmas arra, hogy az Alkotmány értelmezője megteremtse az egyensúlyt az egyes alapjogok között, és az egyes alkotmányossági kérdésekben úgy alkalmazza a normákat, hogy az alkotmányos tartalom érvényre jusson.[180] Wiener A. Imre szerint a mérlegelést befolyásolja, hogy az adott cselekmény bűncselekménnyé nyilvánításában létezik-e társadalmi konszenzus, a büntetőjogi felelősség milyen kört érint és ki van ellene, vizsgálni kell a cselekmény morális tartalmát, továbbá szem előtt kell tartani a büntetőjog ultima ratio jellegét, mert a büntetéssel fenyegetettség indokoltságát veszti, amint céljai megvalósítására alkalmatlanná válik.[181]

3. A BÜNTETŐJOG TOVÁBBI ALKOTMÁNYOS ELVEI

Az Alkotmánybíróság 30/1992. AB határozatában a következő, azóta is irányadó álláspontját fejtette ki a büntetőjog jogrendszerben kijelölt helyéről, amely szerepe szerint a jogi felelősségi rendszerben az ultima ratio. A büntetőjog társadalmi rendeltetése, hogy a jogrendszer egészének szankciós zárköve legyen. A büntetőjogi szankció, a büntetés szerepe és rendeltetése a jogi és erkölcsi normák épségének fenntartása akkor, amikor már más jogágak szankciói nem segítenek. Az alkotmányos büntetőjogból fakadó tartalmi követelmény, hogy a törvényhozó a büntetendő magatartások körének meghatározásakor nem járhat el önkényesen. Valamely magatartás büntetendővé nyilvánításának szükségességét szigorú mércével kell megítélni: a különböző életviszonyok, erkölcsi és jogi normák védelmében az emberi jogokat és szabadságokat szükségképpen korlátozó büntetőjogi eszközrendszert csak a feltétlenül szükséges esetben és arányos mértékben indokolt igénybe venni, akkor, ha az alkotmányos vagy az Alkotmányra visszavezethető állami, társadalmi, gazdasági célok, értékek megóvása más módon nem lehetséges.

A jogalkotó feladata, hogy egy cselekmény társadalomra veszélyességének mérlegelése után meghatározza az ellene történő fellépés intézményeit és rendszerét, köztük a büntethetőség feltételeit. E művelet elvégzése során figyelemmel kell lennie az Alkotmánybíróság által fent részletezett szempontokra, azaz vizsgálnia kell, hogy a

[177] GÁRDOS-OROSZ, 2009. p. 421.
[178] GÁRDOS-OROSZ, 2009. p. 425.
[179] GÁRDOS-OROSZ, 2009. p. 417.
[180] GÁRDOS-OROSZ, 2009. pp. 426-427.
[181] WIENER A. I., Alkotmány és büntetőjog. *Állam és Jogtudomány.* 1995. (37. évf.) 1-2 szám. pp. 102-103.

kriminalizáció, mint szükségszerűen alapjogi korlátozás alkotmányos indokokon alapul-e, szükséges, arányos és végső soron igénybevett-e a tényállás megalkotása.

Az 58/1997. (XI. 5.) AB határozat, a 673/B/2004. AB határozat szerint a büntetőjogi felelősségre vonás feltételeinek konkrét meghatározásakor a jogalkotónak kötelessége gondoskodni arról is, hogy a jogi szabályozás a lehető legteljesebb mértékben visszatükrözze a büntető tényállás által védeni kívánt jogi érdek megsértésének rendszeresen megjelenő típusait.

4. A BÜNTETŐPOLITIKA SZEREPE

Az Alkotmánybíróság következetes, így például a 1427/B/1995. számú határozatában kifejtett álláspontja szerint a büntetőpolitika, az egyes bűncselekmények törvényi tényállásának mikénti szabályozása – az Alkotmány keretei között – a jogalkotó hatáskörét képezi. Az Alkotmánybíróságnak nincs jogosítványa a büntetőpolitika által megfogalmazott szükségletek, követelmények és célok helyességéről és indokairól, így különösen azok célszerűségéről és hatékonyságáról határozattal dönteni. Az Alkotmánybíróság csak a normában testet öltött politikai döntés alkotmányosságáról vagy alkotmányellenességéről határozhat. Ezt viszont olyan alkotmányossági vizsgálat keretében cselekszi, amelynek során figyelemmel van nemcsak az alaptörvény textusára, hanem annak normatív és intézményes összefüggéseire, és ugyanígy tekintettel van a Btk. rendelkezéseire és intézményeinek koherenciájára. Az Alkotmánybíróságnak tehát arra van jogosítványa, hogy a büntetőpolitika alkotmányos korlátait állapítsa meg, de ne a politika tartalmáról döntsön, ennek során pedig különös tekintettel legyen az alapjogok védelmének alkotmányos büntetőjogi garanciáira.

A fenti alapelveket kiegészítve az Alkotmánybíróság az 1214/B/1990 határozatában kifejtette, hogy a kriminálpolitika célszerűségi megfontolásai nem sérthetik a büntetőjog alkotmányos elveit és garanciáit. Amikor tehát a kriminálpolitika kriminológiai és büntetőjog-elméleti felismeréseket pusztán célszerűségi megfontolásokból úgy hasznosít a büntetőjogi rendszer normáiban, hogy azok sértik az alkotmányos büntetőjogi elveket és garanciákat, az Alkotmánybíróságnak legitim jogosítványa ezekről döntenie.

Alkotmányossági szempontból következésképpen teljes mértékben irreleváns annak vizsgálata, hogy a kriminalizációt milyen jogpolitikai célkitűzések, szempontok befolyásolták és az is, hogy az állam büntetőpolitikájában az adott tényállás milyen szerepet tölt be.

A jogpolitikai célkitűzésekkel általában ellentétes oldalon felhozott érvekkel – úgymint a büntetőjogi tilalmazás hiányzó morális alapjára hivatkozó dekriminalizációs törekvésekkel – kapcsolatban ugyancsak hangsúlyozni kell, hogy alkotmányossági szempontból ezek sem tehetők a vizsgálódások tárgyává.

5. A RENDSZER EGYSÉGE

Az Alkotmánybíróság a 11/1992. (III. 5.) számú határozatban, majd a 42/1993. (VI. 30.) számú döntésében kifejtette és megismételte, hogy a büntető jogszabályok alkotmányosságát nem csupán az Alkotmányban kifejezetten szereplő büntetőjogi garanciákkal kell mérni, a büntetőjogra számos más alapelv és alapjog is irányadó. A képviselt értékek tekintetében azonban társadalmi konszenzusra van szükség, amely biztosítja egy norma társadalmi befogadását. Ez az egyetértés már hosszú idő óta jelen van

a vagyon elleni bűncselekmények normáiban és dogmatikájában. A büntetőjogi felelősséget és a büntetőjogi felelősségre vonást a büntetőjog olyan intézményének kell tekinteni, amelyet koherens és egymásra utaló büntetőjogi normák egységes szellemben szabályoznak. A koherens szabályozás alkotmányos értelme az állam büntetőjogi önkényének kizárása.

A 769/B/2006. AB határozat szerint a büntetőhatalom gyakorlásának törvényessége nemcsak a nullum crimen sine lege és a nulla poena sine lege klasszikus elvének érvényesülését jelenti. Az alkotmányos büntetőjog magában foglalja a büntetőjogi felelősségre vonás jogszerűségének a büntetési rendszer alakításának törvényességére vonatkozó tartományát is. Az Alkotmánybíróság már a 11/1992. (III. 5.) AB határozatában kifejtette, hogy az egyén alkotmányos szabadságát, emberi jogait nem csak a büntetőjog különös részének tényállásai és büntetési tételei érintik, hanem alapvetően a büntetőjogi felelősség, a büntetéskiszabás és büntethetőség összefüggő zárt szabályrendszere.

Az alkotmányos büntetőjognak tehát egyaránt részét képezik a büntetőeljárási és büntetés-végrehajtási szabályok is. Itt tartom szükségesnek felvetni egy egyelőre nyitottan hagyott kérdést – anélkül, hogy büntetéstani kérdéseket feszegetnék –, amely így hangzik: *mennyire lesz valaha is hatékony egy olyan büntetőjogi norma, amely a következő fejezetekben sorolt érvekre tekintettel nem rendelkezik oly mértékű társadalmi elfogadottsággal, mint rendszerének hasonló elemei, és így a megsértéséért rendelt szankció morális tartalmának hiányától szenved*. Ez a kérdés és a válasz majd a későbbiekben főként a szerzői jogi bűncselekmények elemzésekor kerül újra elő, hiszen a szerzői jogi bűncselekmények legtöbbje csekély tárgyi súlyú, ekként a kiszabható büntetések széles palettájának is csak szűk köre alkalmazott, kisebb prevenciós hatást elérve, mint a büntetőeljárásokban érvényesített polgári jogi igény maga. Mindezek a megfontolások azonban az előző fejezetben írtak ismétlése nélkül alkotmányos büntetőjogi szempontból irrelevánsak.

KÜLÖNÖS RÉSZ

Tartalom:

V. FEJEZET: A SZÁMÍTÁSTECHNIKAI BŰNCSELEKMÉNYEK (BTK. 300/C. §, 300/E. §)

1. A FEJEZET TÁRGYA

A magyar szabályozás jellegzetessége, hogy a jogalkotó két szakaszba, a Btk. 300/C. § valamint a 300/E. § tényállásaiba sűrítette a számítástechnikai bűncselekményeket, és a gazdasági bűncselekményeket tartalmazó fejezetben helyezte el azokat.

A 300/C. § több különböző bűncselekményt foglal magába, Nagy Zoltán szerint tulajdonképpen négyet. [182] Az (1) bekezdés az elektronikus adatfeldolgozó és -továbbító rendszerekhez való illegális hozzáférést, a (2) bekezdés a) pontja az e rendszerekben kezelt adatállomány jogosulatlan „megrongálását", míg a b) pont az e rendszerek működését akadályozó manipulációt rendeli büntetni. A (3) bekezdés, az úgynevezett „számítógépes csalás" utóbbiaknak a haszonszerzés végett történő, kárt okozó elkövetési formája. Tehát – figyelemmel a nemzetközi dokumentumokban is külön-külön meghatározott bűncselekményekre – alapvetően helytelennek minősül az a bűncselekményi elnevezés, amely például az adott cselekményt a Btk. 300/C. § (1) bekezdésébe ütköző, de a (2) bekezdés a) pontja szerint minősülő és büntetendő számítástechnikai adatok elleni bűncselekmény vétségének jelöli.

A számítástechnika mindennapi élet megannyi területén való jelenléte okán a számítástechnikai bűncselekményeket nem kizárólag haszonszerzési célzattal lehet elkövetni, de haszonszerzési cél esetén sem feltétlenül gazdasági indíttatású, gazdálkodás rendjét sértő az elkövetés. A számítástechnikai bűncselekmények helytelen tényállás-szerkesztésének és rendszertani elhelyezésének igazolására valamennyi tényállásban meghatározott bűncselekmény részletes elemzése szükséges.

2. AZ EGYES TÉNYÁLLÁSOK

2.1. A „hacking", avagy a jogosulatlan belépés

A Cyber-crime Egyezmény 2. Cikke alapján az aláíró államnak büntetnie kell a jogosulatlan belépést számítástechnikai rendszerbe a következő szempontokra figyelemmel. Jogosulatlan belépés – némiképp tautologikus meghatározással – a számítástechnikai rendszerbe vagy annak bármely részébe történő jogosulatlan és szándékos belépés. A szerződő fél kikötheti, hogy a bűncselekményt a biztonsági intézkedések megsértésével vagy számítástechnikai adatok megszerzésére irányuló, illetőleg más tisztességtelen céllal, avagy egy másik számítástechnikai rendszerhez kapcsolódó számítástechnikai rendszerre vonatkozóan kövessék el.

Az EU Tanács 2005/222/IB kerethatározatának 2. cikke rendelkezik az információs rendszerekhez való jogsértő hozzáférésről. Ennek alapján minden tagállam meghozza a szükséges intézkedéseket annak érdekében, hogy a valamely információs rendszerhez vagy annak egy részéhez való szándékos jogosulatlan hozzáférés legalább a jelentősebb esetekben bűncselekménynek minősüljön. Minden tagállam határozhat úgy, hogy az említett magatartás csak akkor minősüljön bűncselekménynek, ha azt valamely biztonsági intézkedés megsértése által követték el. A kerethatározat tehát előrébb hozza a behatolásért

[182] NAGY Z., A számítástechnikai rendszer és adatok elleni új bűncselekmények. *Belügyi Szemle* 2002/11-12. p. 30.

megállapítandó felelősséget, hiszen már valamely számítástechnikai rendszerhez való jogellenes hozzáférést is büntetendővé nyilvánít, azaz a bűncselekmény elkövetéséhez nem szükséges valamely számítástechnikai rendszer védelmét kijátszani (pl. jelszót kellett feltörni, belépési kódot megszerezni), nem szükséges a rendszert védelemmel ellátni, elegendő az is, hogyha valaki a nem védett rendszerbe jogosulatlanul belép. Parti Katalin szerint ez a rendelkezés egyrészt az előrehozott felelősségi alakzat miatt nem felel meg a büntetőjog dogmatikai feltételrendszernek, hiszen ha valaki nem kifejezetten vagy nem védett rendszerbe hatol be, nem lehet feltétlenül tudomása arról, hogy cselekménye jogellenes. Másrészt a nem védett rendszerbe való belépés büntetőeljárásbeli bizonyítása, a belépés szándékossága, illetve magának a belépés tényének igazolása technikailag nem védett rendszer esetében nem, vagy csak nehezen megoldható.[183]

A hazai jogrendszerben ennek megfelelően számítástechnikai rendszer jogosulatlan használatának vétségét követi el a Btk. 300/C. § (1) bekezdése szerint, aki számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve, illetőleg azt megsértve bent marad.

Elkövetési magatartás a számítástechnikai rendszerbe történő jogosulatlan behatolás, illetve a belépés jogosultságának kereteit túllépő bennmaradás. Míg az első esetben a belépőnek nincs jogosultsága belépni, létező és működő védelmi intézkedést megszegve lép be, addig a második esetben jogosultan lép be ugyan a védett rendszerbe, de a jogosultság kereteit túllépve bennmarad. Az elkövetés történhet közvetlenül az adatállomány kezelésére szolgáló számítástechnikai rendszeren keresztül vagy közvetetten az azzal kapcsolatban lévő rendszerek közvetítésével, a lényeg, hogy csak akkor tényállásszerű a magatartás, ha az a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével, kijátszásával történik, mert ha a rendszert semmilyen biztonsági megoldás nem óvja, vagy a rendszer védelmi eszköztára nem az elkövetés eredményeként nem működik, akkor nem valósul meg bűncselekmény.[184] A jogosulatlan hozzáférés különös védelem alatt álló adatokat kell, hogy érintsen, azonban mivel a jogszabály nem követeli meg, hogy a védelmet megvalósító biztonsági intézkedések műszaki-technikai jellegűek legyenek, azok elvileg lehetnek akár testi, személyi akadályok is. További ismérv, hogy a védelmi intézkedésnek objektíve és szubjektíve is alkalmasnak kell lennie arra, hogy a jogosult titoktartási akarata felismerhető legyen.[185] A bűncselekmény befejezett, amint a tettes az első hozzáférési korlátot átlépte és számára az adatok vagy az adatfeldolgozó rendszer további lépései nyitva állnak.[186]

A gazdasági motiváció, a haszonszerzési célzat nem feltétele az elkövetésnek, ahogy az sem, hogy a számítástechnikai rendszerben tárolt adaton az elkövető később bármilyen műveletet végezzen, vagy magának a számítástechnikai rendszernek a működését

[183] PARTI K., Az eladók már rég hazamentek. A büntetőjog mint az online pornográfia szabályozásának eszköze. PhD értekezés. p. 235. Forrás: http://doktori-iskola.law.pte.hu/files/tiny_mce/File/Archiv/Parti_Phd.pdf [2012-02-19]

[184] NAGY Z., A számítástechnikai rendszer és adatok elleni új bűncselekmények. *Belügyi Szemle* 2002/11-12. p. 31.

[185] SZABÓ I., Informatikai bűncselekmények. In. TAKÁCS T. (ed.), *Az informatikai jog nagy kézikönyve*, Complex Kiadó Budapest, 2009. p. 607.

[186] GELÁNYI A., A számítógépes bűnözés szabályozásának összehasonlítása a magyar és a svájci jogban. In. GÁL I. L. & NAGY Z. A. (ed.) *Informatika és büntetőjog*, Pécs, 2006. p. 67.

akadályozza.[187] A fordulat alaki bűncselekményt valósít meg, a kísérletnek nincs gyakorlati jelentősége.[188] A jogosulatlan belépés után megvalósított további jogosulatlan műveletek – például adatok törlése – már a következő bekezdés valamelyik fordulatát valósítja meg, amelybe a jogosulatlan belépés vétsége beolvad a súlyosabb jogtárgysértésre figyelemmel.

2.2. A „számítógépes szabotázs"

A Cyber-crime Egyezmény 4. Cikke alapján számítástechnikai adat megsértése a számítástechnikai adatok jogosulatlan és szándékos megkárosítása, törlése, megrongálása, megváltoztatása vagy megsemmisítése. A fél fenntarthatja magának a jogot annak kikötésére, hogy az 1. bekezdésben meghatározott cselekmény eredményeként jelentős kár következzen be. A Cikk tényállása lényegében az informatikai adat meghamisítását, a benne foglalt információ megváltoztatását öleli fel. Az 5. Cikk alapján számítástechnikai rendszer megsértése: számítástechnikai rendszer működésének számítástechnikai adatok bevitelével, továbbításával, megkárosításával, törlésével, megrongálásával, megváltoztatásával vagy megsemmisítésével való jogosulatlan és szándékos, jelentős mértékű akadályozása.

Az EU Tanács 2005/222/IB kerethatározatának 3. cikke rendelkezik a rendszerbe való jogsértő beavatkozásról. Ennek alapján minden tagállam meghozza a szükséges intézkedéseket annak érdekében, hogy valamely információs rendszer működésének számítógépes adatok bevitele, továbbítása, megrongálása, törlése, minőségi rontása, megváltoztatása, elrejtése vagy hozzáférhetetlenné tétele révén történő szándékos és súlyos akadályozása vagy megszakítása, amennyiben azt jogosulatlanul követték el, legalább a jelentősebb esetekben bűncselekménynek minősüljön. Az EU Tanács 2005/222/IB kerethatározatának 4. cikke rendelkezik az adatokba való jogsértő beavatkozásról. Ennek alapján minden tagállam meghozza a szükséges intézkedéseket annak érdekében, hogy a valamely információs rendszer számítógépes adatainak szándékos törlése, megrongálása, minőségi rontása, megváltoztatása, elrejtése vagy hozzáférhetetlenné tétele legalább a jelentősebb esetekben bűncselekménynek minősüljön.

A hazai szabályozásban a számítástechnikai adatok elleni bűncselekmény vétségét[189] az követ el, aki a számítástechnikai rendszerben tárolt, feldolgozott, kezelt vagy továbbított adatot jogosulatlanul megváltoztat, töröl vagy hozzáférhetetlenné tesz. Elkövető bárki lehet, tehát a rendszerbe más esetben jogosultan beavatkozó is. Elkövetési magatartása a számítástechnikai adatok jogosulatlan megváltoztatása, törlése vagy hozzáférhetetlenné tétele.[190] Az adat megváltoztatása az adat tartalmának műszaki úton való változtatása. Az adat törlésével az adat kikerül a rendelkezésre jogosult rendelkezési köréből, szoros értelemben véve megsemmisül, azaz az adathordozóról történő visszaállítása lehetetlen. Az objektív szemlélettel szemben indokoltabb azonban az elkövető tudattartamát előtérbe

[187] A jelszó belépés utáni megváltoztatása viszont már megalapozhatja a (2) bekezdés a) pontjának megállapítását.

[188] BELOVICS E., MOLNÁR G. & SINKU P., *Büntetőjog Különös Rész.* (ed. Szentpétery Petronella) HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2007. p. 561.

[189] A bűncselekmény megnevezésére a Legfőbb Ügyészség által előírt elnevezéseket a szakirodalom jelöléseivel párhuzamosan használom.

[190] Például számítástechnikai rendszer és adatok elleni bűncselekményt valósít meg a főiskola számítástechnikai hálózatának felügyeletét ellátó informatikus, aki a hallgatók vizsgakötelezettségét és vizsgaeredményeit nyilvántartó számítástechnikai rendszerben levő adatok jogosulatlan megváltoztatásával - a vizsgát előírás ellenére nem tett hallgatóval kapcsolatban - olyan adatokat rögzít a rendszerben, amelyek szerint a hallgató a meghatározott tantárgyból eredményes vizsgát tett. (BH2009.264)

helyezni, azaz töröltnek kell tekinteni azt az adatot is, amit csak különleges szakértelem és eljárások eredményeként lehet visszaállítani.[191] A tényállás kommentárja szerint az elkövetési magatartás ez esetben a jogosulatlan, illetve jogtalan programmanipulációval fogalmazható meg, amely jelentheti a védelemben részesített adatok megváltoztatását, amely gyakorlatilag a programutasítások teljes vagy részleges átírását, a program lefutásának megváltoztatását jelenti.

Ezzel, az Egyezmény által meghatározott számítástechnikai adat fogalmából kiinduló értelmezéssel nem lehet teljes mértékben egyetérteni, mivel a számítástechnikai adat és rendszerelemek vizsgálata során a programot az adatot körülölelő rendszer elemeként lehet meghatározni. A programmanipuláció már a (2) bekezdés b) pontjának megvalósítását jelentheti, amennyiben az a rendszer megfelelő működésére is kihatással van. A törvény megfogalmazásából következik, hogy akár egyetlen adat törlésével is befejezett a bűncselekmény. Amennyiben az adaton végzett jogosulatlan művelet a számítástechnikai rendszer működésének akadályozását is eredményezi, akkor a (2) bekezdés b) pontjában meghatározott cselekmény valósul meg.[192]

Számítástechnikai rendszer elleni bűncselekmény vétségét követi el a b) pont alapján az, aki adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését jogosulatlanul akadályozza. Ebben az esetben a védett jogi tárgy a számítástechnikai rendszer hibátlan működése. Elkövetési magatartás az adat bevitele, továbbítása, megváltoztatása, törlése, illetve egyéb olyan művelet végzése, amely a rendszer működését akadályozza. Az akadályozás csak abban az esetben állapítható meg, amennyiben az jelentős az adott rendszer működésének következményeihez viszonyítva, de ide kell érteni azt is, ha a rendszer üzemeltetője az adatfeldolgozás esetén a feladatait a továbbiakban nem, vagy csak jelentős többletráfordítással tudja ellátni.[193] Külön értelmezést igényel az „egyéb művelet" kifejezés, amely önmagában meglehetősen tág fogalom. Ehelyütt mellőzve a tudományos igényű részletességet, egyfajta tautológiával élve a „művelet" jelölheti egyrészt az informatika alapját képező logikai alapműveleteket (igaz/hamis), de az adatokon végezhető valamennyi lehetséges technikai eljárás gyűjtőelnevezéseként is használatos (adatok törlése, többszörözése, továbbítása, stb.). A „művelet" kifejezés egyfajta elektronikus környezetben történő elkövetést sugall, tehát a számítástechnikai rendszer elleni fizikai támadás, rongálás – mégha az az adatok ellen is irányul – érezhetően szétfeszíti a fogalom szemantikai kereteit.

A cselekmény akkor tényállásszerű, ha az elkövetési magatartást jogosulatlanul követi el a beavatkozó. Mivel a „jogosulatlan" jelző a tényállás szövegében az eredményre utal, a cselekményt elkövetheti az is, aki egyébként jogosult a számítástechnikai rendszerbe belépni, ott az adatokon műveleteket végrehajtani, jogosultsága azonban nem terjed ki a rendszer működésének akadályozására. A tényállás eredménye a rendszer működésének akadályozása, így a bűncselekmény rendbelisége is a támadott számítástechnikai rendszerek számától függ.

A gazdasági motiváció, a haszonszerzési célzat nem feltétel ebben az esetben sem, de az elkövetés érinthet több jogtárgyat is egyszerre.[194] Amennyiben a számítástechnikai

[191] SZABÓ, 2009. p. 610.
[192] BELOVICS et al. p. 562.
[193] SZABÓ, 2009. p. 612.
[194] Például, amennyiben az elkövető valamilyen úgynevezett „keylogger" funkciójú kémprogramot telepít a célszemély számítógépére és így jut hozzá a sértett bizonyos adataihoz, majd annak segítségével változtatja

rendszer közérdekű üzemnek is tekinthető, felmerülhet a közérdekű üzem megzavarása bűntettének megállapítása, amely kizárja a Btk. 300/C. § (2) bekezdés b) pontját.

Az a) és b) pontok esetén az ott leírt elkövetési magatartások bármelyikének megkezdésével jut a cselekmény kísérleti szakba, mindez azonban nem azonos az elkövetéshez szükséges eszköznek, tárgynak a bűncselekmény elkövetésére alkalmassá tételével, hiszen ebben az esetben a Btk. 300/E. §-ba ütköző cselekmény valósul meg.[195]

2.3. A „számítógépes csalás"

A Cyber-crime Egyezmény 8. Cikke alapján számítógéppel kapcsolatos csalás a másnak jogosulatlanul és szándékosan történő vagyoni károkozás, amelyet a) számítástechnikai adatok bármilyen bevitelével, megváltoztatásával, törlésével vagy megsemmisítésével; b) a számítástechnikai rendszer működésébe való bármilyen beavatkozással, de mindkét esetben anyagi haszon saját vagy más részére történő jogosulatlan megszerzésének céljából követnek el.

A vagyoni érdekeltséget feltételező elkövetési motívumokat, valamint az elkövetéssel történő károkozást a magyar szabályozás ismét a Btk. 300/C. §-ban helyezte el, mégpedig (3) bekezdésében. Számítástechnikai rendszer működésének haszonszerzés végett történő akadályozását követi el az, aki jogtalan haszonszerzés végett a) a számítástechnikai rendszerbe adatot bevisz, az abban tárolt, feldolgozott, kezelt vagy továbbított adatot megváltoztat, töröl vagy hozzáférhetetlenné tesz, vagy b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését akadályozza, és ezzel kárt okoz.

Az elkövetési magatartások részben megegyeznek a (2) bekezdésben írtakkal, azonban a (3) bekezdés tényállásai az alanyi oldalt tekintve célzatosak, azaz a cselekményeket az elkövető jogtalan haszonszerzés végett követi el. Az elkövető tevékenysége lehet eleve jogosulatlan, de hivatásánál fogva akár jogosultsággal is rendelkezhet valamely magatartás tanúsítására, azonban cselekményét szándékosan nem az engedélyezett eredmény elérése érdekében, hanem jogtalan haszonszerzés céljából követi el. Egy jogosulatlan manipuláció megítélésénél mindig a konkrét számítástechnikai rendszer gazdájának, jogosultjának a nyilatkozata irányadó.[196] A „számítógépes csalás" eredmény-bűncselekmény, azaz a károkozás, illetve a kár bekövetkezte tényállási elemként szerepel. Mindaddig, míg a kár nem következik be, a cselekmény a kísérlet stádiumában marad. A kár meghatározásánál lényeges, hogy az a cselekmény eredményére utal, nem módjára, így a kárnak nem a számítástechnikai rendszerben kell bekövetkeznie, hanem annak manipulációjával összefüggésben, a tevékenység eredményeként. Ez következik abból a megfogalmazásból, hogy nem csupán a károkozást fogalmazza meg a törvény, hanem a kár bekövetkeztét összeköti a jogtalan haszonszerzés célzatával. Önmagában ugyanis a rendszer működésének akadályozásával, adatok törlésével stb. – bár a rendszer működtetője, használója károsodik – az elkövető számára nem keletkezik jogtalan haszon. E tényállásnál tehát azokat a cselekményeket kell figyelembe venni, amelyek az adatfeldolgozási

---

meg a sértett egyes jelszavait, akkor az egyébként megállapítható Btk. 300/E. § beolvad ugyan a 300/C. § (2) vagy (3) bekezdés a) pontjaiba, de a Btk 178/A. §-ba ütköző magántitok jogosulatlan megismerésének bűntette halmazatban megvalósulhat az elkövető célzata függvényében, és amennyiben a tudomására jutott adatokat felhasználja.

[195] TÓTH M., *Gazdasági bűnözés és bűncselekmények.* KJK-KERSZÖV, Budapest, 2002. p. 327.

[196] BELOVICS et al. p. 563.

folyamat befolyásolása következtében károsító vagyoni diszpozíciót eredményeznek.[197] A bűncselekménynek alsó értékhatára nincs, ezért figyelemmel a (4) bekezdés a) pontjára az alapeset kétmillió forint károsszegig állapítható meg.[198]

A biztonsági kockázatok szorosan összefüggnek az informatikai eszközök és rendszerek üzleti értékével, a kár ezért sok esetben könnyen meghatározható, a cloud computing fejlesztési irányzata azonban e kijelentés hosszú távú érvényességét is lassan homályos ködbe borítja.

A gyakorlatban számos esetben felmerül a „számítógépes csalás" és a hagyományos, a Btk. 318. §-ba ütköző csalás elhatárolásának kérdése akkor, ha mindkét bűncselekmény tényállási elemei egyaránt megvalósulni látszanak azaz, ha van jogtalan haszonszerzési célzat, bekövetkezett kár, a számítástechnikai rendszerbe bevitt valótlan adat, de kérdéses a megtévesztés megállapíthatósága.[199] Az elhatárolási ismérv ilyenkor az, hogy a számítástechnikai rendszer az elkövetés, vagy a leplezés eszköze volt-e. Kérdés, hogy az elkövető csak felhasználta-e a számítógépben rejlő lehetőségeket és úgy követett el csalást, hogy azt a számítógép segítségével kívánta eltitkolni, vagy már eleve a csalás elkövetése érdekében manipulálta az adatokat. Szabó Imre szerint ha a tettes a számítógép üzembentartójának okozott kárt adatmanipulációval kívánta eltüntetni, akkor nem jogtalan haszonszerzés végett tanúsította az elkövetési magatartást, hanem a leplezés érdekében. Ha azonban a jogtalan haszon megszerzése, kifizetése érdekében az ahhoz szükséges jogcímet is programmanipulációval teremti meg az elkövető – például valótlan adatok bevitelével számítástechnikai rendszerbe – akkor a számítógépes csalás megállapítása indokolt.[200] A bírósági gyakorlat, ha nem is számítógépes csalás, hanem a Btk. 318. §-a szerinti csalás esetén az elkövető által egyébként megfizetni köteles kár összegének leplezését is csalásnak tekinti, s vele halmazatban állapítja meg a leplező cselekményt, például az okirat-hamisítást. E gondolat mentén, az okozott kár leplezése érdekében elkövetett adatmanipuláció esetén a csalás mellett a Btk. 300/C. § (2) bekezdése állapítható meg halmazatban.

2.4. A rendszer védelmét biztosító technikai intézkedés kijátszása

A 300/E. § tényállása alapján a számítástechnikai rendszer jogosulatlan használatának elősegítése vétségének két fordulata ismert. Az első fordulatot követi el, aki a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából, az ehhez szükséges vagy ezt könnyítő számítástechnikai programot, jelszót, belépési kódot, vagy számítástechnikai rendszerbe való belépést lehetővé tevő adatot a) készít, b) megszerez, c) forgalomba hoz, azzal kereskedik, vagy más módon hozzáférhetővé tesz. Elkövetési tárgya a bűncselekmény elkövetését lehetővé tevő vagy ahhoz szükséges, illetőleg azt megkönnyítő számítástechnikai program, jelszó, belépési kód, vagy a számítástechnikai rendszerbe való belépést lehetővé tevő adat. Elkövetési magatartása a program, jelszó, kód készítése, megszerzése, forgalomba hozatala, hozzáférhetővé tétele, kereskedés. A forgalomba

[197] SZABÓ, 2009. p. 615.
[198] A számítógépes csalás bűntettének alapeseténél a törvény nem állapít meg értékhatárt, így az bármilyen csekély mértékű kár okozása esetén megállapítható. (BH2005.419)
[199] Példaként említhetjük a következő esetet: az elkövetők egy pénznyerő játékautomata pénzadagoló nyílását szabaddá téve egy nagyobb értékű bankót többször húznak át a pénzszámlálón úgy, hogy nem engedik azt beesni a játékautomata kasszájába. Ezzel a művelettel téves, nagyobb értékű pénzösszegnek megfelelő, valótlan adatot visznek be a számítástechnikai rendszer kritériumainak megfelelő felépítéssel rendelkező játékautomatába, majd az összeget nyereményként a szórakozóhely pultosával kifizettetik.
[200] SZABÓ, 2009. pp. 614-615.

hozatal nem azonos az értékesítéssel, vagyis az ellenérték fejében történő elidegenítéssel, hanem annál szélesebb kategória - ide tartozhat nagyobb számú közönség számára történő hozzáférhetővé tétele is (internet). Az elkövetési magatartás jogosulatlan, azonban ezt a törvény szövege közvetlenül nem nyilvánítja ki, viszont abból következően, hogy az elkövetési magatartásokra a Btk. 300/C. §-ban írt bűncselekmények elkövetése céljából kerül sor, egyértelmű, hogy a felsorolt magatartások jogosulatlan tevékenységek. A tényállás sui generis előkészületi jellegű bűncselekmény, bár nem szükséges, hogy elkövetője szándékában álljon később a Btk. 300/C. §-ban megfogalmazott cselekmény elkövetése. Az előkészületi jelleg miatt a 300/C. § valamely tényállásának megvalósítása magába olvasztja az elkövetést.

A második elkövetési magatartás alapján az (1) bekezdés szerint büntetendő, aki a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő, számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszerbe való belépést lehetővé tevő adat készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit másnak a rendelkezésére bocsátja. A bűncselekmény alanya bárki lehet, aki az adott irányú gazdasági, műszaki, szervezési ismeretekkel rendelkezik. Ez azonban nem jelenti azt, hogy a bűncselekményt csak speciális alany követheti el, nem minősül delictum propriumnak, hiszen ezen szakmai ismeretek nem minősülnek olyan személyes kvalifikáltságnak, mely megalapozná a speciális alanyi kört. A cselekmény nem önálló bűncselekmény, hanem a Btk. 300/C. §-ban meghatározott bűncselekmény elkövetése céljából előkészületi és bűnsegédi jellegű magatartás. Az elkövetési magatartás a szükséges ismeretek rendelkezésre bocsátása, amely nem más, mint az (1) bekezdés a) pontjában írt készítéshez nyújtott bűnsegély. Ezzel az egyébként bűnsegédi magatartás nyert önálló tettesi alakzatot. Nem szükséges tehát, hogy az a személy, akinek az elkövető ismereteit rendelkezésre bocsátotta, valóban felhasználja a Btk. 300/E. § (1) szerinti programot, kódot, vagy elkövesse a Btk. 300/C. §-ban írt bűncselekményt. Ennek megfelelően a cselekmény befejezett, ha a készítésre vonatkozó ismeretek átadása megtörtént. Abban az esetben viszont, ha a Btk. 300/C. § szerinti bűncselekmény elkövetése megtörtént, úgy a (2) bekezdés szerinti tettes a Btk. 300/C. § szerinti bűncselekmény bűnsegéde lesz.

A számítástechnikai bűnözés a jelen korban csaknem teljes mértékben az internettel áll kapcsolatban, struktúrája természetesen folyamatosan változik, időnkben egyre inkább előtérbe kerülnek a kis összegre tömegesen elkövetett csalások, az automatizált támadások.[201] Az elkövetési módszerek változása miatt röviden itt tartom indokoltnak szót ejteni a Cyber-crime Egyezmény esetleges kritikájáról. Az Egyezmény jelentős lépést jelent ugyan a jogellenes cselekmények sztenderdizálásában, azonban időközben egyre inkább elterjedtek az olyan új elkövetési technikák, mint például a *cloud computing-ra* vagy a *botnet-re*[202] épülő támadások, amelyek kívánatos kriminalizálására a Cyber-crime

[201] PARTI K., VIRÁG Gy., Beszámoló a Számítógépes bűnözéssel foglalkozó kormányközi munkacsoport (Intergovernmental Expert Group on Cybercrime) üléséről, (Bécs, 2011. január 17-21.) és az ennek kapcsán felmerült kérdésekről. 2. Forrás: Ügyészségi Intranet.

[202] A botnet angol kifejezés, a robot network szókapcsolat összevont rövidítését jelenti. Botnet esetén az elkövetők több, egyéni személyi számítógép feletti irányítást vesznek át és az így szervezett hálózat működését automatikussá teszik, ezzel olyan összehangolt károkozásra képesek, mint egy DDos támadás. A DoS *(Denial of Service)* fogalom magyar megfelelője a szolgáltatás-leállítással vagy szolgátatás-megtagadással járó támadás. A támadás célja a szolgáltatás megbénítása azáltal, hogy a kiszolgáló szervert elárasztják csatlakozási kérelemmel tényleges csatlakozási szándék nélkül. A nagyszámú fals csatlakozási kérelem a hálózat valamely erőforrását annyira igénybe veszi, hogy a szolgáltatás színvonala jelentősen csökken vagy akár teljesen elérhetetlenné válik. A támadás célja nem az illegális hozzáférés hanem az, hogy

Egyezmény előírásai már nem feltétlenül nyújtanak elegendő biztosítékot.[203] Egy példával élve vitatott a botnet hálózatok szervezésének megítélése, hiszen a botnetek nem minden esetben akadályozzák egy számítástechnikai rendszer működését, és nem feltétlenül okoznak kárt, legfeljebb csak igénybe veszik a rendszert, ezért sem az Egyezmény 8., sem az 5. Cikke nem állapítható meg aggálytalanul.[204]Az Egyezmény elsődleges célja az volt, hogy egyfajta kiinduló pontként valamennyi aláíró államban megteremtse vagy egységesítse a számítástechnikai bűncselekmények jogi szabályozását, és a nem kívánatos, társadalomra veszélyes cselekményekre válaszul – figyelemmel a kettős inkrimináció alapelvére – megteremtse a felelősségre vonás alapjait. Mivel a jogosulatlan belépés minden fenti esetben aggálytalanul megállapítható, a cselekmény minősítésének lehetősége adott, az már az egyes aláíró államok jogalkotásán múlik, hogy az egyes elkövetési magatartásokhoz – következményeik függvényében – milyen súlyosabb büntetéssel járó minősített eseteket határoznak meg.

2.5. Egyéb számítástechnikai jellegű tényállások

A Cyber-crime Egyezmény a 3. Cikkben írja elő a jogtalan kifürkészés büntetendővé nyilvánítását, amely szerint büntetendő: a számítástechnikai rendszeren belüli, az abból származó, illetőleg a rendszerbe irányuló számítástechnikai adatok nem nyilvános továbbítása során technikai eszközök felhasználásával történő jogosulatlan és szándékos kifürkészése, ideértve az ilyen adatokat továbbító, a számítástechnikai rendszerből származó elektromágneses sugárzást. A fél kikötheti, hogy a bűncselekményt tisztességtelen céllal vagy egy másik számítástechnikai rendszerhez kapcsolódó számítástechnikai rendszerre vonatkozóan kövessék el.

A hazai szabályozásban a fenti előírások nem külön tényállásban öltenek testet, hanem a levéltitok megsértése és a magántitok jogosulatlan megismerésének bűncselekményi tényállásaiban.

A levéltitok megsértésének vonatkozó alakzatát a Btk. 178. § (1) bekezdése alapján az követi el, aki másnak közlést tartalmazó zárt küldeményét, a tartalmának megismerése végett felbontja, megszerzi, vagy ilyen célból illetéktelen személynek átadja, úgyszintén *aki távközlési berendezés útján továbbított közleményt kifürkész,* ha súlyosabb bűncselekmény nem valósul meg. A távközlési berendezés fogalma – a távközlés folyamatos digitalizációjának korában – mint számítástechnikai rendszer értelmezhető. A bűncselekmény jogi tárgyára figyelemmel a cselekmény a 178. §-ban megfelelő helyre került, a személyi szabadság védelme és az adatvédelem szellemében alkotta meg a jogalkotó ezen tényállást.

A Btk. 178/A. § (1) bekezdés d) pontja alapján a magántitok jogosulatlan megismerése bűntettének a dolgozat szempontjából releváns része a következő: *aki magántitok jogosulatlan megismerése céljából hírközlő berendezés útján, illetőleg számítástechnikai*

---

a megtámadott szerver által biztosított szolgáltatás igénybevétele a felhasználók számára lehetetlenné váljon. A DDoS (*Distributed Denial of Service)* azaz elosztott szolgáltatás-megtagadással járó támadás rövidítése. A DDoS támadások egy összetettebb fajtája, amely a támadón és támadotton kívüli számítógépekben rejlő „erőt", illetve a külső számítógépek nagy mennyiségét hasznosítja a támadáshoz.

[203] PARTI K., VIRÁG Gy., Beszámoló a Számítógépes bűnözéssel foglalkozó kormányközi munkacsoport (Intergovernmental Expert Group on Cybercrime) üléséről, (Bécs, 2011. január 17-21.) és az ennek kapcsán felmerült kérdésekről. p. 4.

[204] PARTI K., VIRÁG Gy., Beszámoló a Számítógépes bűnözéssel foglalkozó kormányközi munkacsoport (Intergovernmental Expert Group on Cybercrime) üléséről, (Bécs, 2011. január 17-21.) és az ennek kapcsán felmerült kérdésekről. p. 4.

rendszeren másnak továbbított közleményt, adatot kifürkész, és az észlelteket technikai eszközzel rögzíti bűntettet követ el. Ennél a tényállásnál egyértelmű, hogy számítástechnikai bűncselekmény elkövetését is büntetni rendeli. A közlemény kifürkészésén minden olyan magatartást érteni kell, melynek célja a közlemény tartalmának jogosulatlan megismerése, úgy hogy másnak a titkát, aprólékos gonddal, figyelemmel keresve azt, felderíti. A bűncselekmény megvalósulásának további feltétele, hogy a magántitok megismerése jogosulatlan legyen. Ez akkor következik be, ha magánszemélyek olyan titkos eszközöket használnak, amelyeket csak a külön törvényekben meghatározott hatóságok, az ott meghatározott célból, engedély alapján alkalmazhatnának. Elkövetési tárgya: a magántitok. Magántitok alatt kell érteni mindazt a csak kevesek előtt ismert tényt, adatot, körülményt – amely lehet személyi, családi, vagyoni helyzetre vonatkozó, illetve eszmei jellegű is – melynek megőrzéséhez a sértettnek méltányolható érdeke fűződik.

Összegezve, ezen tényállások is informatikai bűncselekményeknek tekinthetők, azonban a védett jogi tárgy ezek esetében nem egyszerűen az adat, hanem az Alkotmány rendelkezéseire is figyelemmel a személyi szabadság, a privacy.

3. EGYESÜLT KIRÁLYSÁG: COMPUTER MISUSE ACT 1990

A kontinentális jogrendszerektől távoli, mégis példaértékűnek tekinthető az Egyesült Királyság megoldása a számítástechnikai bűncselekmények tényállásainak kidolgozásában. A számítógépes visszaélésekről szóló törvényt – *Computer Misuse Act*[205] – meglehetősen korán, 1990 augusztusában fogadták el, főképpen a vírustámadások és hacker-tevékenységek üldözése céljából. A törvény első formájában három fő cselekményt rendelt büntetni. Ezek 1) jogosulatlan hozzáférés számítógépes állományhoz (adat, program), 2) jogosulatlan belépés számítógépes rendszerbe súlyosabb bűncselekmény elkövetése, vagy annak megkönnyítése céljából valamint 3) számítógépes állományok jogosulatlan módosítása. A 2006-os *Police and Justice Act*[206] több helyen is módosította a törvényt, így bővítette az első tényállás elkövetési magatartásait egy újabb fordulattal, ugyanakkor megemelte büntetési tételét, valamint kibővítette az eredeti három tényállást további tényállásokkal.[207] A törvényt számos volt brit gyarmati államban vették át kisebb módosításokkal. A CMA 1990. nem tartalmaz minden, a törvényben előforduló alapfogalmat, érdekes módon a tényállások egyik legfontosabb alapfogalmát, a számítógépet (vagy számítástechnikai rendszert) a Cyber-crime Egyezménnyel ellentétben nem tartalmazza, tartalmának kialakítását a gyakorlatra bízza.

A tényállások közül az első szakasz generális tényállásként szabályozza a jogosulatlan belépést:[208] Az (1) bekezdés alapján bűncselekményt követ el, aki számítógép valamely funkcióját jogosulatlanul és szándékosan arra használja, hogy hozzáférjen bármely számítógépen tárolt adathoz, programhoz vagy mindezeket lehetővé tegye. A (2) bekezdés rendelkezései alapján a bűncselekménynek nem kell a) meghatározott adatra, programra, b) meghatározott fajta adatra, programra, vagy c) meghatározott számítógépen tárolt adatra, programra irányulnia. A büntetni célzott magatartás tipikus hacker tevékenység, így például más jelszavának felhasználásával, biztonsági intézkedések kijátszásával lehet

[205] http://www.opsi.gov.uk/acts/acts1990/UKpga_19900018_en_1.htm [2012-02-19]
[206] http://www.opsi.gov.uk/Acts/acts2006/ukpga_20060048_en_1 [2011-07-31]
[207] FAFINSKI, S., Somputer Misuse: the Implications of the Police and Justice Act 2006. *The Journal of Criminal Law* (2008) 72. p. 54.
[208] A tényállások magyar szövege a szerző saját fordítása.

elkövetni, nem szükséges hozzá a számítástechnikai rendszerben tárolt adatnak, programnak a megváltoztatása, nem szükséges a károkozás.

A második szakasz a jogosulatlan belépés további bűncselekmények elkövetésének szándékával vagy ezek megkönnyítése végett. Az (1) bekezdés alapján bűncselekményt követ el, aki jogosulatlan belépést azért követ el, hogy a) e szakasz alá tartozó cselekményt kövessen el, vagy b) ilyen bűncselekmény általa vagy más általi elkövetését elősegítse. A tényállás (2) bekezdése határozza meg utaló jelleggel a célzott bűncselekményeket. A (3) bekezdés alapján nem szükséges, hogy az elkövető a célzott bűncselekményt a jogosulatlan belépéssel egyidejűleg vagy később kövesse el, míg a (4) bekezdés szerint a bűnösséget az is megalapozza, ha a célzott, későbbi bűncselekmény elkövetése lehetetlen. Ez a tényállás gyakorlatilag az előző szakasz kibővítése, azaz megvalósítja a második tényállást, aki az első szakaszban meghatározott jogosulatlan belépést azért valósítja meg, hogy azzal további bűncselekményt kövessen el, azaz előkészületi vagy eszközcselekményként követi azt el.

A harmadik bűncselekmény a számítástechnikai eszközök jogosulatlan módosítása. A *Police and Justice Act 2006.* által bevezetett új tényállások többek között az úgynevezett DoS-támadásokat *(denial-of-service attack)* hivatottak szankcionálni. Ezek olyan cselekmények, amelyek egy számítástechnikai rendszer erőforrásait hozzáférhetetlenné teszik használói számára. Magába foglalja azokat a rosszindulatú törekvéseket, amelyekkel például egy internetes oldal, szolgáltatás működését átmenetileg vagy tartósan akadályozzák. Ennek egyik tipikus módszere, hogy a cél-szervert külső kommunikációs üzenetekkel „bombázzák", telítik, így az nem tud szabályszerűen mindegyikre „felelni", vagy olyan lassan teszi, hogy gyakorlatilag szolgáltatása elérhetetlen. A korábbi, eredeti 1990-es Computer Misuse Act alapján nem voltak büntethetőek ezek a cselekmények, ezért volt szükség a 3. szakasz megváltoztatására. Az új 3. szakasz a következőképpen alakult át. Az (1) bekezdés alapján bűncselekményt követ el, aki a (2) és (3) bekezdés fennállása esetén szándékosan, bármilyen jogosulatlan műveletet végez számítógéppel. A (2) bekezdés alapján az elkövető elkövetéskori szándéka: a) a számítógép működésének akadályozására irányul, b) bármely számítógépen tárolt adathoz vagy programhoz való hozzáférést akadályozza, c) program működését vagy adat megbízhatóságát károsítja, d) mindezek elkövetését lehetővé teszi. A (3) bekezdés alapján az is büntetendő, akit gondatlanság terhel a (2) szakasz a)-d) pontjaiban foglaltak elkövetésében. A (4) bekezdés szerint az elkövető szándékának és a gondatlan elkövetésnek nem kell a) meghatározott számítógépre, b) meghatározott programra, adatra vagy, c) meghatározott típusú programra, adatra irányulnia. Az (5) bekezdés alapján e szakaszban a) az elkövetés magába foglalja a közvetett elkövetést, b) a cselekmények láncolatát, c) az akadályozás, lehetetlenné tétel, elrejtés magába foglalja mindezek átmeneti megvalósulását is. A 3. szakasz tényállásai alapján büntethetők azok a cselekmények, melyekkel az elkövető számítástechnikai rendszerbe belépve adatokat, programokat (állomány) töröl, változtat meg. Az elkövetéshez nem szükséges károkozás vagy jogtalan előny szerzésének célzata.

A *Police and Justice Act 2006.* által bevezetett új tényállás a 3A szakasz alatt található. Ennek címe: A 3. szakasz elkövetéséhez szükséges eszközök előállítása megszerzése, forgalmazása. Az (1) bekezdés alapján bűncselekményt követ el az, aki az előző szakaszok elkövetéséhez, az elkövetés megkönnyítéséhez szükséges eszközt előállít, átalakít, átad, kínál. A (2) bekezdés szerint bűncselekményt követ el, aki ilyen eszközt 1-3. szakaszok elkövetéséhez, vagy valószínűleg való elkövetésükhöz átad vagy kínál, vagy az elkövetéshez segítséget nyújt. A (3) bekezdés alapján bűncselekményt követ el, aki ilyen eszközöket az 1-3 szakaszok elkövetése céljából szerez meg. A (4) bekezdés értelmezése

szerint e szakasz alkalmazásában „eszköz”-nek minősül minden elektronikus formában megjelenő adat, program.

4. EGYESÜLT KIRÁLYSÁG: COMMUNICATION ACT 2003.

Az infokommunikációs infrastruktúra védelmét nem csak a Computer Misuse Act 1993. tényállásai látják el, a kommunikációs szolgáltatások jogosulatlan igénybevételére vonatkozóan egy másik törvény, a 2003-as Comminication Act is tartalmaz deliktumokat.

A Communication Act 2003. 125. § (1) bekezdése alapján kommunikációs szolgáltatás tisztességtelen igénybevételét valósítja meg, aki kommunikációs szolgáltatást úgy vesz igénybe, hogy az adott szolgáltatásra vonatkozó szabályok szerinti ellenszolgáltatás teljesítését elkerülje. A (2) bekezdés a tényállás alóli kivételként állapítja meg Copyright, Designs and Patents Act 1988 (c. 48) 297(1) szakaszában meghatározott cselekményt (dishonestly obtaining a broadcasting or cable programme service provided from a place in the UK). A 126. § (1) és (2) bekezdései büntetni rendelik azt az esetet, ha valaki a 125. § általa vagy más általi elkövetése céljából, az ahhoz szükséges eszközt birtokolja, irányítja, vagy azt másnak átadja, kínálja.

A tényállások révén szankcionálhatók például az idegen kifejezéssel élve *„piggybacking”-nek* és *„wardriving”-nak* nevezett cselekmények, amelyek lényegében a vezeték nélküli internekapcsolat jogosulatla igénybevételét takarják.

5. AMERIKAI EGYESÜLT ÁLLAMOK: THE COMPUTER FRAUD AND ABUSE ACT

Az Amerikai Egyesült Államokban az 1986-os *Computer Fraud and Abuse Act (18. U.S.C. § 1030*, a továbbiakban: CFAA*)* rendeli büntetni a számítástechnikai bűncselekményeket, közöttük a számítógépes csalást. A törvényt 1994-ban és 1996-ban, majd a 2001. szeptember 11-i eseményekre válaszul az *USA Patriot Act*, majd 2008-ban az *Identity Theft Enforcement and Restitution Act* révén többször is jelentősen módosították, többek között új tényállási elemet vezetettek be és egyes fogalmakat részletesebben is meghatároztak.

A CFAA hét speciális tényállást tartalmaz. Valamennyi tényállás megállapíthatósága esetén feltétel, hogy az elkövető szándékosan és jogosulatlanul lépjen be számítástechnikai rendszerbe, vagy a belépéshez jogosultsággal rendelkezik ugyan, azonban jogosultságait olyan lehetőségek kihasználására alkalmazza, amelyekre engedélye már nem terjed ki.[209]

Az első tényállás a jogosulatlan belépést bünteti, amely bűncselekményt az követi el, aki jogosultság nélkül lép be számítástechnikai rendszerbe, vagy jogosultságának kereteit túllépi, és minősített adatot[210] szerez meg, azt jogosulatlan személy számára átadja, továbbítja, vagy mindezek elkövetésében közreműködik, vagy a minősített adatokat visszatartva a jogosultak számára hozzáférhetetlenné teszi.[211]

A második tényállás a jogosulatlan belépést vagy jogosultság kereteinek túllépését követően a pénzintézetek, a szövetségi állam és magántulajdonban lévő rendszerekben tárolt, államközi kereskedelemre vonatkozó adatok megszerzését bünteti.[212] A szakasz

[209] ADAMS, Jo-Ann M.: Controlling Cyberspace: Apllying the Computer Fraud and Abuse Act to the Internet. *Computer & High Technology Law Journal* [Vol.12. 1996.] p. 421.
[210] A minősített adatok a tényállás szempontjából részben utaló szakaszokban vannak meghatározva.
[211] CFAA § 1030 (a) (1)
[212] CFAA § 1030 (a) (2)

lényegében az üzleti titoknak minősülő adatokra elkövetett gazdasági kémkedést *(economic espionage)* szankcionálja.[213]

A harmadik tényállás az első tényállás szerinti jogosulatlan belépést rendeli büntetni a szövetségi állam tulajdonában és használatában lévő számítástechnikai rendszereket érintő cselekmények esetén.[214]

A negyedik tényállás az első tényállás szerinti jogosulatlan belépést rendeli büntetni, amennyiben az csalárd - haszonszerzési - szándékkal történik, azonban ez alól van egy kivétel, mégpedig a gépidőlopás esete, ha az egy éven belül 5000 $ kárt nem okoz.[215] A haszonszerzési célzat ebben az esetben nem feltétlenül anyagi jellegű érdekeltséget jelent, a tényállásban szereplő „*obtain anything of value"* kifejezés alapján az adatok megtekintésén túlmenő, többlet előnyt jelent.[216] A gépidőlopás az egyébként térítés ellenében igénybe vehető erőforrások jogtalan használatával megvalósított jogtalan belépés, amely esetben a haszonszerzés például a gépidő használati díjának „megspórolásában", vagy magában az erőforrások használatában jelentkezik.

Az ötödik tényállás lényegében kettő bűncselekményi alakzatot határoz meg attól függően, hogy károkozásra irányul-e az elkövető cselekménye. Az első fordulatot az követi el, aki valamely védett számítástechnikai rendszerben valamely program, információ, kód vagy parancs bevitelével kárt okoz, függetlenül attól, hogy a számítástechnikai rendszerbe való belépéshez jogosultsággal rendelkezik-e vagy sem.[217] A második fordulat szerint büntetendő az, aki a számítástechnikai rendszerbe, haszonszerzési vagy károkozási célzat nélkül történt jogosulatlan belépéssel okoz szándékán kívül kárt.[218] A kár a tényállás szempontjából az adat, program, rendszer vagy információ teljességének, integritásának, elérhetőségének károsodását jelenti.[219] Jelen esetben a kár fogalma terminológiailag nem azonos sem az amerikai, sem a magyar Btk. kárfogalmával, pusztán az adatok károsodását jelenti.

A cselekmények másként minősülnek, amennyiben a számítástechnikai rendszerben keletkező kár valamelyik kormányszerv, az igazságszolgáltatás, nemzetvédelem, nemzetbiztonság rendszereit érintik. A törvény tehát a stratégiai fontosságú informatikai rendszerek elleni támadást a terrorizmus fogalma alá tartozónak tekinti, és nyilvánvalóan szigorúbban rendeli büntetni.[220]

A hatodik tényállás a számítástechnikai rendszerekbe való belépést lehetővé tevő jelszavakkal való haszonszerzési (csalási) szándékkal történő kereskedést tiltja.[221] A jogosulatlan belépést lehetővé tevő jelszóval való kereskedelem a kormányzati számítástechnikai rendszereket vagy az államközi illetve külkereskedelmet érinti.[222]

---

[213] DOYLE, C., Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statue and Related Federal Criminal Laws. Congressional Research Service report for Congress 2010. p. 31.
[214] CFAA § 1030 (a) (3)
[215] CFAA § 1030 (a) (4)
[216] Computer Crimes - American Criminal Law Review [Vol. 45:233 2008.] p. 250.
[217] CFAA § 1030 (a) (5) (A) (I)
[218] CFAA § 1030 (a) (5) (A) (II)-(III)
[219] CFAA § 1030 (e) (8)
[220] PODGOR, E. S., Computer Crimes and the USA PATRIOT Act. *Criminal Justice*, 2002. Summer. p. 63.
[221] CFAA § 1030 (a) (6)
[222] Computer Crimes - American Criminal Law Review [Vol. 45:233 2008.] 250.

A törvény a módosítások következtében extraterritoriális hatállyal is rendelkezik, mivel az ún. állami, szövetségi, nemzetbiztonsági érdekek miatt védett számítógépek *(protected computer)* esetén az Egyesült Államokon kívüli lévő számítógépek, szerverek esetében is alkalmazható.[223]

A törvény nem tartalmazza sem a belépés *(access)*, sem a jogosultság *(authorization)* fogalmát, de meghatározza a kár és a veszteség tartalmát *(demages, loss)*. A kár *(demages)* négy körülmény esetén állapítható meg: 5000 $ anyagi kár egy évben, fizikai sérülés, közegészség, közbiztonság elleni fenyegetés. Veszteségnek *(loss)* tekinthető minden olyan költség, amely a károk megtérítése, enyhítése kapcsán felmerül.[224] A kár fogalma tehát más eseteket ölel fel, mint a Btk. „kár" és „vagyoni hátrány" fogalmai, inkább a hazai polgári jogi kár-fogalommal mutat rokon vonásokat.

A CFAA tényállásainak szellemiségét tekintve megállapítható, hogy a jogalkotói szándék egyaránt figyelembe vette a számítástechnikai rendszerek nemzetbiztonsági és kereskedelmi szempontú támadásait is. Jóllehet az USA szövetségi és állami szintű jogalkotásának sajátosságai is tetten érhetők a jogszabályban, az azonban világosan kitűnik, hogy a törvény a számítástechnikai bűncselekmények problémakörét komplexen, átfogóan, egy rendszerbe illesztve igyekezett kezelni.

6. A SZABÁLYOZÁS ÉRTÉKELÉSE

A számítástechnikai tényállások értelmezéséhez alapvetően a bűncselekményi tényállás elhelyezkedése szolgált elsődleges vezérfonálként. A Büntető Törvénykönyv fejezetei a bűncselekmények jogi tárgyait veszik alapul, a hasonló társadalmi értéket sértő vagy veszélyeztetető magatartásokat szankcionáló tényállásokat gyűjtve össze. Az egyes fejezeteknek azonban nemcsak anyagi jogi jogértelmezési funkciója lehet, hanem eljárásjogi vonatkozásai is vannak, amikor a Be. különleges illetékességi okként meghatározott szervek kizárólagos feladatává teszi egy-egy fejezetben található bűncselekményekkel szembeni eljárás lefolytatását.[225] Mindez komoly kihatással lehet a nyomozás, ügyészi nyomozás-felügyelet, és az ítélkezés megfelelő működésére olyképpen, hogy nemcsak jogértelmezési ellentmondásba keveredhet a jogalkalmazó, amikor a számítástechnikai bűncselekményekkel találja szemben magát, hanem az egyes székhely-szervekre adott esetben felesleges többletterhet ró a téves rendszertani elhelyezés.

A többfajta tartalmat rögzítő és ekként többféle érdeket megtestesítő adatot és az azt körülvevő rendszert támadó cselekmények nem kizárólag gazdasági, vagy haszonszerzési indíttatásúak lehetnek. A mindennapi élet valamennyi területén, a konvergencia hatásaként általánosan elterjedt a számítástechnikai adattömeg kezelése, feldolgozása, amely ma már számos különböző értékű vagy fontosságú társadalmi viszonyra van kihatással, és amelyekkel szemben a tényállás nem kellően differenciált, mondhatni teljesen „érzéketlen". A tartós népszerűségnek örvendő közösségi oldalak felhasználói profiljainak „feltörése", azok módosítása éppúgy számítástechnikai bűncselekményt valósíthat meg, mint egy játéktermi nyerőgép működését megzavaró beavatkozás. A kisebb társadalmi súlyú problémák mellett a nemzetgazdaság számára jelentős gazdasági szervezetek, az állami szervek, a hatóságok egymás közötti vagy az állampolgárokkal, ügyfelekkel

[223] PODGOR, 2002. p. 63.
[224] PODGOR, 2002. p. 63.
[225] Mivel a Btk. 300/C. § a Btk. gazdasági bűncselekményekről szóló XVII. Fejezetében található, a Be. 17. § és a Be. 30. § rendelkezései alapján a büntetőeljárás lefolytatására a megyei bíróság székhelyén lévő helyi bíróságok – és az azok mellett működő helyi ügyészségek – jogosultak.

folytatott kommunikációja során a biztonságos, hiteles adatáramlás garantálása a gazdasági érdekeken túlmutatva nemzetbiztonsági szempontból is komoly jelentőséggel bír.[226] Ennek okán egyre több állam jogrendszerében találhatók meg a nemzetvédelmi szempontból stratégiai fontosságú informatikai hálózatok védelmét szolgáló jogszabályok (például az *USA Patriot Act* az Egyesült Államokban), amelyek 2001. szeptember 11. után az internetszolgáltatók adatmegőrzési és szolgáltatási kötelezettségének szigorításával (állami érdekeket szem előtt tartó előírásokkal) egyes szabadságjogok sérelmével együtt járó monitoring rendszerek kialakítását tették lehetővé.[227] A sérthető társadalmi érdekek palettája tehát meglehetősen széles, az állampolgár személyi vagy nehezen forintosítható vagyoni érdekeltségétől elindulva a nemzetgazdaság egészének felbecsülhetetlen értékéig terjedhet. A magyar büntető törvényben azonban még nincs biztosítva a kritikus informatikai infratruktúra árnyaltabb védelme, a közérdekű üzem működésének megzavarása vagy az állam elleni bűncselekmények fejezetében található rombolás tényállása nem feltételenül elegendő.

Az európai jogfejlődés egy másik irányát az Egyesült Királyság külön törvénykönyve jelenti, amely egységesen, összefoglalva szabályozza ezeket a bűncselekményeket, elvonatkoztatva a konkrét társadalmi viszonyoktól. Az *1990. Computer Misuse Act* megoldása követendő példának tekinthető, tényállásai egyértelművé teszik, hogy mit értenek az Egyesült Királyságban számítástechnikai bűncselekmények alatt, nem okoznak a magyar szabályozáshoz hasonló jogértelmezési zavarokat. Hasonlóképpen jellemezhetjük a *Computer Fraud and Abuse Act* rendszerét is.

Éppen ezért az önálló dogmatikai alap felépítése, a jogértelmezés segítése és a Btk. rendszertani felépítésének való megfelelés miatt érdemes fontolóra venni a lehetséges társadalmi érdekeket megtestesítő minősített esetekkel kiegészített tényállásokat összegyűjtve a Btk. önálló, számítástechnikai bűncselekményeket magába foglaló fejezetének megalkotását.

A Btk. 300/C. § tényállásainak alkotmányossági szempontú vizsgálata az arányosság feltételének való megfelelés körül járható be. Az információs társadalom technológia-szemléletű elemzése alapján megállapítható volt, hogy az emberi környezet egyre több elemében található számítástechnikai rendszernek, rendszerelemnek tekinthető eszköz, amit a mindennapi életvitel során számos esetben használunk (például: fedélzeti számítógéppel ellátott gépjármű, multifunkciós mobiltelefon, internetes közösségi oldalak, számítógép a napi munkavégzéshez, adattároláshoz, stb). A minket körülvevő eszköz-környzet büntetőjogi védelmének első vonala, az önvédelem. Mivel az adat által hordozott információ vagyoni értékkel is bír, így megőrzésére a kormányzati „nyílt rendszer" elvének[228] érvényesítése kapcsán minden érintett szervezet vagy szerv (legyen az államigazgatási vagy gazdálkodó jellegű) elsősorban maga köteles megteremteni a

[226] A „kiber-terrorizmus" először Észtország példáján mutatta meg technika-függőségünket 2007 áprilisában és májusában. Ez az egész nemzetgazdaságot érintő online támadást feltehetően orosz szerverekről intézték az észt internet és az ahhoz kapcsolódó számítógépes hálózatok ellen. A bankok, kormányzati szervek, a média lebénult, több napba telt, mire sikerült kiküszöbölni a több millió eurós kárt okozó támadást. A probléma természetesen nem maradt meg az észt államhatárok között, hiszen a támadás a NATO-szerződést is érintve nemzetközi fellépést is indokolttá tett. A támadást követően létrehozták a Nemzeti Cyber-Védelmi Központot (Cooperative Cyber Defence Centre of Excellence) (http://www.ccdcoe.org/) [2011-07-31]

[227] PODGOR, 2002. p. 61.

[228] 1039/1993. (V.21.) Korm. határozat, amelyet a közelmúltban az 1119/2010. (V. 13.) Korm határozat helyezett hatályon kívül.

védelem feltételeit. Elvárt tehát, hogy számítástechnikai rendszereinket – amelyek felett e tekintetben rendelkezhetünk – valamilyen védelmet szolgáló biztonsági intézkedéssel biztosítsuk. Ezen tényállási elem minden lehetséges számítástechnikai rendszer elleni támadás esetében nélkülözhetetlen a tényállásszerűség megállapítása szempontjából, ekként a kriminalizáció formálisan arányosnak tekinthető.

Az arányosság kérdése inkább abból a tartalmi aspektusból merül fel, hogy az (1) bekezdés esetében a büntetőjogi védelem kizárólag a védelmi intézkedés kijátszására és a rendszerbe történő belépésre vonatkozik, a számítástechnikai rendszer jellege, az ott tárolt adatok értéke, minősége külön értékelést nem nyer. Egy példával élve: egy közösségi oldal (pl.: iwiw, Facebook, Myvip) felhasználói profiljába történő jogosulatlan belépés a jelszó megszerzésével, vagy feltörésével ugyanolyan elbírálás alá esik, mint egy gazdálkodó társaság rendszerének feltörése és onnan a vagyoni értéket képviselő adatoknak a kimásolása, noha utóbbi akár jelentősebb károkozással is járhat, mint egy súlyosabban büntetendő számítógépes csalás (Btk 300/C. § (3) bekezdés). A jogalkotó tehát figyelmen kívül hagyva az információtechnikai eszközök elterjedése miatt megjelent számos új társadalmi érdeket, jogi tárgyat, kellő differenciálás nélkül, meglehetősen szélesen határozta meg az eltérő társadalomra veszélyességgel bíró cselekmények büntethetőségének feltételeit.

Egy másik oldalról megközelítve a problémát, egy nem védett számítástechnikai rendszerbe történő belépés (például vezeték nélküli internetes kapcsolat felkutatása és használata során tiltott pornográf felvételek letöltése és emiatt indított büntetőeljárás) is eredményezhet olyan jogsérelmet, amely büntetőjogi védelemre tarthat igényt. Mindezek összevetése révén a tényállás nem kellően „érzékeny” a lehetséges jogtárgysértésekre, a technikai eszközökkel telített környezet miatt a szabályozásnak a közeljövőben ki kell terjednie a megfelelő szabálysértési alakzatok és újabb bűncselekményi tényállások (az erőforrások védelme érdekében a „gépidőlopás”, az információk differenciáltabb védelme érdekében az „adatlopás”) megalkotására is.

Alkotmányossági követelmény továbbá a védett jogtárgyra és az elkövetési magatartásra vonatkozó törvényhozói akarat világos kifejezésre juttatása. A tényállások kodifikálási technikájából és rendszertani elhelyezéséből lényegesen eltérő jogalkalmazói döntések születhetnek, amennyiben a Btk. 300/C. § tényállásait kizárólag gazdasági jellegű bűncselekménynek tekintjük.

Szintén a jogbiztonság szempontjából felmerülő kérdés, hogy a Btk. 300/C. § (2) és (3) bekezdésének értelmezése szempontjából az „egyéb művelet végzése” mint elkövetési magatartás kellően pontos normatartalmat hordoz-e. Bár a jogalkotó több tényállásban alkalmazta az „egyéb módon” kifejezést, jelen esetben mégis aggályos, mert olyan nyitott tényállást eredményez, amelynél a számítástechnikai rendszer működését hátrányosan befolyásoló valamennyi – a művelet szóból kiindulva – informatikai tevékenység tényállásszerű elkövetési magatartás lehet az adat felvételétől annak megsemmisüléséig, amely végső soron nyitott törvényi tényállássá alakítja a deiktumot.

A jogbiztonság vonatkozásában további problémát jelent egy-egy informatikai jelenség büntetőjogi fogalmakkal történő megragadása. Az adat megsemmisülése, törlése is új értelmet nyerhet az internet infrastruktúrájának fejlődése miatt, lévén hogy egy adat – annak továbbítása, tárolása során – több állomásokon (cache, proxy) kerülhet rögzítésre, több helyen hagyhat nyomot, önmagáról töredéket, vagy önmaga másolatát, a virtualizáció kiteljesedésének hatására pedig egy adott helyen történt adattörlés esetén az adat más

forrásokból olykor visszaállítható. Ekként az adat törlésének büntetőjogi értelemben szigorú, kiterjesztő értelmezést kerülő meghatározása a jövőben még nehezebb lesz, figyelemmel a rendszer adott időben, adott állapota szerinti meghatározhatóságára is. Mindez egyúttal felveti a többi, ma még kezelhető informatikai fogalom jövőbeli büntetőjogi alkalmazhatóságának kérdését is.

VI. FEJEZET: SZERZŐI JOGI BŰNCSELEKMÉNYEK (BTK. 329/A. §)

1. A FEJEZET TÁRGYA

A legtöbb büntetőjogi jogalkalmazó rendszeresen találkozik a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének valamely bűncselekményi alakzatával és ekkor – a bizonyítás, az elkövetési érték meghatározásának, a rendbeliség megállapításának nehézségei mellett – alkalmanként eszébe jut a következő gondolat: ez az elkövető éppen én is lehetnék. A vagyon elleni bűncselekmények komplex, hosszú idő alatt kiérlelt dogmatikájával szemben a szerzői jogi bűncselekmények környezetének megértése még számos kihívást tartogat az alkotmányos büntetőjog értékrendjét magukénak valló jogászok számára. Vajon a Btk. 329/A. §-a maradéktalanul megfelel az alkotmányossági elvárásoknak?

A fejezet másik tárgya az infokommunikációs konvergencia miatt összetett szerzői jogi szabályozás és a büntetőjogi dogmatika találkozásában született anomáliák bemutatása és feloldása. Ennek során a cél továbbra is annak igazolása, hogy a büntetőjogi dogmatika nem minden esetben képes kezelni az információs társadalom szülte, megváltozott jogi helyzeteket. A jogalkotó által meghatározott szabályok alkalmazása pedig felveti a már az ókori római jogtudományban megfogalmazott felismerést: *summum ius summa iniuria*, azaz a jog maradéktalan és következetes alkalmazása esetenként akár már jogtalanságot is eredményezhet. Hogyan alakul a szerzői jogi tényállás esetén a cselekmény rendbelisége, kik a bűncselekmények sértettjei, és milyen bizonyítási problémákkal találkozhat a jogalkalmazó? Mindezekre a kérdésekre keresem a választ a fejezetben.

Mielőtt azonban mélyebben elmerülnék az egyes részproblémák elemzésében szükségesnek tartom leszögezni azt, hogy a dolgozat a szerzői jog komplex szabályozása és az értekezés informatikai ihletettsége miatt kizárólag a Btk. 329/A.§ és a 329/B. §-ok vizsgálatára szorítkozik, mégpedig a leggyakoribb elkövetési magatartásokra, a zenei- és filmalkotások jogellenes felhasználására figyelemmel. Ekként nem tárgya a dolgozatnak például a bitorlás bűncselekménye, de a szerzői joghoz tartozó védjegyek szabályozása sem.

2. A PROBLÉMÁK MEGFOGALMAZÁSA

2.1. Alkotmányossági deficit

Az alsó értékhatár hiánya. Alkotmányossági szempontból elgondolkodtató kérdéskört vet fel a Btk. szerzői jogi tényállásának alapesete, amely – már nem kizárólag a jogásztársadalom, hanem a laikusok számára is egyre inkább egyértelműen – aránytalanul széles körben öleli fel a büntetendő cselekmények körét. A fejezet célja annak bizonyítása, hogy a Btk. 329/A. §-a jelen formájában a magyar jogrendszer alkotmányos elveibe és értékeibe ütközik. A bűncselekmény alapesete, a Btk. 329/A. § (1) bekezdésének rendelkezései alapján 1.- Ft-tól 2.000.000.- Ft-ig terjedő elkövetési érték (vagyoni hátrány) esetén állapítható meg. Sem a szabálysértésekről szóló 1999. évi LXIX. törvény, sem az egyes szabálysértésekről szóló 218/1999. (XII. 28.) Kormányrendelet nem határoz meg tényállást a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésére, azaz a szerzői vagy szerzői joghoz kapcsolódó jogokat sértő jogellenes cselekmények szabálysértési alakzattal nem rendelkeznek. Ezzel szemben a nem erőszakos jellegű vagyon elleni bűncselekmények mindegyike rendelkezik alsó büntethetőségi értékhatárral. A Btk. 329/A. §-ában meghatározott tényállás tehát a megvalósítható jogsértések tárgyi súlyára,

társadalmi veszélyességére tekintet nélkül, a kellő differenciálást mellőzve minősíti bűncselekménnyé a szerzői jogi törvénybe ütköző valamennyi, haszonszerzési célzatú vagy vagyoni hátrányt okozó magatartást a jelentős érték határáig.

Az elkövetési érték bizonytalansága. Az egyik további, a tényállás keretjellegből és a szerzői jog meglehetősen komplex rendszeréből fakadó gócpont az elkövetési érték meghatározása, hiszen a legtöbb jogsértés abban jelentkezik, hogy a jogsértő személy elmulasztja megfizetni a mű felhasználásáért járó díjat. Tipikus esetben – a zenei alkotások többszörözése vagy nyilvános előadása esetén – a közös jogkezelők jogdíjközleménye alapján, de a felhasználó döntése szerint sor kerülhet egyfelől tételes jogdíjfizetésre vagy úgynevezett átalánydíjas jogdíjfizetésre is. A két módon kiszámított jogdíj és ekként az elkövetési érték nagyobb számú jogsértően felhasznált mű esetén jelentősen eltérő összegekhez vezethet, amely helyzet jogalkalmazói feloldására az in dubio pro reo elve, és ezzel a terheltre kedvezőbb összeg elfogadása lehetőségként fennáll. Az átalány díjtétel alkalmazása azonban maximalizálja az elkövetési értéket, amely a tipikus elkövetések esetén feleslegessé teszi a tényállás és ekként a felelősségre vonás differenciálását. Alkotmányossági problémát az a körülmény vet fel, hogy a tényállás az elkövetési érték két, eltérő eredményre vezető módjának alkalmazását – ekként a jogalkalmazói önkény lehetőségét, és az egyéni felelősség értékelhetetlenségét – teszi lehetővé, ezzel sérti a normavilágosság, a jogbiztonság elvét.

A büntetőjogi és polgári jogi felelősség összemosása. Gyakorlati, alkotmányossági szempontból mégis releváns problémát jelent az a további körülmény, hogy a jogalkotó a Btk. 329/A. § keretténállásának megalkotásakor büntetőjogilag értékelhető többlet tényállási elemet, vagy értelmező rendelkezést nem határozott meg. A nehézséget az okozza, hogy a büntetőjogi felelősség a keretténállás-jelleg okán szinte megegyezik a polgári jogi felelősség jogellenességi elemével. Egyszerűbben fogalmazva, aki a jogosult szerzői jogi törvényben meghatározott jogát szándékosan megsérti, mind büntetőjogi, mind polgári jogi tekintetben jogsértést követ el.[229] E problémakörben jelentős szerepet játszik az a további körülmény, hogy a közös jogkezelő törvénynek nem minősülő jogdíjközleménye a szerzői jogi törvény mellé – egyes esetekben helyébe – lépve tölti ki a Btk. 329/A. §-ának kereteit, amikor meghatározza a jogdíjfizetés módját és elmulasztásának egyes következményeit. Egy példát említve a MAHASZ a hangfelvételek nem kereskedelmi forgalomba hozatal céljából történő többszörözéséért fizetendő hangfelvétel előállítói jogdíjakat és e felhasználások egyéb feltételeit szintén aktuális jogdíjközleményeiben határozza meg. Az átalánydíjas jogosítás esetén egy adott időszakban bármennyi zeneszámot lehet többszörözni, az átalánydíjat pedig időszakonként előre kell megfizetni. A jogdíjközlemény szerint a díjfizetés elmulasztása (a 15 napon túli késedelembe esés) a korábbi időszak többszörözéseit – kivéve a darabonkénti díjfizetés esetét – is jogosulatlanná teszi, ezért a MAHASZ álláspontja szerint a Btk. 329/A. § (1) bekezdése is megvalósul.

2.2. A tényállás büntetőjogi dogmatikai kezelhetetlensége

A Btk. 329/A. §-ba foglalt bűncselekmény rendbeliségének megállapítására vonatkozóan egyidejűleg több eltérő érvelés él a bírósági és ügyészségi gyakorlatban, ezt felismerve a fejezet ezen egymásnak ellentmondó, gyakran nem következetes elméleteket veszi sorra.

[229] A haszonszerzési célzat és a vagyoni hátrány okozása nem tekinthető a tényállás értelmezése során hangsúlyosnak, hiszen a szerző vagyoni jogait sértő cselekmények minden esetben vagyoni hátrány okozásával vagy haszonszerzési célzattal történnek.

Az egyik teória szerint az egyes szerzői művek felhasználásának engedélyezése és a jogdíjfizetés a közös jogkezelő szervezeteken keresztül történik, ezért a bűncselekmény rendbelisége is ezen jogkezelőkhöz igazodik. Ezen álláspont alapja az, hogy általában a közös jogkezelők aktusa helyezi a felhasználót – az egyes felhasználásokhoz szükséges engedélyeket átalány vagy darabonkénti díjazás ellenében kiadva – a szerzői jogi törvénynek megfelelő jogosítotti helyzetbe, ezért a Btk. 329/A. § megsértése ehhez igazodva, jogkezelőnként egy rendbeli – folytatólagosan elkövetett – bűncselekmény megállapítását indokolja. A másik gyakorlat szerint a szerződéssel átruházott jogok esetén az utolsó jogosult tekinthető kiemelt sértettnek, ezért a cselekmény rendbelisége is hozzá idomul. A vagyon elleni bűncselekmények dogmatikájából kiindulva azonban azon harmadik érvelés érezhető a legerősebbnek, amely a bűncselekmény rendbeliségét a sértettek számához igazítja. Utóbbi esetben a szerzői és szomszédos jogok megsértésének nyomozását nagymértékben megnehezítheti, hogy egy elkövetési tárgy kapcsán több sértett is lehet (például hangfelvételek esetén, ahol egyetlen felvételen 12-14 mű, művenként két-három zeneszerző, szövegíró, zeneműkiadó érdekelt lehet, és a felvételen több előadóművész szerepelhet), ezért a vagyoni hátrányt mindegyikükre meg kell határozni.[230]

A dogmatikailag helyes megoldás kidolgozásához meg kell vizsgálni a szerzői jogi jogviszonyokat, tisztázni kell, hogy a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének kik a sértettjei, mi a bűncselekmény jogi tárgya. Ennek elemzése során szükségszerűen kitérek a közös jogkezelő szervezetek büntetőeljárásban való fellépésének lehetséges formájára is, górcső alá véve a jogalkalmazói gyakorlat erre irányuló megállapításait.

3. AZ ALKOTMÁNYOSSÁGI KÉRDÉSEK

3.1. A szabályozási rendszer

A szerzői joggal kapcsolatos jogszabályok által szabályozott jogterület a jogrendszer egészén végighúzódik, éppen ezért a szabályozás rendszerének átfogó, rövid bemutatása nem mellőzhető. Mindez szükséges annak vizsgálata érdekében is, hogy a szabályozás minden eleme megfelel-e a szerzői jog céljának, és az egyes jogágaknak szánt szerepeknek. Csak ezután vehető bírálat alá az egyes rendszerelemek működésének anomáliái, megalapozva ezzel a szabályozás hibás voltának bizonyítását.

3.1.1. Az Alkotmány szintje

Egy cselekmény bűncselekménnyé nyilvánítása szükségszerűen egyes alapvető jogok korlátozásával jár, hiszen az embereknek tartózkodniuk kell kívánt magatartásuktól, vagy valamely joguk teljes körű gyakorlásától, mindezt legtöbbször valamely más személyt megillető jogok védelme érdekében. Melyek ezek a konkuráló jogok?

Az alapvető jogok. Az 1949. évi XX. törvény (a továbbiakban: Alkotmány) 8. §-a alapján „(1) A Magyar Köztársaság elismeri az ember sérthetetlen és elidegeníthetetlen alapvető jogait, ezek tiszteletben tartása és védelme az állam elsőrendű kötelessége. (2) A Magyar Köztársaságban az alapvető jogokra és kötelességekre vonatkozó szabályokat törvény állapítja meg, alapvető jog lényeges tartalmát azonban nem korlátozhatja.”. Az új Alaptörvényben mindez a következőképpen ölt testet: „(1) AZ EMBER sérthetetlen és

[230] LONTAI E., FALUDI G., GYERTYÁNFY P. & VÉKÁS G., *Magyar polgári jog – Szellemi alkotások joga*. Eötvös József Könyvkiadó, Budapest 2008. p. 125.

elidegeníthetetlen alapvető jogait tiszteletben kell tartani. Védelmük az állam elsőrendű kötelezettsége. (2) Magyarország elismeri az ember alapvető egyéni és közösségi jogait. (3) Az alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg. Alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható.". E rendelkezések igénylik a legrészletesebb értelmezést, ezért a vonatkozó alkotmánybírósági határozatokat a későbbiekben ismertetem.

A tulajdonhoz való jog. Az Alkotmány 13. § (1) bekezdése alapján „A Magyar Köztársaság biztosítja a tulajdonhoz való jogot.", míg az új Alaptörvényben az alkotmányozó a következőképpen rendelkezett: „Mindenkinek joga van a tulajdonhoz és az örökléshez.". A tulajdonjog az alkotmányjog körében tágabb, eltérő jelentéssel bír, mint a magánjogi tulajdon-fogalom, így felölel többek között egyes vármányosi jogosultságokat és szellemi alkotásokhoz fűződő vagyoni jogosultságokat is. Ki kell azonban emelni, hogy az Alkotmánybíróság viszonylag sokáig várt annak kimondásával, hogy a szerzői jog által védett alkotások, teljesítmények alkotmányos értelemben véve a tulajdon egyik típusának tekinthetők.[231] Nem hagyható figyelmen kívül az sem, hogy a szellemi alkotások – mint ahogyan a kifejezés elnevezésében is szerepel – nem a jog által meghatározott jogviszony eredményeképpen, hanem egy ember szellemi tevékenységének produktumaként, alkotásaként jönnek létre. Ekként a szerzői jog a tulajdonhoz való jog mellett szorosan kötődik az Alkotmány 70/G. §-ban meghatározott művészeti élet szabadságához is, amelynek tiszteletben tartása és támogatása a magyar állam intézményvédelmi kötelezettségét teremti meg. Itt tartom szükségesnek röviden kitérni a szerzői jogról szóló 1999. évi LXXVI. törvény preambulumára, amely meghatározza a szerzői jogi szabályozás célját, amely ekként szól: „A technikai fejlődéssel lépést tartó, korszerű szerzői jogi szabályozás meghatározó szerepet tölt be a szellemi alkotás ösztönzésében, a nemzeti és az egyetemes kultúra értékeinek megóvásában; egyensúlyt teremt és tart fenn a szerzők és más jogosultak, valamint a felhasználók és a széles közönség érdekei között, tekintettel az oktatás, a művelődés, a tudományos kutatás és a szabad információhoz jutás igényeire is; gondoskodik továbbá a szerzői jog és a kapcsolódó jogok széles körű, hatékony érvényesüléséről.". A szellemi alkotások védelme kapcsán a szabályozás módjára jellemző, hogy a tulajdonhoz fűződő jogok elsődlegességét középpontba emelő és döntő részben anyagi szemléletet tükröző védelme az alkotó ember személyiségéhez kapcsolódó érdekek és jogosultságok jogi oltalmával egészül ki.[232] Kétségtelen, hogy e kettősségben rejlik a szerzői jog szabályozásának különleges volta, azonban az értekezés vizsgálódásának céljára figyelemmel – mivel a Btk. vagyon elleni bűncselekményekről szóló fejezetében elhelyezett 329/A. § tényállása a szerzői művek jogosultjainak vagyoni jogosultságait védi – ezért a továbbiakban a vonatkozó szerzői jogi szabályokat az elsősorban vagyoni értékű jogokkal kapcsolatos jogviszonyokat magába foglaló tulajdonjogi fogalom részének tekintem.[233] Mivel az alkotmányjog által használt fogalomrendszer egyébként is önálló, a jogtudomány többi részterületétől olykor eltérő, bővebb jelentésekkel ruház fel egyes fogalmakat, a szerző jogviszonyok védelme érdekében megalkotott jogszabályok alkotmányossági vizsgálata során a szerzői jog jogrendszeri elhelyezése nem meghatározó jelentőségű, így ennek részletesebb kifejtését mellőzőm.

[231] GYENGE A., *Szerzői jogi korlátozások és a szerzői jog emberi jogi háttere.* HVG-ORAC Budapest, 2010. p. 171.
[232] SUM, 2009. p. 201.
[233] Megemlítendő, hogy a szerzői jogról szóló 1999. évi LXXVI. törvény preambuluma e jogterület szabályozásának célját ismertetve szintén „szellemi tulajdonjog"-ot említ.

A cselekvés szabadsága. Míg az egymással szembekerülő elemek egyike, védeni kívánt értéke a tulajdonjog és a művészeti alkotás szabadságának ötvözete, addig a másik oldalon az emberi cselekvés szabadsága jelenik meg. Az Alkotmány 54. § (1) bekezdése deklarálja a méltósághoz való jogot, azaz a „Magyar Köztársaságban minden embernek veleszületett joga van az élethez és az emberi méltósághoz...". A 8/1990. (IV. 23.) AB. határozatban az AB az emberi méltósághoz való jogot az általános személyiségi joggal azonosította, amelynek összetevői többek között: a személyiség szabad kibontakoztatásához való jog, az önrendelkezés joga, az általános cselekvési szabadság.[234] Az emberi méltóság tehát olyan anyajognak tekinthető, amely felöleli többek között az általános cselekvési szabadságot is. A fejezet vizsgálódása tárgyában a szerzői jogi szabályozás vonatkozásában ezen cselekvési szabadság kerül konfliktusba a tulajdonjog alkotmányos védelmével szemben.

3.1.2. A magánjogi szint

Mivel az alkotmányjogi értelemben vett tulajdon-fogalom tágabb a polgári jogi értelemben használtnál, a szerzői mű alkotóját megillető vagyoni jogosultságok is értendők alatta. A jogalkotó az ebben az összefüggésben értelmezett alkotmányos alapjog védelme érdekében alkotta meg a szerzői jogról szóló 1999. évi LXXVI. törvényt, amely a Polgári törvénykönyvről szóló 1959. évi IV. törvénnyel és a Polgári perrendtartásról szóló 1952. évi III. törvénnyel együtt biztosítja a jogsérelmet szenvedett jogosult számára igényének érvényesítését.

3.1.3. A büntetőjogi szint

A Cyber-crime Egyezmény 10. Cikke írta elő egyes számítástechnikai vonatkozással bíró, szerzői vagy szerzői joghoz kapcsolódó jogot sértő cselekmények büntetni rendeltségét a következőképpen. Az Egyezmény alapján minden szerződő fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön az Irodalmi és Művészeti Művek Védelméről szóló Berni Uniós Egyezménybe és az azt felülvizsgáló 1971. június 24-én megkötött Párizsi Egyezménybe, a Szellemi Tulajdonjogok Kereskedelmi Vonatkozásairól szóló Egyezménybe, a Szellemi Tulajdon Világszervezete Szerzői Jogi Szerződésébe foglalt és a Fél által elfogadott kötelezettségeknek megfelelően meghatározott szerzői jogok – kivéve a fenti egyezményekben megállapított bármely személyhez fűződő jogok – megsértése, amennyiben azt *szándékosan, kereskedelmi méretekben* és számítástechnikai rendszer útján követik el. Továbbá minden szerződő fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön az Előadóművészek, a Hangfelvétel-előállítók és a Műsorsugárzó Szervezetek Védelméről szóló Római Egyezménybe, a Szellemi Tulajdonjogok Kereskedelmi Vonatkozásairól szóló Egyezménybe, a Szellemi Tulajdon Világszervezetének az Előadásokról és a Hangfelvételekről szóló Szerződésébe foglalt és a fél által elfogadott kötelezettségeknek megfelelően meghatározott szomszédos jogok – kivéve a fenti egyezményekben megállapított bármely személyhez fűződő jogok – megsértése, amennyiben azt *szándékosan, kereskedelmi méretekben* és számítástechnikai rendszer útján követik el.

A hazai szabályozásban a szerzői vagy szerzői joghoz kapcsolódó jogok megsértését az 1978. évi IV. törvény 329/A. §-a rendeli büntetni. Az (1) bekezdése alapján „Aki másnak a

[234] ZAKARIÁS K. & SZIRBIK M., Az élethez és az emberi méltósághoz való jog. In. JAKAB A. (ed.), *Az Alkotmány kommentárja II.* Századvég Kiadó Budapest, 2009. p. 1905.

szerzői jogról szóló törvény alapján fennálló szerzői vagy ahhoz kapcsolódó jogát haszonszerzés végett, vagy vagyoni hátrányt okozva megsérti, vétséget követ el, és két évig terjedő szabadságvesztéssel büntetendő.”.

A bűncselekmény bűntetti alakzatát a (3) bekezdés tartalmazza, amely szerint: „A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a szerzői vagy szerzői joghoz kapcsolódó jogok megsértését a) jelentős vagyoni hátrányt okozva, b) üzletszerűen követik el.”. A tényállás egyértelműen keretténállás, amelyet a szerzői jogi törvény rendelkezései töltenek ki tartalommal. A bűncselekményt elköveti, aki haszonszerzés végett, vagy vagyoni hátrányt okozva a szerzői jogi törvénybe ütköző módon használ fel valamely művet, vagy sérti meg a jogosult egyéb vagyoni érdekeit.

A gyakorlatban legtöbbször előforduló eset egy mű vagy művek valamely jogellenes felhasználása és a jogdíj meg nem fizetése, amely nyilvánvalóan haszonszerzés végett történik, vagy vagyon hátrányt okoz. Az alapvetően kötelmi jogi jogviszony megsértésében megnyilvánuló jogellenes cselekmény elbírálása, megítélése legtöbbször magánjogi gondolkodásmódot és túlnyomórészt polgári jogi jogértelmezést igényel, amely sokszor idegen a büntetőjogi dogmatikától.

3.2. Az alkotmányosság vizsgálandó szempontjai

A legtöbb alapjog korlátozása kapcsán az Alkotmánybíróság által alkalmazott szükségesség-arányosság teszt felhívásával megállapítható, hogy a szerzői tulajdon védelme érdekében az egyén cselekvési szabadsága igenis korlátozható. Elfogadom, hogy a szerzői alkotások védelme érdekében büntetőjogi tényállás megalkotásának alkotmányosan elfogadható célja van, a korlátozás valóban szükséges. Ezért kizárólag az utolsó lépcsőfokot jelentő arányossági próbának kell alávetni a Btk 329/A. §-át.

Az Alkotmánybíróság által megfogalmazott alkotmányossági kritériumok ismeretében a kriminálpolitikai megfontolásokat kirekesztve kizárólag a következő kérdésekre kell választ kapnunk. Elsőként: a Btk. 329/A. §-a arányos, mértéktartó és megfelelő választ ad-e a veszélyesnek, nem kívánatosnak ítélt jelenségre, azaz az alkotmányos alapjogok korlátozása esetén irányadó követelménynek megfelelően a cél eléréséhez a lehetséges legszűkebb körre szorítkozik-e? Másodikként: a jogalkotó adott-e alkotmányosan elfogadható indokot a szabályozás hatályos formájára? Végül harmadsorban: a tényállás megfelel-e a normavilágosság követelményének?

3.4. A szabályozás értékelése

3.4.1. Az ultima ratio formai oldaláról

A Btk. 329/A. § vizsgálata alapján a következők állapíthatók meg. A tényállás a Büntető Törvénykönyv Különös Részében, azon belül is a vagyon elleni bűncselekményeket összegyűjtő fejezetben található. Valamennyi vagyon elleni bűncselekménynek – az arányosság szellemében, alkotmányosan – szabálysértési alakzata is létezik. Ezzel szemben a vizsgált tényállás nem rendelkezik a büntethetőség alsó összeghatáráról, és szabálysértési alakzata sem létezik. Az állam által a polgári jogon keresztül biztosított igényérvényesítést követően csak és kizárólag a büntetőjogi felelősségre vonás alkalmazása jelenti a jogvédelem következő és egyben legmagasabb, végső szintjét. A hatályos szabályozás tehát még csak formálisan sem tesz eleget az arányosság követelményének, mivel a

társadalomra csekély fokban veszélyes szerzői jogot sértő cselekményeket is bűncselekménnyé nyilvánítja.

Végül megemlítendő, hogy a vagyon elleni bűncselekmények koherens szabályozása is megköveteli, hogy a jogalkotó a bűncselekmény szabálysértési alakzatát is meghatározza a bűncselekményi határ meghatározásával, hiszen a büntetőjog szerepe valamennyi más vagy elleni bűncselekmény esetén alkotmányos szerepének megfelelően már egyértelműen behatárolt.

3.4.2. Az ultima ratio tartalmi oldaláról

A formai vizsgálat után – amennyiben el is fogadnánk, hogy nincs szükség szabálysértési tényállásokra – kérdésként merül fel, hogy jelen esetben a büntetőjogi felelősségre vonás ultima ratio-ként aposztrofált lehetősége valóban betölti-e annak tartalmi elvárásait, azaz a büntetőeljárás előtt megindítható polgári jogi eljárás lehetősége egyedül elegendő-e. A „végső soron történő igénybevétel" nem lehet azonos, nem szabad, hogy azonos legyen az „alternatívával", amely tartalmilag kiüresíti az Alkotmánybíróság által levezetett, fentebb ismertetett alapelveket.

A jogalkalmazók körében jól ismer módon a szerzői jogi jogosult és képviselője számára nyilvánvalóan egyszerűbb és költséghatékonyabb megoldás az, ha nem magánjogi úton érvényesítik igényüket, hanem büntetőeljárást kezdeményeznek. Miért? Mert a büntetőeljárás során az állami hatóságok, az őket gúzsba kötő officialitás elve okán mozgásba lendülve, költséget és munkaidőt nem kímélve, a magánéletbe történő legkomolyabb beavatkozásokkal lefolytatják a bizonyítási eljárást – olyan bizonyítási eszközök beszerzését biztosítva ezáltal, amelyek a polgári jogi eljárás keretében egyebekben nem lennének beszerezhetők – amelynek eredményességét követően polgári jogi igényt lehet érvényesíteni.[235]

A kriminalizáció mellett a legtöbb szerzői jogi bűncselekmény súlyára figyelemmel elgondolkodtatók a nyomozásnak a magánszférába való behatolásakor történő alapjog-korlátozások esetei is. A nyomozás és a bizonyítás során az egyik leggyakrabban alkalmazott kényszerintézkedés a lefoglalás, amellyel biztosítható, hogy a szerzői jogi tartalmakat tároló adathordozót szakértő vizsgálja meg. Ennek során nemcsak a bűncselekménnyel kapcsolatba hozható személyes információk, adatok kerülnek szélesebb körben ismertté, hanem magánéleti vagy üzleti titkok is. A legtöbb szerzői jogi bűncselekmény súlya nem minden esetben indokolja a büntetőeljárással szükségszerűen együtt járó kényszerintézkedések alkalmazását. A büntetőeljárás kényelmes megoldásnak tűnik annak ismeretében, hogy a szerzői jogvédelem komplex rendszerében – az intézményi szervezetrendszert is ide értve – maga a szerzői jogi törvény ruházta fel a jogosultak közös jogkezelőjét vagyonjogi ügyekben képviseleti joggal, ekként nem csak a felhasználási díjak begyűjtése, hanem a polgári ügyekben való fellépés kiszélesítése is feladatuk volna ezen egyesületeknek még akkor is, ha a polgári perben való bizonyítás terhe és költségei érthető módon számos nehézséggel jár.

A Btk. 329/A. § keretténylállása a szerzői jogról szóló törvény rendelkezéseinek megsértésén kívül büntetőjogi többletfeltételt nem állapít meg, így a büntetőjogi felelősség

[235] A polgári jogi felelősség és eljárás szabályai alapján a bizonyítási teher szintén a keresetet benyújtó, a jogsértést állító felet terheli.

alapja teljes mértékben megegyezik a polgári jogi felelősség megállapításának módjával.[236] E rendszerben eltűnik az ultima ratio-kénti alkalmazás követelményének érvényesülése.

A jogalkotó a szabályozás ezen formájának nem adta alkotmányosan elfogadható indokát. A társadalom „betörése" a szellemi tulajdon tiszteletére nem a büntetőjog rendeltetése, sokkal inkább az állami oktatásba és ismeretterjesztésbe, valamint a büntetőjogon kívüli igényérvényesítés biztosításába utalt feladata. A vizsgált tényállásban megjelenő téves büntetőjog-politika elfogadhatatlan, alkotmányossági szempontból pedig egyébként sem tekinthető megfelelő indoknak, mert nélkülözi a törvényes cél más módon el nem érhetőség követelményét is!

3.4.3. A jogbiztonság és a normatartalom világossága oldaláról

A fent részletezett jogállamiság elvéből levezethető jogbiztonságnak a tényállás a következő okok miatt nem felel meg. A fejezet elején, a problémafelvetés alkalmával jeleztem, hogy az elkövetési érték meghatározására – amely a bűncselekmény minősítése szempontjából meghatározó jelentőségű – több módon kerülhet sor. Elfogadhatatlan, hogy a jogsérelem megtörténte után, a tényállás alapján a terheltre terhesebben kiható módszerrel határozza meg az elkövetési értéket a jogalkalmazó, az egymáshoz közeli eredményekre vezető módszerek közötti választás pedig eleve önkényes jogalkalmazáshoz vezetne.

Szintén a jogállamisághoz köthető elvárás, hogy egy cselekmény büntetendővé nyilvánítása esetén valamennyi jogsértő felkutatására és megbüntetésére van szükség a szabályozás legitimitásához, társadalmi elfogadtatásához. A köztudomás szerint is magas látencia egyik jellemzőjeként a szerzői jogi bűncselekmények felfedezésére a legtöbb esetben más bűncselekmények nyomozása során járulékosan, például számítógép lefoglalásával járó büntetőeljárások keretén belül, ad hoc jelleggel kerül sor, vagy alkalmanként ütemezett, a közös jogkezelők által végrehajtott ellenőrzések alkalmával. E körülmények viszont a büntetéssel fenyegetettség következetlen érvényesülését, a szabályozás céljának elenyészését eredményezik.

3.4.4. A jogdíjközlemények vonatkozásában

A jogdíjközlemény alapján az engedély visszamenőleges elvesztése nem alapozhatja meg egy korábbi, díjfizetéssel jogosított időszak cselekményeinek (többszörözéseinek) jogellenességét. Máshogy fogalmazva nem lehet felelősségre vonni a felhasználót egy múltbeli, akkor jogszerű cselekménye miatt egy jelenkori szerződéssértő mulasztás miatt, hiszen a korábbi időszakban volt jogdíjfizetés, tehát a felhasználás jogszerű volt. Megint máshogy fogalmazva: nem képezheti a büntetőjogi felelősségre vonás alapját egy jelenkori mulasztás, ami a terhelt múltbeli, jogszerű cselekményét teszi visszamenőlegesen jogellenessé, következésképpen a jogellenesség megállapítása visszamenőleges hatályú, azaz az Alaptörvény XXVIII. cikk (4) bekezdésében és a Btk. 2. §-ában meghatározott nullum crimen sine lege elvét sérti. A jogdíjközlemény szabályainak büntetőjogi alkalmazása tehát több visszásságot is felvet. Egyrészt: amennyiben a megelőző időszakhoz képest a késedelembe eséssel érintett időszakban nem történt újabb zeneszámok többszörözése, akkor a jogdíjközleménnyel ellentétben, büntetőjogi szempontból nincs jogtárgysértés, mivel nincs újabb többszörözött szerzői mű, és a

[236] A szerzői jogi jogsértések nyilvánvalóan vagyoni hátrányt okoznak, mivel a szerzői alkotások valamennyi releváns felhasználása – ide nem értve a szabad felhasználás eseteit – jogdíjfizetési kötelezettséget von maga után.

mulasztáson kívül nincs szerzői jogi tekintetben elkövetési magatartás: felhasználás (többszörözés). Másrészt: a jogdíjközlemény nem jogszabály, nem törvény, csupán az elkövetési értékre vonatkozóan tesz megállapításokat. A szerzői jogi törvény az, amely alapján meg kell ítélni egy felhasználás jogszerűségét. Pusztán egy díjtétel-konstrukció nem teljesítése, önmagában a nemfizetés ténye a többszörözés hiányában nem felhasználás, csupán szerződésszegés. Ha nincs az adott negyedévben többszörözés, a jogdíjfizetés elmaradása csupán kötelmi igényt keletkeztet. Harmadrészt: a jogdíjfizetés eleve a jövőre vetítetten történik, a jövőbeni többszörözések jogosítása érdekében. A még meg nem történt többszörözésre vonatkozóan szintén nem lehet büntetőjogi felelősséget megállapítani, felhasználás hiányában. Összességében megállapítható, hogy a jogdíjközlemények előírásaira történő hivatkozás sok esetben elfogadhatatlan az elemzett tényállás megítélésénél.

3.5. Következtetések

A hatályos szabályozás komplex rendszerének ismeretében a feltett kérdésekre a következő válaszok adhatók. Arra vonatkozóan, hogy arányos-e a tényállásban megjelenő szabályozás megállapítható, hogy a vitatott tényállás meghatározása során a jogalkotó nem mérlegelte kellő körültekintéssel azt, hogy a szerzői jogot sértő cselekmények mindegyike oly módon veszélyezteti a fennálló jogrendet, hogy a társadalom védelmére a jogrendszerben megállapított egyéb szankciók már nem elegendőek, s ezért a büntetőjogi felelősség meghatározásával teljes körű szabályozására van szükség. Ennek következtében túl szélesen határozta meg a büntetendővé nyilvánított magatartások körét, ezzel megsértette az Alkotmánybíróság 30/1992. (V. 26.) számú határozatában részletezett alkotmányos büntetőjognak a jogállamiságból fakadó azon követelményét, amely szerint az emberi jogokat szükségképpen korlátozó büntetőjogi eszközrendszernek a cél eléréséhez a lehetséges legszűkebb körre kell szorítkoznia.

Azzal kapcsolatban, hogy a hatályos szabályozásnak van-e alkotmányosan elfogadható indoka a következők állapíthatók meg. A jogalkotó nem adta alkotmányos indokát az arányosság elvébe ütköző szabályozásának, ekként önkényesen járt el, amikor a büntethetőség feltételeit a hatályos módon határozta meg. Az állam ezzel is túllépte büntetőhatalmának alkotmányos kereteit. A jogbiztonság vonatkozásában – a korábbi fejezet megállapításait tovább nem részletezve – egyértelmű, hogy a tényállás nem felel meg a jogbiztonság követelményének, tartalma nem egyértelműen megállapítható, túlzott teret engedhet a jogalkalmazói önkénynek. Mindezek ismeretében a Btk. 329/A. §-a a magyar alkotmányos büntetőjog elveinek nem felel meg, az alkotmány rendelkezéseibe ütközik, azaz erre irányuló alkotmánybírósági normavizsgálat kezdeményezése esetén meg kell semmisíteni.

A címet Wiener A. Imre gondolataival akként zárom, hogy az állam büntetőhatalma csak ott és annyiban érvényesülhet, ahol céljának megfelel, és jogalapját veszti, ha e célt nem tudja szolgálni, vagy csak nagyobb sérelem árán szolgálja, mint amelyet elhárít.[237] Éppen ezért a jogalkotónak utólagos eredményességi vizsgálat keretén belül mihamarabb felül kell vizsgálnia a szabályozás rendszerét az alkotmányos büntetőjog alapelveinek maradéktalan érvényesülése érdekében, az Alkotmánybíróság feladata pedig – erre irányuló beadvány esetén – állást foglalni a tényállás sorsát illetően.

[237] WIENER A. I., Alkotmány és büntetőjog. *Állam és Jogtudomány.* 1995. (37. évf.) 1-2 szám. p. 103.

4. DOGMATIKAI ANOMÁLIÁK: HALMAZATI KÉRDÉSEK ÉS A SÉRTETT

4.1. A halmazati kérdések

4.1.1. Az alapok: jogi tárgy, elkövetési tárgy és a sértett a szerzői vagy szerzői joghoz kapcsolódó jogok megsértése esetén

A büntető anyagi jogi dogmatikai egyik furcsállott tétele jelenik meg szinte valamennyi hazai büntetőjogi tankönyvben vagy tudományos publikációban, amikor a halmazati kérdések boncolgatása során egy eljárásjogi fogalom, a sértett kiléte és száma minősül meghatározó szempontnak. A sértett büntető anyagi jogi dogmatikától rendszeridegen, mégis bevett fogalma azonban a szerzői jogi tényállások esetében könnyen téves minősítésekhez vezethet. A Be. rendelkezései alapján a sértett a büntetőeljárás egyik, meghatározott jogokkal felruházott résztvevője, akinek személyét az eljárási törvény egyfajta tautológiaként írja körül: az 52. § (1) bekezdése alapján sértett az, akinek jogát vagy jogos érdekét a bűncselekmény sértette vagy veszélyeztette. A sértetti fogalom anyagi jogi „kölcsönvételének" alapja annak jogi tárgyra utaló tartalma – azaz a jog vagy jogos érdek sérelme, veszélyeztetése –, amely viszont már anyagi jogi kategória. A további kérdés ettől kezdve megint csak az, hogy ki is a bűncselekmények sértettje, kinek és milyen jogát sérti vagy veszélyezteti a bűncselekmény. Ennek meghatározása valamennyi korábban felsorolt diskurzus előfeltétele, csakis ezután kerülhet sor a halmazat megállapításának részletes tárgyalására, és a sértett-alapú rendbeliség következményeinek felismerésére.

Az anyagi jogi dogmatika jelen kérdéskörének egyik legfontosabb alapfogalma a jogi tárgy, amely röviden és tömören az a jelenség, amit a büntetőjog véd, illetőleg a bűncselekmény támad, hiszen egy cselekmény nem önmagában, hanem a jogi tárgyra való kihatásában veszélyes a társadalomra. Bócz Endre szavaival élve a jogi tárgy az absztrakció magas szintjén jelentkező, inhomogén elemekből álló fogalom, amely a lényegét tekintve emberek és dolgok közötti viszonyok olyan változatait – és változásait – fogja át, amelyekben a társadalmi értékek és érdekek kívánatosnak vélt egyensúlya nem bomlik meg. Az emberek és a tárgy-társadalmi környezet folytonos kölcsönhatása alkotta társadalmi létezés egyik eleme azon céltudatos emberi tevékenység, amely olyan változás létrehozására irányul, amely a tevékenykedő tudatosult szükségleteinek kielégítésére az aktuális létezőnél alkalmasabb. Következésképpen a tettes magatartásával a konkrét fennálló és elismert jogi értéket megjelenítő viszonyrendszer valamelyikére hat, és ha az természetes személy, akkor ez az ember válhat a bűncselekmény passzív alanyává, egyébként a jogi tárgyat megjelenítő konkrét viszonyrendszer elemét elkövetési tárgynak nevezzük.[238]

A szerzői jogi tényállások kapcsán is az említett konkrét viszonyrendszereket, bizonyos szerzői jogi alapjogviszonyokat érdemes vizsgálni, és azok közül is a rendeltetésük szerint értéket hordozókat kiemelni, amelyek egy időben való megsértése adott esetben majd a megfelelő halmazati szempontok kiválasztását alapozhatja meg.[239] A szerzői jogi tényállások szűkebb jogi tárgya a szerzők és szomszédos jogi jogosultak vagyoni jogai, áttételesen a szellemi alkotás ösztönzése, a nemzeti és egyetemes kultúra értékeinek megóvása az alkotó ember elismerésének biztosítása, míg a bűncselekmények elkövetési

[238] BÓCZ E., Passzív alany, áldozat, sértett. *Rendészeti Szemle*. 2007/9. pp. 104-106.
[239] Ilyen viszonyrendszer: a mű szerzőének vagyoni jogai, a mű felhasználása és engedélyezése, a szerzői és szomszédos jogok egymáshoz való kapcsolata.

tárgya a műpéldány, figyelemmel az azon fennálló vagyoni jogosultságokra is.[240] A mű jogellenes felhasználásának mikéntje pedig az előző bekezdésben említett szükségletekhez igazodva képezi az elkövetési magatartást. A szerzői vagy szerzői joghoz kapcsolódó jogok megsértése kapcsán mindenekelőtt azt kell megjegyeznünk, hogy keret- és nyitott tényállásként a Btk. 329/A. §-a egy önálló törvénnyel szabályozott jogviszony-rendszer megsértését rendeli büntetni, középpontjában a művel és az ahhoz kapcsolódó – szerzői és szomszédos jogi – jogosultakkal, másként fogalmazva a sértett ezen vagyoni jogok jogosultja.[241]

Itt tartom szükségesnek megemlíteni, hogy a Btk. 329/A. §-a, helyesen a vagyon elleni bűncselekményekről szóló fejezetben található, ezen okból kifolyólag csak a sértettek vagyoni jogosultságai relevánsak annak ellenére is, hogy a tényállás megfogalmazása lehetővé tenné a bűncselekmény elkövetésének megállapítását a személyhez fűződő jogok sérelme esetén is. Utóbbi esetben a jogalkotó nem tekintett minden, a szerzői jogi törvényben meghatározott személyhez fűződő jogot sértő magatartást olyan mértékben társadalomra veszélyesnek, hogy azokat bűncselekményként szabályozza.

4.2.2. A sértett anyagi jogi szempontból – az egység-többség kérdése

A vagyon elleni bűncselekmények esetén a bűncselekmények rendbelisége általában a sértettek személyéhez kötött, azok számához igazodik. E tézis alkalmazhatatlansága a szerzői joggal kapcsolatos bűncselekmények körében a következő okokban rejlik. A szerzői jogról szóló 1999. évi LXXVI. törvény (a továbbiakban: Szjt.) különbséget tesz a szerzői és a szerzői joghoz kapcsolódó jogok között, de a jogosultakat mindkét esetben vagyoni jellegű jogosultságokkal ruházza fel, amelyek megsértésével adott esetben bűncselekmény valósulhat meg. Ez az elmélet a gyakorlatban számos formában testet öltött már, így például a Szerzői Jogi Szakértő Testület[242] a 27/99. számú szakvéleményében – e kérdésre csak utalva – kifejtette: a lefoglalt hamisítványok elkészítése és forgalomba hozatala sérti a szerzők és a szomszédos jogi jogosultak jogait. A szerzői oldalon jogsérelmet szenvednek a zeneszerzők, a szövegírók, és a zeneműkiadók azáltal, hogy a hamisítványok után nem történt jogdíjfizetés.[243] A kérdés tehát az, hogy egy adott mű engedély nélküli felhasználásával a terhelt valójában mennyi jogosult – azaz sértett – vagyoni jogait sérti.

A zenei és filmalkotások olyan „összekapcsolt" és „közös műveknek" tekinthetők, amelyek létrehozása több szerző alkotó munkájának eredménye, és érzékelhetővé tételük is jogokkal felruházott személyek tevékenységén keresztül történik. A közös művek egyik fő jellemzője, hogy az egymást kiegészítő és erősítő alkotásrészek szerzőinek a közös

[240] A mű nem azonos a műpéldány fogalmával. A mű mint szellemi alkotás (például regény) konkrét megjelenési formája a műpéldány (könyv).
[241] A szerzői jogi jogviszonyok rendkívül változatos formát ölthetnek a mű létrehozásától kezdve az alkotás jogi oltalmán át a megfelelő felhasználásáig. A tanulmány utóbbi két szakasz abszolút és szerződéses jellegű jogviszonyát emeli ki.
[242] A Szerzői Jogi Szakértő Testületet 1970-ben hozták létre. Feladatait, szervezeti és működési rendjének keretszabályait a szerzői jogról szóló 1999. LXXVI. törvény (Szjt.) állapította meg újra. Az Szjt. 101. § (1) bekezdése szerint a Testület a Magyar Szabadalmi Hivatal mellett működik. Az Szjt., illetve a Szerzői Jogi Szakértő Testület szervezetéről és működéséről szóló 156/1999. (XI. 3.) Korm. rendelet alapján, a Testület szerzői jogi jogvitás ügyekben felmerülő szakkérdésekben a bíróságok és más hatóságok megkeresésére, illetve a felhasználói jog gyakorlásával kapcsolatos kérdésekben peren kívüli megbízás alapján jár el. (Forrás: http://www.mszh.hu/testuletek/szjszt/ (2010-02-28))
[243] VIDA J., A szerzői jog büntetőjogi védelmének néhány gyakorlati kérdése, különös tekintettel a zeneművekre. *Ügyészek Lapja*, 2005/5. p. 16.

elhatározással létrejövő új mű egészére is keletkeznek kizárólagos szerzői jogai, az alkotás maga pedig a szerzők együttes akaratnyilvánítása, pontosabban az együttességet megalapozó jogügyletének eredményeképpen jön létre.[244] Az összekapcsolt művek jogi vonatkozásaihoz a szerzői jogról szóló törvény 5. § (2) bekezdését kell értelmeznünk, amely alapján, ha a közös mű részei önállóan is felhasználhatók, a saját rész tekintetében a szerzői jogok önállóan gyakorolhatók. A továbbiakban egy konkrét példán keresztül szemléltetem, mely jogosultaknak milyen szerzői joga sérülhet.

A szellemi tevékenységből fakadó, egyéni, eredeti jellegű zenemű szerzője a szerzői jogi jogosult, akinek az Szjt. 18 § (1) bekezdése alapján kizárólagos joga van arra, hogy művének többszörözéséhez másnak engedélyt adjon. Maga a mű fizikai valóságban nem létezik, lényegében hangjegyek megfelelő elrendezése a képzeletbeli kottában, érzékelhetővé zenekari előadása útján válik. A zeneművet egy adott zenekar – stílusától függően – számos, különböző módon is előadhat, legyen szó rock együttesről vagy kamarazenekarról. A közös bennük az, hogy egyedi előadásukat a törvény külön-külön védelemben részesíti, azaz előadóművészi minőségükben az Szjt. alapján a szerzői joghoz kapcsolódó jogok, szomszédos jogok illetik meg őket. Az Szjt. 73. § (1) bekezdésének c) pontja alapján az előadóművész joga, hogy hozzájárulását adja rögzített előadásának többszörözéséhez. Tovább haladva a példán, egy szűkebb zenefogyasztói piacon való megjelenéshez a megfelelő infrastruktúrával nem rendelkező előadóművész a kiadó segítségét veszi igénybe, amely profitorientált gazdasági szervezet a művet előadóművészek által érzékelhetővé tett formájában materializálja, azaz a megfelelő adathordozón elhelyezve és a fogyasztók számára többszörözve hozzáférhetővé teszi. Ebbéli tevékenységét az Szjt. szintén védelemben részesíti a szerzői joghoz kapcsolódó jogok között, mivel a 76. § (1) bekezdésének a) pontja alapján – a konkrét példánknál maradva – a hangfelvétel előállítójaként jogosult, hogy hangfelvételének többszörözéséhez hozzájáruljon. A fent sorolt jogosultakat a különböző felhasználásokért díjazás illeti meg. E jogviszonyrendszert kitűnően szemléltetik a MAHASZ honlapján közzétett következő adatok.[245] A kereskedelmi forgalomban szereplő zenei adathordozó értékében a számos összetevő közül egy rész a forgalmi adó, további elem a kiskereskedelmi árrés, amelyből a CD-t árusító üzlet fedezni tudja költségeit. A fennmaradó összeg a kiadó által alkalmazott nagykereskedelmi átadási ár, amelyből egy rész a szerzői jogdíj, amit a lemezkiadó az Artisjusnak köteles megfizetni. Az előadóknak járó díj, az ún. royalty[246] 8-15% körüli részt képvisel, a kulturális járulék az átadási ár 2%-a, amit az államnak kell megfizetni, míg a terjesztés költsége a nagykereskedelmi ár körülbelül 10%-a, amely fedezi a raktározási, logisztikai, kiszállítási költségeket.[247]

Polgári jogi tekintetben az említett jogosultaknak párhuzamosan fennálló, kizárólagos engedélyezési joga és díjigénye van. Ha tehát egy elkövető a felsorolt jogosultak engedélye nélkül jogosulatlanul többszöröz egy műpéldányt, azzal mindegyik jogosult vagyoni érdekét sérti, következésképpen alaki halmazatként egy rendbeli szerzői jogok megsértésének vétségét és két rendbeli szerzői joghoz kapcsolódó jogok megsértésének vétségét követi el. Jelen példa a zeneművek többszörözésére épülve mutatta be a rendbeliség meghatározását, azonban hasonlóan kell eljárni a többi összekapcsolt mű és

[244] SUM, 2009. p. 235.
[245] http://mahasz.hu/m/?menu=gyik [2011-07-31]
[246] A kiadói szerződés (amely maga is egyfajta felhasználási szerződés) alapján a kiadó alapvető kötelezettsége a felhasználásért járó díj megfizetése, amelynek összegében a felek két módon állapodhatnak meg: fix összegben vagy a példányok árának és az eladott példányok számának függvényében (royalty).
[247] http://mahasz.hu/m/?menu=gyik [2011-07-31]

felhasználásuk esetén, így például a filmalkotások esetén is. A teória alkalmazhatatlansága abban mutatkozik, hogy jelentős számú zenei mű és filmalkotás érintettsége esetén rendkívül időigényes feladat a művek szerzői és szomszédos jogi jogosultjának és jogviszonyaik hiánytalan felderítése.

Egy álláspont még az előzőnél is tovább megy.[248] Eszerint a szerzői jogsértések többsége a sértettek számához igazodik, és mivel a jogsértő magatartás tipikusan a hang-, illetve képhordozókkal kapcsolatban valósul meg, ezért ebben az esetben a sértett a hangfelvétel-, illetve filmelőállító, illetve az előállító jogán a forgalmazó, zenét tartalmazó hordozók esetében pedig emellett a többszörözési jogokat kezelő zenei közös jogkezelő szervezet is. A közös jogkezelő szervezet sértetti szerepére részletesen a következő fejezetben térek ki, de már most jelezni kell, hogy a szerzői jog védelmének és ultima ratio a büntetőjog védelmének alapja nem a közös jogkezelők érdeke és igénye, hanem a már korábban említett: a szellemi alkotás ösztönzésében, a nemzeti és az egyetemes kultúra értékeinek gyarapításában megnyilvánuló társadalmi érdek.

Egy látszólagos kitérőt téve a szerzői jog vagyoni jogviszonyai leginkább a tulajdonjog abszolút szerkezetéhez hasonlíthatók, amennyiben igen erős, kizárólagos jogosultságokat biztosítanak a jogosultak számára. Könnyedén felmerülhet tehát az az elképzelés, hogy a hasonlóságot felhasználva a szerzői jogi tényállások értelmezése során is a szilárdabb dogmatikával rendelkező többi vagyon elleni bűncselekmény jogalkalmazói gyakorlatát használjuk fel, hiszen a tulajdonjoghoz hasonlóan, ahol egy dolgon több személy akár azonos, akár eltérő jogokat gyakorol (közös tulajdon, tulajdonos és haszonélvező, stb.), a szerzői jogban is előfordulhat, hogy egy művön több személy eltérő joga áll fenn.[249] Az osztatlan közös tulajdon esetében minden tulajdonos külön jogosult rendelkezni a dolog felett, ezért arra nézve a tulajdonostárs nem követhet el a lopást. A szerzői jogban azonban a különböző jogosultakat jellemzően nem egy mű köti össze, hanem különböző művek egymásra épülésével, összekapcsolásával keletkeznek, keletkezhetnek quasi újabb védett termékek, amelyek felhasználásával összefüggésben jöhetnek létre különböző jogviszonyok, amelyek fent említett vagyoni vonatkozásai kapnak szerepet a Btk. 329/A. és 329/B. §-ban.[250] Azaz az összekapcsolt művek szerzői elvileg elkövethetnek szerzői jogi bűncselekményt a közös műre nézve.

4.2.3. A közös jogkezelőkhöz kötött rendbeliség

A bevezetőben említett első álláspont szerint az egy közös jogkezelőhöz kötött jogosítás esetén – több mű esetén a folytatólagosságra is tekintettel – egy rendbeli bűncselekményt kell megállapítani. A műnek jogdíj fizetés nélkül folytatott nyilvánossághoz közvetítése esetén mindez praktikus lehet, hiszen egy adott időszakra vonatkozó zeneszolgáltatás esetén a lehetséges sértettek számának felderítése képtelenség – például egy közösség számára nyitva álló helyiségben elhelyezett rádión történő zeneszolgáltatás esetén –, és az ilyen esetben egyébként is átalány jogdíjat kell fizetni az Artisjus számára. Ezen álláspont másik részeként más jogkezelők érdekkörébe tartozó jogosítás esetén azonban annyi

[248] BÉRCZES L., GYENGE A. & LENDVAI Zs., *A szerzői jogi jogsértések esetén alkalmazható jogi eszközökről – Segédanyag a gyakorlat számára.* ASVA Budapest. 2005. p. 64. Elérhető: http://mek.niif.hu/03400/03428/03428.pdf [2011-07-31]

[249] A gyakorlat például egy rendbeli elkövetést állapít meg az osztatlan közös tulajdonban álló erdőterületről jogtalanul eltulajdonított fa tekintetében annak ellenére, hogy a cselekmény több személy jogát sértette.

[250] A dalszöveg írójának műve kiegészül a zeneszerző művével, amelyhez egy előadóművész saját zenei stílusában szintén szellemi alkotást ad hozzá egységes zenei terméket alkotva. Látszólag tehát egy műről van szó, valójában pedig három védendő szellemi tevékenységről.

rendbeli bűncselekményt kell megállapítani, ahány jogtulajdonos sértett vagyoni hátrányt szenved.[251] E kettősség egymás mellett működésének legnagyobb kerékkötője a sértettek számára alapított rendbeliség mellett hozható érvek erőssége és a kettős szempontrendszer következetlensége.[252] Tipikusan az illegális többszörözések esetében a rendbeliség jogkezelőnkénti meghatározásának helytelensége állapítható meg, amennyiben megvizsgáljuk a tényállás megfogalmazását. A Btk. 329/A. § (1) bekezdése szerint az követ el bűncselekményt, aki másnak a szerzői jogról szóló törvény alapján fennálló szerzői vagy ahhoz kapcsolódó jogát haszonszerzés végett, vagy vagyoni hátrányt okozva megsérti. A rendbeliség anyagi jogi szempontjából a közös jogkezelők által beszedett és visszaosztott jogdíj igénye nem saját, hanem a szerzői és szerzői joghoz kapcsolódó jogok jogosultjainak a szerzői jogi törvényen alapuló alanyi joga.[253] Ezért a rendbeliség kérdésében a szerzői jog által szabályozott és védett társadalmi értékek jogosultjainak a vagyoni igényei vonhatók a vizsgálat körébe és tekinthetők relevánsnak. A közös jogkezelők eljárásjogi szerepéről bővebben a következő címben írok.

4.2.4. Az „utolsó jogosult" személyére alapított rendbeliség

Ezen álláspont szerint a szerződéssel átruházott jogok esetén sértettnek az utolsó jogosult tekinthető, azaz a kiadó.[254] Indoka az, hogy az elkövető tudattartalma a jogellenes cselekmény kapcsán az előállító jogának sérelmét fogja át, valamint azt, hogy elsősorban és közvetlenül az utolsó előállító joga sérül.[255] A szerzők, az előadóművészek, valamint a hangfelvétel-előállítók a párhuzamosan fennálló terjesztési jogok gyakorlásának módját egymás között felhasználási szerződésekben rendezhetik ugyan a felhasználás hatékonysága, illetve a forgalmazás eredményessége érdekében úgy, hogy a terjesztés jogát a szerzőtől és az előadóművésztől is a hangfelvétel előállítója szerzi meg, és azt a továbbiakban – az üzleti forgalomban – kizárólagosan gyakorolja, azonban a láncolat valamennyi jogosultjának továbbra is fennálló jogdíjigényét mindez nem szünteti meg. Az eljárások során általában nem egyértelmű a sértetti pozíció, ezért az esetek többségében – többnyire célszerűségi okokból – a gyakorlat csupán a hangfelvételek előállítóit tekinti sértetteknek, ahogyan ezen álláspont például a BH1998.324. számú eseti döntésben is megjelenik.

4.2.5. Egy huszárvágás: mű és felhasználása

A hatályos szabályozás esetén a valós szerződéses kapcsolatok felderítését elkerülendő, és célszerűségi szempontból is a következő halmazati értelmezés volna kívánatos. A rendbeliséget mindig a konkrét eset körülményeinek ismeretében kell megállapítani a következő vezérlő elvek segítségével. A halmazat alapját a konkrét elkövetés során érintett műpéldány (az elkövetési tárgy) és a jogosulatlan felhasználás (elkövetési magatartás) együttesen képezi. A Btk. 329/A. § keretényállásként általában komplex, polgári jogi jellegű, szerződéses jogviszonyok megsértését rendeli büntetni, ekként a halmazati kérdésekben a büntetőjogi dogmatikai vagyon elleni bűncselekmények többségére

[251] DR. JÁVORSZKI T. & DR. RONGÁNÉ DR. SRAKTA I., A szerzői vagy szerzői joghoz kapcsolódó jogok megsértése bűncselekményének jogalkalmazási kérdései. *Ügyészek Lapja,* 2008/5. p. 37.
[252] A bírói gyakorlatot álláspontjával egyezik ez a nézet, amely megjelenik a BH 2001/307. és a BH 2002/301. számú eseti döntésekben is.
[253] Ami a közös jogkezelők saját igényét illeti – a működési költségüket fedező jogdíjrészlet – a szerzői jog által védett társadalmi érték szempontjából nem releváns, nem lehet a jogi tárgy eleme.
[254] Ezt a megfontolandó álláspontot képviseli Dr. Illés Irén: A szerzői és a szomszédos jogok megsértése bűncselekményének egyes kérdései című tanulmányában. Megjelent: Ügyészek Lapja, 1994. 6.
[255] VIDA, 2005. p. 19.

megszilárdult tételeit részben el kell hagynunk és a maga önálló alapjából kell felépítenünk az okszerű érvelést.

A fenti példámnál maradva, egy meghatározott zeneszám egészét érintő többszörözés természetes egységként egy rendbeli bűncselekmény megállapítására alkalmas a korábban részletezett jogosultak számára tekintet nélkül. A szerzői jogi értelemben vett felhasználás tulajdonképpen a mű egészének vagy valamely azonosítható részének érzékelhetővé tétele, szellemi szükséglet kielégítése.[256] Az összekapcsolt művek (zeneművek, filmalkotások) esetén e szükséglet – amely a korábban említett értékek megbontására sarkallja az elkövetőt – és a felhasználás mikéntje foglalja egységbe a különböző érdekeket.

A felhasználások fajtájától függően egy mű több, eltérő, engedély nélküli felhasználása – annak számától függően – több rendbeli bűncselekmény megállapítását vonja maga után a különböző irányú és jogalapú jogdíjfizetési kötelezettség miatt, amennyiben az elkövetés körülményei egymástól elkülöníthetők. Így például, ha a tettes ugyanazon zeneszámot engedély nélkül nyilvánosan előadja és ettől elkülönülten forgalmazás céljából többszörözi, akkor több rendbeli a bűncselekményt követ el, mivel a cselekmények más jellegű szükségletek kielégítését célozzák. Ugyanazon elkövető által egy zeneszám engedély nélküli, szabad felhasználás alá nem vonható többszörözése, majd jövedelemfokozás céljából történő lejátszása egy szórakozóhely közösség számára nyitva álló helyiségében ugyan két felhasználásnak minősül és kétrendbeli Btk. 329/A. § megállapítását indokolná, mivel a nyilvános előadás eredeti, kereskedelmi forgalomban megvásárolt zenei adathordozóval is elkövethető. Azonban a másolás – bár nem tekinthető szükséges eszközcselekménynek – a szabad felhasználás hatálya alól pontosan a nyilvános előadás – és nem magáncélú másolás – céljából történő többszörözéssel kerül ki, ezért a kettős értékelés tilalmába ütközne, azaz csak egy rendbeli a bűncselekmény. Viszont a zeneszám dalszövegének és dallamának külön-külön engedély nélkül történő felhasználása szintén halmazatot valósít meg, mivel ilyen esetben a jogosultak és maguk a művek is elkülönülnek és – a már említett – szükséglet is különbözik. Hasonlóképpen kell eljárni egy filmalkotás esetében, amikor a teljes filmet (mint egységes művet, amelyen több szerző joga áll fenn: rendező, forgatókönyvíró, zeneszerző) többszöröznek engedély nélkül, azaz ebben az esetben is egy rendbeli az elkövetés, azonban ha a filmzene mint különálló mű önálló, engedély nélküli felhasználása is megtörténik már több bűncselekmény valósul meg.

Nem a büntető törvénykönyvben, hanem a szerzői jogi törvényben található büntethetőséget kizáró okoknak számítanak a szabad felhasználás esetei, amelyek feltételeinek fennállása esetén a felhasználás jogellenességének hiánya miatt bűncselekmény elkövetése nem állapítható meg.

A felhasználások és a felhasznált művek számára alapozott eljárás megfelelő iránymutatásul szolgálna a már-már kaotikus jogalkalmazás számára a szerzői jogi bűncselekmények területén, mivel az ad hoc jelleggel hozott, következetlen döntések a jogbiztonság elvárásait gyakran feledtetik.

[256] LONTAI et al. p. 66.

4.2.6. De lege ferenda

Ami viszont a legmegfelelőbb megoldás lenne – és amelyre már megjelent a jogalkotói szándék[257] – az a tényállás olymódon történő módosítása, hogy az elkövetési magatartás a szerzői vagy szerzői joghoz kapcsolódó jogok kereskedelmi mértékű vagy üzletszerű megsértésére vagy eleve több jogosult jogsérelmére illetőleg több mű felhasználására vonatkozzon. Az üzletszerűség az alaptényállás elemeként törvényi egységet képez, ahogy a „más vagy mások szerzői vagy szerzői joghoz kapcsolódó jogának megsértése" kitétel alkalmazása is.

4.3. A büntetőeljárások alanyai: a sértett, képviselő, egyéb érdekelt

A sértett kilétének megállapításához az eddigi fejezetek már megfelelő alapot biztosítanak, azonban a sértett mellett a büntetőeljárás résztvevőjeként a Be. további két lehetséges személyt is megnevez, elsőként az egyéb érdekeltet, másodikként a képviselőt. Az 55. § (1) bekezdése alapján egyéb érdekelt az, akinek a jogára vagy a jogos érdekére a büntetőeljárásban hozott határozat közvetlen hatással lehet. Amennyiben a Be. nem ír elő személyes közreműködési kötelezettséget az eljárás során, akkor az 56. § (1) bekezdése alapján a sértett a jogait a képviselője útján is gyakorolhatja. Képviselőként azonban csak meghatalmazás alapján ügyvéd, nagykorú hozzátartozó, vagy külön törvényben erre feljogosított személy járhat el.

A gyakorlatban leginkább a zeneművek, szoftverek és filmalkotások illegális többszörözése kapcsán találkozik a jogalkalmazó a szerzői jogok megértésével, amely eljárásokban a szerzők legtöbbször nem vesznek részt, hanem a közös jogkezelő szervezetek közvetítésével kapcsolódnak a büntetőeljáráshoz. Ezek után a kérdés az, hogy a közös jogkezelő melyik szerepkörbe illeszthető be.

Az eljárási szereplők kérdésének alkotmányos büntetőjogi vonatkozása a jogorvoslathoz való alkotmányos jog. Az Alkotmány 57. § (5) bekezdése *alapján a Magyar Köztársaságban a törvényben meghatározottak szerint mindenki jogorvoslattal élhet az olyan bírósági, közigazgatási és más hatósági döntés ellen, amely a jogát vagy jogos érdekét sérti*. Az Alaptörvény XXVIII. Cikkének (7) cikke alapján *mindenkinek joga van ahhoz, hogy jogorvoslattal éljen az olyan bírósági, hatósági és más közigazgatási döntés ellen, amely a jogát vagy jogos érdekét sérti.* A büntetőeljárásban az eljárási szereplők személyének tisztázatlanul hagyása azzal járhat, hogy a hatóság megfoszthatja a tényleges jogosultakat a jogorvoslathoz való joguktól.

4.3.1. A sértett eljárásjogi szempontból

A közös jogkezelő szervezetek a jogosultak által létrehozott olyan szervezetek, amelyeknek a feladata a Szjt. 85. §-ának (1) bekezdése alapján a szerzői művekhez, az előadóművészi teljesítményekhez, a hangfelvételekhez, a sugárzott vagy vezetéken átvitt műsorokhoz, valamint a filmelőállítói és az adatbázis-előállítói teljesítményekhez kapcsolódó és a felhasználás jellege, illetve körülményei miatt egyedileg nem gyakorolható szerzői és szomszédos, illetve adatbázis-előállítói jogok érvényesítése, függetlenül attól, hogy azt a törvény írja elő, vagy az a jogosultak elhatározásán alapul.[258] A közös jogkezelő szervezetek szerzői jogi értelemben nem jogosultak, a jogdíjakat nem

[257] A kézirat lezárásakor a Btk. tervezetét a KIM előkészítette, de Magyarország Kormánya még nem tárgyalta meg.
[258] VIDA, 2005. p. 18.

saját jogon, hanem az általuk képviselt jogosultak nevében, azok számára szedik be. Az Szjt 92. § (2) bekezdése alapján a közös jogkezeléssel érintett díjigényekkel, valamint a megfizetett vagy beszedett díjakkal a jogosultak közötti felosztásukig a közös jogkezelő egyesület rendelkezik. A rendelkezés joga tehát átmeneti, időszakos, és származékos, szemben a szerző és a szomszédos jog jogosultjának folyamatos, alanyi jogával. Ugyan a bűncselekmény legtöbbször pontosan az elmaradt jogdíjfizetésben nyilvánul meg, és ebben az időszakában a jogdíjjal a közös jogkezelő jogosult rendelkezni, azonban e rendelkezési jog alapján mégsem tekinthető sértettnek, mivel ez nem abszolút jellegű jogosítvány, a jogdíj csak a megállapított felosztási rend szerint osztható szét a jogosítottak között, nem saját belátás szerint.

Az Szjt. 92. § (1) bekezdése alapján a nyilvántartásba vett közös jogkezelő, a közös jogkezelés körébe tartozó vagyoni jogok gyakorlása és bíróság előtti érvényesítése során a szerzői vagy szomszédos jog jogosultjának kell tekinteni. Vitatható, hogy ez a rendelkezés büntetőeljárásra alkalmazható lenne, hiszen a büntetőeljárásnak elsősorban nem a vagyoni jogok érvényesítése a célja, hanem a bűncselekmény felderítése, az elkövető felkutatása és felelősségre vonása. A büntetőeljárásnak csak járulékos kérdése a sértett polgári jogi – jelen esetben elmaradt hasznának –, vagyoni igényének érvényesítése. Ezek alapján a közös jogkezelő sértett nem lehetne, hacsak a jogdíjigényt nem értelmezzük jogos érdeknek. Bár ebben az esetben magyarázatra szorul az is, hogy egy érdek mitől lesz jogos, hiszen ha az érdek attól jogos, hogy a jog elismeri és kikényszeríthetővé teszi, akkor már joggá válik.[259] A Be. 58. (1) bekezdése sem oldja fel ezt a helyzetet, amikor úgy rendelkezik, hogy amennyiben a bűncselekménynek több sértettje van, maguk közül kijelölhetik a sértetti jogokat gyakorló természetes, illetőleg jogi személyt. Mivel a sértettek csak maguk közül választhatnak valakit, a közös jogkezelő újfent kiesik a választható személyek közül.

A korábbi fejezetek alapján sértettnek a szerzői jogi törvény szerzői és szomszédos jogi jogosultjai minősülnek. Az úgynevezett kisjogos jogosításokat érintő jogsértések esetén – amikor a felhasználás engedélyezése a közös jogkezelőkön keresztül történik, tipikusan a film- és zeneművek többszörözése, nyilvános előadása, stb. – ezek a jogosultak a büntetőeljárásokban jellemzően nem vesznek részt semmilyen formában, ide értem a szoftvereket érintő jogsértések miatt indult büntetőeljárásokat is. Az úgynevezett nagyjogos engedélyezés körébe tartozó jogellenes felhasználások esetén – például dramatikus zeneművek (operák, operettek, musicalek) egészének, részleteinek felhasználása előtt, vagy képzőművészeti alkotások kiállítása alkalmával közvetlenül a szerzőtől, jogutódjától vagy az őt képviselő ügynökségtől kell engedélyt kérni – az egyénileg jól behatárolható sértet vagy sértetti kör miatt a jogosult – helyesen – sértettként vesz részt az eljárásokban.[260]

4.3.2. Képviselő

Az adott büntetőeljárásra meghatalmazással nem rendelkező közös jogkezelő a Be. alapján csak külön törvényben erre feljogosított személyként járhat el. Mi lehet jelen esetben ez a külön törvény? Az Szjt. idézett 92. § (1) bekezdésének alkalmazása a büntetőeljárásban a fent említett okok miatt erősen vitatható. Az 58. § (3) bekezdése alapján, ha a

[259] BÓCZ E., Passzív alany, áldozat, sértett. *Rendészeti Szemle.* 2007/9. p. 120.

[260] Például: egy elismert magyar grafikus műveinek kiállítására a szerzővel (és adott esetben a műpéldány tulajdonosával) kötött szerződés alapján van helye, azonban ugyanezen már nyilvánosságra hozott műveknek naptárakban vagy csokoládécsomagoláson történő többszörözésre a közös jogkezelőnek fizetett jogdíj ellenében van lehetőség.

bűncselekménynek több sértettje van, vagy egyének pontosan meg nem határozható, nagyobb létszámú csoportja tekintendő sértettnek, a sértett képviselőjeként a közhasznú szervezetekről szóló törvény hatálya alá tartozó olyan szervezet is eljárhat, amelyet sértettek vagy sértettek egyes csoportjainak érdekképviseletére hoztak létre. Vida József álláspontját elfogadva az egyes jogkezelő szervezetek alapszabályának vizsgálata után megállapítható, hogy a közös jogkezelő szervezetek ma sem felelnek meg maradéktalanul a fenti követelményeknek. Következésképpen jelenleg sincs hatályban olyan törvény, amely feljogosítaná a közös jogkezelőket a büntetőeljárásban történő képviselői fellépésre.

4.3.3. Egyéb érdekelt

A három említett szereplő közül csak az egyéb érdekelt marad. A büntetőeljárásban hozott határozat a közös jogkezelő szervezet jogára, jogos érdekére közvetlen hatással lehet, így a kérdésre a válasz adott. A közös jogkezelők a jogkezelésükbe tartozó szerzők vagy szomszédos jogok jogosultjainak vagyoni igényeinek megsértése esetén a büntetőeljárásban egyéb érdekeltként vehetnek részt. Természetesen amennyiben az eljárás a közös jogkezelő feljelentése alapján indul, az eljárásban feljelentőként is rendelkezik külön eljárási jogokkal.

4.4. A dogmatikai anomáliák összefoglalása

A jelenlegi gyakorlat szerint a szerzői vagy szerzői jogot sértő bűncselekmények esetén nem tisztázott egyértelműen az, hogy az eljáró hatóságok kit tekintenek sértettnek. A fejezet első részének megalapozott jogszabályi hivatkozásai alapján egyértelműen kijelölhetők ugyan a sértetti pozíció lehetséges szereplői és a közös jogkezelők fellépésének formája egyéb érdekeltként, azonban mindez nem tekinthető megfelelően rendezettnek. Az ideális eset az volna, ha a Be. képviselőkre vonatkozó rendelkezéseit olyképpen fogalmazná át a jogalkotó, hogy abba a közös jogkezelő ipso iure be tudjon illeszkedni, vagy egyfajta törvényi képviselőként, egyértelműen sértetti jogok gyakorlásával ruházná fel e szervezeteket.

A rendbeliség kérdésében a szerzői jogi szabályozás a vagyon elleni bűncselekményekre kialakult büntetőjogi dogmatika alkalmazhatatlan. A szellemi alkotások jogának sajátságos felépülése miatt az egymással párhuzamos jogok megsértésével megállapítható halmazat alapjaként a mű és annak felhasználása volna kívánatos. A sértettek számához ragaszkodó elméletek elfogadásával a tényállás hiánytalan, valóságnak megfelelő felderítésének kötelezettsége a hatóságot aránytalan munkateherrel sújtaná.

A fejezet mellőzte az egyes tényállások elemzése során az elkövetők differenciálását, így az internetes elkövetések során értékelhető szerepet játszó internetszolgáltatók (ideértve a közvetítő-, tárhely- vagy tartalomszolgáltatókat egyaránt) cselekvőségéről nem esett szó. Ezen mulasztás oka, hogy a büntetőjogi elkövetők témaköre dogmatikailag már tisztázott, konkrét esetben az egyedüli vizsgálandó kérdés, hogy van-e az adott körülmények között olyan személy (ide értve a jogi személyt és annak képviselőjét is), aki szándékosan valamely tényállási elemet megvalósított, vagy ahhoz másnak szándékosan segítséget nyújtott. A dolgozat célja szempontjából – amely az alkotmányos büntetőjog elveinek érvényesülése az egyes tényállások esetén – ezen kérdés megválaszolása csak konkrét ügyben és konkrét személy tudattartalmának vizsgálata után lehetséges, egyébként irreleváns.

VII. FEJEZET: ZAKLATÁS, STALKING, CYBER-STALKING (BTK. 176/A. §)

A Büntető Törvénykönyv újabb, korábbi szabályozási múlttal nem rendelkező bűncselekményi tényállásai közül a zaklatás vétségének 176/A. § (1) bekezdésébe valamint a (2) bekezdés a)-b) pontjaiba foglalt fordulatai 2008. január hó 1. és 2009. február hó 1. napján léptek hatályba. Ám amíg a (2) bekezdés a) pontja egy azelőtt szabálysértésként szankcionált magatartást emelt bűncselekményi szintre, addig a b) pont és az (1) bekezdés teljesen új tényállásoknak tekinthetők, a bennük leírt cselekményt büntetőtörvény hazánkban eddig még nem rendelte büntetni.

Mivel új, magyar büntetőjogi hagyományokkal nem rendelkező tényállásokról van szó, értelmezésük jogalkalmazói gyakorlata idő hiányában nem alakulhatott ki, ekként mindennapi alkalmazásuk eleve számos problémát teremtett. Ehhez társul a zaklatásnak az ember kommunikációs tevékenységhez fűződő szoros kapcsolata, valamint az infokommunikációs eszközökkel telített mindennapi környezet, amely körülmények megnehezítik a zaklatás jogi tárgyának, a magánéletnek a definiálását. Az értekezés általános részében ismertetett devianciák és a magánszférához fűződő viszony változása tovább bonyolítja egy-egy zaklató cselekmény büntetőjogi megítélését. A fejezet célja éppen ezért – a tényállások értelmezése mellett – ezen értelmezési nehézségek ismertetése.

1. A ZAKLATÁS TÍPUSAI ÉS HÁTTERE

1.1. A zaklató magatartások általában

A jogilag tilalmazott zaklatásnak több formája létezik, ezért a zaklató magatartásoknak eltérő csoportosítása lehetséges az elkövetés helye, az elkövető indítéka, célja és célpontja alapján. Beszélhetünk munkahelyi, szexuális, faji, etnikai alapú, és úgynevezett személyes indíttatású zaklatásról. Utóbbin belül a szakirodalom leginkább három megnyilvánulási formával foglalkozik: a családon belüli erőszakkal, a híresség eket érintő „határok nélküli" pszichoterrorral, valamint a homoszexuális, még inkább a leszbikus kapcsolatokban megjelenő szerelemféltésekből fakadó zaklatással.[261]

A munkahelyi, szexuális zaklatók célja – magától értetődő módon – irányulhat szexuális kapcsolat létesítésére, ám egyes szerzők szerint az elkövetők motivációja a férfiak azon félelméből is fakadhat, hogy pozíciójuk veszélyeztetését látják a nők emancipált viselkedésében.[262] Nemzetközi vonatkozásban a munkahelyi, szexuális zaklatás leküzdésére többek között az Európai Közösségek Bizottságának 1991. november 27-én kiadott, 92/131 (EGK) számú, a nők és a férfiak személyiségi jogainak munkahelyi védelméről szóló ajánlása hívta fel a figyelmet. Az Európai Parlament és a Tanács közös, a férfiak és nők közötti egyenlő bánásmód elvének a munkavállalás, a szakképzés, az előmenetel és a munkakörülmények terén történő végrehajtásáról szóló 76/207/EGK tanácsi irányelv módosításáról szóló 2002/73/EK irányelve tartalmazza a diszkriminációval és a (szexuális) zaklatással kapcsolatos legújabb rendelkezéseket. Ettől elkülöníthető az Európai Tanács 2000. június 29-én elfogadott, 2000/43/EK számú, a személyek közötti, faji- vagy etnikai származásra való tekintet nélküli egyenlő bánásmód elvének alkalmazásáról szóló irányelv által említett etnikai, faji alapú zaklatás.[263]

---

[261] KORINEK B., A stalking és a családon belüli erőszak. *Családi Jog*, 2005/1. p. 33.
[262] THUN É., A szexuális zaklatás mint társadalmi jelenség. *Belügyi Szemle*, 2000. 4-5. szám pp. 14-23.
[263] BTK. Kommentár - COMPLEX

A dolgozat szempontjából lényegesebb a harmadik típusú zaklatás – idegen szóval stalking[264] –, amely kifejezetten személyes jellegű, és amelynek elkövetője jellemzően hosszabb idő óta, folyamatosan vagy visszatérően molesztálja áldozatát, nem feltétlenül szexuális indíttatásból. Ennek egyik leggyakoribb színhelye az infokommunikációs környezet, az internet és mobilkommunikáció.

1.2. A „stalking"

A stalking kifejezés által jelölt zaklató magatartások meghatározására számos definíció született azokban az államokban, ahol már évtizedekkel ezelőtt felismerték e viselkedés társadalomra veszélyességét. J. Reid Meloy szerint a stalking fogalma az USA-ban szinte államonként változik, azonban három fogalmi elemet mindig tartalmaz. Ezek az alapelemek a következők: a) másra irányuló, nem kívánt, háborgató viselkedés, amely b) burkoltan vagy kifejezetten fenyegető, és c) amelynek hatására a megfenyegetett komoly félelmet érez. A stalking pszichiátriai-klinikai értelemben meghatározott személy rendellenes vagy tartós fenyegetése vagy nyugtalanítása.[265] Kalifornia állam büntetőjogi szabályai alapján a „stalking"-ot elköveti, aki mást szándékosan[266], tartósan követ vagy zaklat, és akinek e komoly, fenyegető magatartásával célja másban azon érzetet keltése, hogy saját vagy hozzátartozóinak biztonsága veszélyben van.[267] Rhonda Saunders szerint[268] a vádlónak a következőket kell bizonyítania: a) az elkövető tudatos szándékkal mást tartósan követ vagy zaklat, b) az elkövető komoly fenyegetést tanúsít magatartásával, c) az elkövető viselkedésének az a célja, hogy más a saját vagy hozzátartozójának biztonságáért aggódjon. A tartós, ismétlődő elkövetés megállapításához legalább két ilyen eset szükséges. „A megalapozott fenyegetést *(credible threat)* nem csak szóbeli vagy írásbeli alapú kommunikáció, hanem egyéb más cselekedet vagy mindezek kombinációja is közvetítheti. Kiemelendő a zaklatás viszonylagos volta, azaz az egyes cselekmények és kijelentések mindig valamely konkrét szituációhoz kötve értelmezendők.[269] Akkor tekinthetünk egy fenyegetést komolynak, amennyiben egy ésszerűen gondolkodó személyben komoly félelmet kelt, ha az áldozat hitt abban, hogy az elkövető valóban beváltja fenyegetéseit, vagy a fenyegetés ténylegesen jelentős érdeksérelemmel járt. Ehhez az szükséges, hogy az áldozat tudomást szerezzen a fenyegetésről, amely megvalósulhat közvetve, és harmadik személyen keresztül is."[270] Bran Nicol az USA államainak szabályaihoz hasonló brit jogszabályok elemzése során mindezt azzal egészíti ki, hogy a zaklatásnak nem kell kizárólag az áldozatra korlátozódnia, hanem érintheti annak barátait, családtagjait, háziállatait, tulajdonát, és az elkövetőnek tudnia kell, hogy cselekményével félelmet kelt, vagy mást háborgat.[271] Az Amerikai Egyesült Államokbeli törvényi és tudományos fogalmat összegezve Korinek Beáta szerint a „stalking olyan viselkedési

[264] A stalking angol kifejezés, magyar jelentése: vadásznyelven a vad hajtása, üldözése, kifárasztása.
[265] MELOY, J. R., The Psychology of Stalking. In. MELOY, J. R. (ed.), *The Psychology of Stalking Clinical and Forensic Perspectives*, Academic Press London, 1998. pp. 2-3.
[266] Az angol „maliciously" kifejezés magába foglalja a bűnös, rosszakaró szándékot is.
[267] SAUNDERS, R., The Legal Perspective on Stalking. In. MELOY, J. R. (ed.), *The Psychology of Stalking Clinical and Forensic Perspectives*, Academic Press London, 1998. p. 31.
[268] SAUNDERS, 1998. pp. 31-32.
[269] A szerző által hivatkozott példa a következő. Az áldozat egy levelet kap az elkövetőtől, amelyben azt írja, hogy „Szeretlek", de a borítékba mellékel egy pisztolygolyót is.
[270] SAUNDERS, 1998. p. 32.
[271] NICOL, B., *Stalking*. Reaktion Books Ltd, 2006. pp. 24-25.

tünetegyüttes, aminél a zaklató meghatározott személyre viselkedésével úgy hat, hogy fenyegetéssel belőle félelmet, szorongást vált ki".[272]

1.3. Az elkövetők és motivációik

Meloy csoportosítása alapján, az elkövetők motivációja szerint megkülönböztethetünk instrumentális és expresszív fenyegetéseket. Az első esetben a stalker tudatos, vagy tudat alatti szándékból követi el a zaklatást, akár spontán vagy a lehető legnagyobb hatás elérése érdekében az elkövetést alaposan eltervezve. Ilyen szándék lehet az áldozat irányítása, uralása, megfélemlítése, elcsábítása, vagy az áldozat arra kényszerítése, hogy tegyen valamit. A második esetben az ösztönös, érzelmek táplálta fenyegető cselekményekkel az elkövető célja saját indulatainak szabályozása. Ezek a cselekedetek elsősorban nem célzatosak, mint az előző típusú fenyegetések, inkább egyfajta belső lélektani célt szolgálnak annak ellenére, hogy mindez az áldozatra negatívan hat.[273]

Nicol szempontjai szerint elkülöníthető egyrészt a megszakadt kapcsolaton, másrészt a vágyott kapcsolaton alapuló, harmadrészt a nem bensőséges kapcsolatot keresők által elkövetett zaklatás. Nicol szerint a megszakadt kapcsolaton alapuló teszi ki a zaklatások többségét. Ebben az esetben a zaklató és az áldozata között korábban bensőséges viszony volt, ami utóbb megszakadt. Ezen a csoporton belül is elhatárolhatunk három alcsoportot. Az első esetben az egyik fél megszakítja kapcsolatát a másik féllel, aki ezután azért kezdi el őt molesztálni, hogy visszakényszerítse magához, vagy éppen megbüntesse. A másik alcsoportba tartoznak a munkahelyi zaklatások, amelyek során egy volt alkalmazott azért zaklatja a felettesét, mert őt hibáztatja munkahelyének elvesztéséért, vagy munkatársát, mert közelebb akart kerülni hozzá, de az visszautasította. A harmadik alcsoportba tartoznak a megszakadt szakmai kapcsolatokban kialakuló zaklatások, amelyek során a felek korábban például tanár-diák, orvos-beteg, vagy pszichológus-páciens viszonyban voltak, de ez a viszony megszakadt. A megszakadt kapcsolaton alapuló zaklatások elkövetőinek motivációja lehet egyrészt, hogy a másik fél meggondolja magát, másrészt a másik fél megleckéztetése. A vágyott kapcsolaton alapuló zaklatások esetén a zaklatónak és áldozatának korábban nem volt semmilyen bensőséges kapcsolata egymással, kapcsolatuk egyedüli formája pusztán a zaklatás maga. Ebben az esetben az elkövető célja, hogy a kiszemelt fél valamilyen formában elismerje őt. A zaklató magatartása rendkívül hosszantartó, legtöbbször levelek írogatásában, vagy másféle kommunikációban merül ki, amely kapcsolatfelvételek során a zaklató abban a tévhitben mutatja ki érzelmeit, vágyódását, hogy a vágyott személy ezen kinyilatkoztatások hatására viszonozni fogja érzéseit. Mivel az elkövetők úgy udvarolnak, hogy az udvarlás általánosan elfogadott szabályait figyelmen kívül hagyják, közeledésük gyakran ijesztő.

Az elkövetők gyakran szenvednek skizofréniában vagy mániákus depresszióban, szociálisan egyedülállók, akiknek soha nem volt mással bárminemű komolyabb viszonya. Az elkövetők legtöbbször nők, jellemző rájuk, hogy gyakran fantáziálnak a vágyott személlyel kialakított közeli kapcsolatról, vagy abban a hitben vannak, hogy a másik fél ugyanazt érzi, mint ők. A sértettek legtöbbször az elkövetőnél idősebb férfiak, akik társadalmi és vagyoni viszonylatban magasabb rangot töltenek be. A harmadik csoportba a nem bensőséges kapcsolatot kereső zaklatók tartoznak, akik semmiféle intim kapcsolat létrehozására nem törekednek az áldozattal, hanem céljuk annak valamely vélt vagy valós

[272] KORINEK B., A stalking. In. Korinek L., Kőhalmi L. & Herke Cs. (ed.), *Emlékkönyv Irk Albert egyetemi tanár születésének 120. évfordulójára*. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs p. 118.
[273] MELOY, 1998. p. 8.

sérelem miatti megbüntetése. A sértettek legtöbbször ismerik az elkövetőt, aki úgy gondolja, hogy áldozata rossz hírét keltette, valamiféle igazságtalanságot tett vele. Az elkövetők nem pusztán bosszúra törekednek, hanem tettükhöz igazolás is keresnek. A sértettek által nem ismert olyan „ragadozó", szociopata elkövetők is e csoportba tartoznak, mint a sorozatgyilkosok, erőszakos közösülők, stb.[274] Összegezve az eddigi tapasztalatokat a legtöbb zaklatás esetében megállapítható, hogy az elkövető és a sértett között valamilyen kapcsolat áll vagy állt fenn (volt partner, munkatárs, terapeuta), ezért gyakori, hogy az elkövető már a kapcsolatuk fennállása alatt is molesztálja áldozatát.

2. A ZAKLATÁS SZABÁLYOZÁSA

2.1. A zaklatás megjelenése a Btk-ban

Hazai viszonylatban korábban egyedül az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról szóló 2003. évi CXXV. törvény említette a zaklatást, az egyenlő bánásmód követelményét, az emberi méltóságot sértő, szexuális vagy egyéb természetű magatartásnak tekintve azt, amelynek célja vagy hatása valamely személlyel szemben megfélemlítő, ellenséges, megalázó, megszégyenítő vagy támadó környezet kialakítása. A törvény szerint mindez csak bizonyos jogviszonyban érvényesülhet, így nem biztosít megfelelő védelmet a kifejezetten személyes indíttatású zavaró magatartásokkal szemben, a családjogi és a hozzátartozók közötti viszonyokat pedig kifejezetten kizárja a törvény hatálya alól.[275]

A zaklatás büntetőjogi fenyegetettségének bevezetésével a jogalkotó célja azon súlyosabb jogsértések pönalizálása, amelyek más személy rendszeres vagy tartós háborgatását eredményezik, és amelyek jogviszonytól függetlenül jelentős érdeksérelmet okoznak a magánéletbe való önkényes beavatkozással. A zaklatás tényállásait bevezető törvény indokolása szerint általános tapasztalat, hogy „a zaklató magatartása az idő múlásával általában egyre fenyegetőbb, durvább lesz, ami súlyos pszichés zavarokat okozhat, de adott esetben akár tulajdon vagy személy elleni erőszakos bűncselekmények elkövetéséhez is vezethet", többek között ezért is volt indokolt és régóta kívánatos a tényállás megalkotása.[276] Ezt az aggodalmat sajnálatos módon alátámasztják azok a magyarországi jogesetek is, amelyekben a sértettek halálát okozó elkövető tette előtt kitartóan zaklatta áldozatát, de törvényi tényállás hiányában nem lehetett felelősségre vonni.[277]

A 2008. január hó 1. napjától hatályos tényállást a Büntető Törvénykönyv 176/A.§-aként, az egyes büntető jellegű jogszabályok módosításáról szóló 2007. évi CLXII. törvény 4. §-a vezette be „Zaklatás" címmel. A tényállás címe már önmagában véve is pejoratív jellegű magatartásra utal, magába foglalva az alkalmatlankodva, sürgetve, gyakran mások zavarását és háborgatását, a pszichésen ható, huzamosan nyugtalanító, lelkileg gyötrő magatartást.[278] A 2008. évi LXXIX. törvény a Btk. 176/A. § (2) bekezdését módosította, egy újabb elkövetési magatartással bővítve a zaklatás tényállásait.

---

[274] NICOL, 2006. pp. 25-28. A szerző Paul E. Mullen, M. Pathé és R. Purcell Study of Stalkers című művére hivatkozik.
[275] 2003. évi CXXV. törvény 6. §-a (1) bekezdésének a)-b) pontjai
[276] Complex DVD Jogtár kommentár a Btk. 176/A.§-hoz
[277] KORINEK B., A stalking. In. Korinek L., Kőhalmi L. & Herke Cs. (ed.), *Emlékkönyv Irk Albert egyetemi tanár születésének 120. évfordulójára*. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs pp. 124-129.
[278] HVG-ORAC kommentár a Btk. 176/A.§-hoz

2.2. A zaklatás jogi tárgya

Az elsőként felmerülő kérdés az, hogy mely társadalmi viszony, érték védelme érdekében volt szükség a büntetőjogi tényállás megalkotására. Ez a társadalmi érték a magánszféra, a magánélet[279] szentsége. Nemzetközi dokumentumok igen, a magyar alkotmány viszont nem nevesíti önálló alapjogként a magánélet sérthetetlenségéhez fűződő jogot, azonban az Alaptörvény rendelkezése alapján a következő nemzetközi egyezmények Magyarország jogrendszerére nézve kötelező erővel bírnak. A Polgári és Politikai Jogok Nemzetközi Egyezségokmánya szerint „Senkit sem lehet alávetni a magánéletével, családjával, lakásával vagy levelezésével kapcsolatban önkényes vagy törvénytelen beavatkozásnak, sem pedig becsülete és jó hírneve elleni jogtalan támadásnak." Az Emberi Jogok Európai Egyezményének 8. Cikke szerint „Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák." Az idézett nemzetközi dokumentumok alapján tehát mindenkinek joga van a magánélethez, azonban azt nem határozzák meg, hogy pontosan mit tekinthetünk magánéletnek. Az Alaptörvény önállóan nevesített jogként tehát nem szól a szűk értelemben vett magánéletről, tágabb viszonylatban azonban jelzi, hogy felöleli a magánlakás, a magántitok, a jó hírnévhez való jogot és az információs önrendelkezési jogot (adatvédelmet).

Az 56/1994. (XI. 10.) AB határozat szerint „az Alkotmánybíróság felfogásában az emberi méltósághoz való jog az ún. „általános személyiségi jog" egyik megfogalmazása, azaz a személyiségi jogok „anyajoga", amely a modern alkotmányokban, illetve alkotmánybírósági gyakorlatban a „személyiség szabad kibontakozásához való jog", az „önrendelkezés szabadságához való jog", „általános cselekvési szabadság", továbbá a „magánszférához való jog" elnevezésekkel szerepel [8/1990. (IV. 23.) AB határozat]. A „magánszférához való jogot" az alkotmány konkrét, szubjektív alapjogként nem nevezi meg, de a magánélet szabadságához való jog kétségkívül az egyén autonómiájának, védelmére szolgáló olyan alapjog, amely az ember veleszületett méltóságából ered, amelynek tehát az általános személyiségi jog – az emberi méltósághoz való jog – szubszidiárius alapjoga. A magánszférához való jog, az önmegvalósítás joga, a személyiség szabad kibontakozása és az autonómia védelme megköveteli az alkotmány 8. § (1) bekezdésében írt szempontok érvényesülését, azaz azt, hogy az állam az ember sérthetetlen és elidegeníthetetlen alapvető jogait tartsa tiszteletben és védelmezze".

2.3. A magánszféra fogalma az információs társadalomban

Miután meghatároztam a zaklatás jogi tárgyát, az újabb feladat annak definiálása, hogy mit is értünk magánszféra alatt. A magánszférával rokon, angolszász eredetű fogalom, a privacy. A privacy tartalmának meghatározására többen tettek már kísérletet, mindezek maradéktalan felsorolását mellőzve a következő definíciós próbálkozásokat tartom érdemesnek kiemelni. Alan Westin értelmezése szerint a privacy az egyének, csoportok és közösségek azon igénye, hogy meghatározzák mikor, hogyan és milyen információkat közölnek önmagukról másoknak.[280] Ennek pszichológiai szintjén a privacy a kísérletezés és az önértékelés biztosításán keresztül teremti meg az egyéniség fejlesztésének lehetőségét.[281] Westin szerint a privacy négy fő funkciója 1) az egyéni autonómia, amely az egyéniség fejlesztésének és mások általi befolyásolástól való függetlenség igényével lép

[279] A továbbiakban a két fogalmat egymás szinonimájaként használom.
[280] WESTIN, A., *Privacy and Freedom*, New York, Atheneum, 1967.
[281] JOINSON, A. N. & PAINE, C. B., Self-disclosure, privacy and the Internet. in: In. Joinson, A., McKenna, K., Postmes, T. & Reips, U-D. (ed.), *The Oxford Handbook of Internet Psychology*, Oxford University Press, 2007. p. 243.

fel, 2) az érzelmi szabadság, amely biztosítja a mindennapi élet feszültségeinek feloldását, a pihenést, 3) az önértékelés, amely az egyéniség, a történések és a tapasztalatok egységét teremti meg, 4) végül a korlátozott és védett kommunikáció, amely a személyes információk bizalmi alapon történő megosztását és személyes kapcsolatok létrehozását jelenti.[282]

Altman szerint a privacy az „én"-hez való hozzáférés engedélyezésének megválasztását jelöli, és úgy gondolja, hogy mindez a közösségi interakciók szabályozásán keresztül érhető el, amely viszont biztosítja a külvilággal való kapcsolat kezelését és végső soron az önmeghatározást.[283] Kérdésként merül fel, hogy milyen vonatkozásai vannak az infokommunikációs eszközökkel zajló interakcióknak a privacyra? Egyrészt a személyes információk megítélése az egyik legjelentősebb etikai problémakör az információs társadalomról szóló diskurzusokban. A felhasználók online lépései már nem pusztán cselekmények, hanem adatok, amelyek birtokolhatók, felhasználhatók. Másrészt a magánélet színterei quasi újabb életterekkel bővültek, a hálózati lét, az online közösségi élet szintén a privacy körébe vonható.

Tekintettel arra, hogy a zaklatás tényállásának értelmezéséhez a hazai jogirodalomból még hiányoznak az eligazító, a jogalkalmazóknak megfelelő segítséget nyújtó források, a magánszféra (magánélet) fogalmának megértéséhez a fent említett rokon jogterület, az adatvédelem „privacy"-fogalomkörét hívtam segítségül. Jóri András Ferdinand D. Schoemann és Alan Westin kutatásaira hivatkozva többek között olyan állapotként értelmezi, amelyben „az egyénhez – a hozzá kapcsolódó információkhoz, életnek intim tényeihez, gondolataihoz és testéhez – való hozzáférés korlátozott".[284] Jelentheti az „én" és a „mások" viszonyrendszerében az egyén általános cselekvési szabadságát.[285] Lehet olyan abszolút szerkezetű viszonyrendszer, amely kizárólagos rendelkezést biztosít jogosultja számára a benne foglaltak felett. Majtényi László szerint a „személyes privacy védelme elsődlegesen az ember magánvilágának védelmét jelentette, amibe rendszerint beleértették a védettséget a háborítatlan magán- és családi életre, a fizikai és lelki integritásra, a becsület védelmét, a jó hírnév védelmét, a mentességet a magánélet tényeinek feltárásával szemben, a személyes identitás védelmét, mentességet a megfigyeléstől, a levelezés, a szóbeli közlések védelmét…".[286] A magánszféra – idegen szóval privacy – fogalmának tehát számos megközelítése lehetséges, a kifejezés az egyén önrendelkezési jogának egyre erősebb kibontakozásával párhuzamosan újabb és bővebb tartalmakat nyert.

A magánszféra, magánélet rendszerének fogalma a fent kifejtettek alapján is több értelmezési szintet foglalhat magába, ezért a zaklatás tényállása szempontjából a magánszféra rendszerének három alapelemből való felépítését látom helyesnek.[287] A magánszféra, magánélet felöleli:

> a) az egyedülálló egyént (az előbbiek alapján a hozzá kapcsolódó információkhoz, életnek intim tényeihez, gondolataihoz és testéhez való hozzáférést, jogát a fizikai és lelki integritásra, a becsület védelmét, a jó hírnév védelmét, a mentességet a magánélet tényeinek feltárásával szemben, a személyes identitás védelmét, mentességet a megfigyeléstől, a levelezés, a szóbeli közlések védelmét),

[282] JOINSON & PAINE, 2007. p. 243.
[283] ALTMAN, I.: *The environment and the social behavior*. Monterey, CA: Brooks/cole, 1975. p. 24.
[284] JÓRI A., *Adatvédelmi kézikönyv.* Osiris Kiadó, 2005. p. 12.
[285] JÓRI A., *Adatvédelmi kézikönyv.* Osiris Kiadó, 2005. p. 15.
[286] MAJTÉNYI L., *Az információs szabadságjogok.* Complex Kiadó, 2006. p. 68.
[287] SZATHMÁRY Z., Gondolatok a zaklatásról. *Magyar Jog*, 2009/12. pp. 726-734.

b) az egyénnek családjára vagy háztartására kiterjedő kapcsolatrendszerét, és

c) az ennél nagyobb, önkéntes választásán alapuló társasági viszonyrendszerét, ide értve az online közösségi életét is.

A magánszféra háromszintű rendszerének felfogása esetén a háborgató cselekmények is az imént felsorolt rendszerelemek, rétegek valamelyikén keresztül avatkozhatnak be a sértett teljes magánéletébe.

2.3. A zaklatás a magánszféra védelmének rendszerében

A legtöbb társadalomban vannak olyan jogi és nem jogi normák, amelyek a magánszférára vonatkoznak, ám ezek a normák viszonylag új vívmányok, Jóri András szerint hiányoznak a múlt és a jelen primitív társadalmaiból.[288] A magánszféra mai, összetett jogi védelmének alkotóelemei több jogágon, számos jogintézményen keresztül biztosítják az emberi méltóságból eredeztethető háborítatlan magánélethez fűződő jogot. Ilyen jogi normák – a teljesség igénye nélkül – az adatvédelem, az információs önrendelkezés jog alkotmányos védelmének normái, vagy a polgári-, közigazgatási- és büntetőjognak a becsület, a magánlakás, a magán- és levéltitok védelmére vonatkozó szabályai is. A Btk-ban tehát eddig is voltak a magánszférát sértő cselekményeket szankcionáló tényállások - így például a becsületsértés, rágalmazás, magánlaksértés, az adatvédelmi és titoksértési bűncselekmények -, amelyek a fent körvonalazott magánszféra egy-egy rétegét sértő magatartásokat rendelik büntetni. Az egyéni önrendelkezési jog felértékelődése miatt a számos „klasszikus" jogszabályi garancia mellett e komplex jogvédelem legújabb elemei, a Büntető Törvénykönyv 2008. január 1. napjától, majd a módosítások révén 2009. február hó 1. napjától hatályos tényállása, a zaklatás.

A zaklatás jogi tárgya a magánszféra – magánélet fogalmáról szóló részben kifejtettek alapján az emberi méltósághoz, a magánszféra tiszteletben tartásához fűződő jog, ebből következően a jogalkotó a tényállást a szabadság és az emberi méltóság elleni bűncselekmények között helyezte el büntető törvénykönyvben. Személyes jellegére tekintettel – a rágalmazáshoz és becsületsértéshez hasonlóan – magánindítványra üldözendő bűncselekmény, azaz büntetőeljárás csak a jogosult feljelentése alapján indulhat.

Egy cselekmény büntetőjogi tilalmazásának alapja a cselekmény társadalmi viszonyokat, értékeket támadó (sértő vagy veszélyeztető) jellege. A jogalkotó miután felismeri egy cselekmény társadalomra veszélyességét és annak olyan fokát, hogy bűncselekményként való szabályozásáról dönt, a cselekmény olyan generális ismérveit gyűjti össze, amelyekből megalkotható maga a törvényi tényállás. A zaklatást a hétköznapi életben talán könnyű felismerni, a jog számára viszont sokkal nehezebb a releváns jellemzők megragadása. A továbbiakban a tényállást elemezve azt vizsgálom, hogy mennyire sikerült szavakba önteni és a törvényi tényállásba egyesíteni ezen releváns tényeket.

3. A ZAKLATÁS ELKÖVETÉSI MAGATARTÁSAI

3.1. Az (1) bekezdéses zaklatás

A Btk. 176/A. §-a zaklatásnak három fordulatát tartalmazza. Az (1) bekezdésbe ütköző zaklatás vétségét az követi el, aki „abból a célból, hogy mást megfélemlítsen, vagy más

[288] JÓRI, 2005. p. 15.

magánéletébe, illetőleg mindennapi életvitelébe önkényesen beavatkozzon, rendszeresen vagy tartósan mást háborgat, így különösen mással, annak akarata ellenére telekommunikációs eszköz útján vagy személyesen rendszeresen kapcsolatot teremteni törekszik, ha súlyosabb bűncselekmény nem valósul meg". Az (1) bekezdés szerinti zaklatás vétségének elkövetési magatartása tehát más személy rendszeres vagy tartós háborgatása. A zaklató cselekmények eltérőek lehetnek, amelyeket összefoglaló néven, háborgatásként fogalmaz meg a törvény. Ezek közül az egyik legtipikusabb, a hétköznapi életben leggyakrabban előforduló eset, amikor az elkövető telekommunikációs eszköz útján[289] vagy személyesen törekszik rendszeres kapcsolatteremtésre. Tehát nem szükséges a kapcsolatnak létrejönnie, a törvény szerint elegendő az erre irányuló törekvés. Azaz megvalósítja a zaklatást, aki rendszeresen, zavaró módon „megcsörgeti" a sértett telefonját, majd azonnal bontja a vonalat, úgyszintén az is, aki kommunikáció nélkül a sértettet zavarva liheg, nyög a telefonban. Az elkövetési magatartásként megjelenő „háborgat" kifejezés a zaklatás szinonimája, olyan gyűjtőszó, amely quasi nyitott törvényi tényállást teremtve felölel minden olyan magatartást, amely más magánéletének, mindennapi életvitelének megzavarására alkalmas, a magánszféra sérelmét „eredményezheti". Más rendszeres követése, a családi otthon előtti rendszeres várakozás, vagy ajándékok küldözgetése is adott körülmények között a háborgatás megállapítására alkalmas lehet. A bűncselekmény célzatos, tehát csak akkor tényállásszerű az elkövető magatartása, ha a háborgatással célja, hogy a sértettet megfélemlítse, vagy magánéletébe, illetőleg mindennapi életvitelébe önkényesen beavatkozzon. Az elkövető más magánéletébe történő beavatkozási szándékának önkényessége azt jelenti, hogy az nélkülöz mindennemű jogszabályi vagy sértetti jóváhagyást, felhatalmazást. A tényállásszerűség további feltétele, hogy a háborgatás rendszeresen vagy tartósan történjen.

3.2. A (2) bekezdés a) pontja, a „veszélyes fenyegetés"

A (2) bekezdés a) pontjába ütköző zaklatás vétségét az követi el, aki „félelemkeltés céljából mást vagy rá tekintettel hozzátartozóját személy elleni erőszakos vagy közveszélyt okozó büntetendő cselekmény elkövetésével megfenyeget". E cselekmény elkövetőjét 2008. január hó 1. napja előtt veszélyes fenyegetés szabálysértése miatt lehetett felelősségre vonni.[290] A törvény a szabálysértési tényállás a) pontját bűncselekményi szintre emelte, és az (1) bekezdésben foglalt zaklatáshoz képest súlyosabb büntetéssel, két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel szankcionálja. A Btk. 138. §-a értelmében a fenyegetés olyan súlyos hátrány kilátásba helyezése, amely alkalmas arra, hogy a megfenyegetettben komoly félelmet keltsen. A zaklatás ezen fordulata is feltételez célzatot, az elkövető a sértettet vagy rá tekintettel hozzátartozóját azért fenyegeti meg, hogy benne a félelem valóban ki is alakuljon. A fenyegetésnek kvalifikáltnak kell lennie, csak a személy elleni erőszakos vagy közveszélyt okozó büntetendő cselekménnyel való megfenyegetést rendeli büntetni. Konkrétan tehát nem határozza meg, hogy ebben az esetben mely magatartások tekintendők ilyennek, azonban a Btk. 261. §-a (9) bekezdésének a) pontja (vagy az értelmező rendelkezések között az erőszakos többszörös visszaeső fogalma) segítségünkre lehet, hiszen a

[289] A telefonhívások mellett ide sorolhatóak az sms, az e-mail, a hangüzenetek küldése, és a kéretlen elektronikus levelek, reklámok (spam) tömeges küldözgetése is, bár ez utóbbi esetben a pontos elkövetők meghatározása számos akadályba ütközik.

[290] 2008. január 1-je előtt veszélyes fenyegetés szabálysértését követte el az 1999. LXIX. törvény 151. §-a szerint „Aki a) mást félelemkeltés céljából olyan bűncselekmény elkövetésével komolyan megfenyeget, amely a megfenyegetett személy vagy annak hozzátartozója élete, testi épsége vagy egészsége ellen irányul, b) mást félelemkeltés céljából a megfenyegetett személyre vagy annak hozzátartozójára vonatkozó, a becsület csorbítására alkalmas tény nagy nyilvánosság elé tárásával komolyan megfenyeget."

terrorcselekmény vonatkozásában felsorolja, hogy mi minősül személy elleni erőszakos, közveszélyt okozó, vagy fegyverrel kapcsolatos bűncselekménynek. A fenyegető kijelentéseknek konkrétnak, kifejezettnek kell lenniük. Az áttételesen személy elleni erőszakos cselekményre utaló, vitaszituációkban a hétköznapi nyelvhasználat során gyakorta elhangzó, vulgáris kifejezések - amelyek célja más megfélemlítése ugyan -, nem jelenthetik automatikusan a zaklatás második bekezdésének megvalósítását.

3.3. A (2) bekezdés b) pontja, a „veszélyes látszatkeltés”

A (2) bekezdés b) pontja szerinti zaklatást az követi el, aki „annak a látszatnak a keltésére törekszik, hogy a sértett vagy hozzátartozója életét, testi épségét vagy egészségét sértő vagy veszélyeztető esemény következik be”. Az új fordulatot az 2008. évi LXXIX. törvény vezette be 2009. február 1-jei hatállyal. A zaklatás ezen fordulatának elkövetési magatartása egyfajta burkolt fenyegetés. Amennyiben kifejezett fenyegetésről van szó, akkor az elkövető a (2) bekezdés a) pontja alapján vonható felelősségre. Nehezen értelmezhető azonban a „látszatnak a keltésére törekvés” kifejezés, hiszen a látszatkeltés magába foglalhat minden olyan magatartást, amely egy be nem következő esemény megtörténésének reális esélyét hiteti el a sértettel. Tehát olyan színlelésként értelmezhető viselkedést, vagy magatartást jelent, amely egy későbbi esemény akár a zaklató, akár más személy általi előidézésére, akár valamely személytől függetlenül történő bekövetkezésére utal. A tényállás alkalmazásának eseteit valószínűleg a jogalkalmazói gyakorlat fogja nagymértékben alakítani a való életben megtörténő magatartásokra vonatkoztatva, ami aggályos abban a tekintetben, hogy nem egyértelműen kijelölhetők azok a magatartások, amelyeket a jogalkotó büntetni kíván.

3.4. A tényállások összevetése

A zaklatás két bekezdése tehát három, egymástól teljes mértékben különböző elkövetési magatartást foglal magába, az (1) bekezdéses zaklatás esetén azonban általános tapasztalat, hogy a zaklató egy idő után megvalósítja a (2) bekezdés a) pontjába ütköző zaklatást is, vagy a sértett sérelmére erőszakos cselekményeket követ el. A három fordulat egyik célzata azonos, azaz a félelemkeltés. Míg az (1) bekezdés a magánéletbe való önkényes beavatkozástól, háborgatástól védi a személyt, addig a (2) bekezdésbe illesztett veszélyes fenyegetés és a veszélyes látszatkeltés inkább az erőszakos jellegű bűncselekmények megvalósulása előtt – azok megtörténtét megakadályozandó – egy pre-előkészületi jellegű előrehozott felelősségi alakzatot szankcionál.

Amennyiben az elkövető mindkét bekezdésbe ütköző magatartást valósít meg azonos sértett sérelmére, akkor az (1) bekezdésbe ütköző zaklatás beolvad ugyan a súlyosabban minősülő (2) bekezdés szerinti zaklatásba, azonban súlyosító körülményként való megállapítása indokolt, sőt minősítő körülményként való értékelése de lege ferenda megfontolandó. Emellett a zaklatás mindkét fordulatát bűntetté minősíti az a körülmény, ha a bűncselekményt az elkövető volt házastársa vagy volt élettársa, volt bejegyzett élettársa, illetve nevelése, felügyelete, gondozása vagy gyógykezelése alatt álló személy sérelmére követi el.

4. A CYBER-STALKING

A Btk. maga is nevesíti az (1) bekezdéses zaklatás során a legtipikusabb elkövetési magatartások közül a telekommunikációs eszköz útján történő elkövetést, amely a fejezet szempontjából az internet mint számítástechnikai rendszer segítségével elkövetett zaklatást

jelenti. Az internet és a mobiltechnológia az elkövető és áldozatának kapcsolatát tekintve két alapvető lehetőséget teremt. A távoli hozzáférést – azaz azt az esélyt, hogy az elkövető bárhol is tartózkodjon, eléri áldozatát – míg a másik oldalon, az állandó hozzáférhetőséget az áldozat helyzetétől függetlenül. Érdemes tehát ezzel az elkövetési móddal kicsit részletesebben foglalkozni.

Az internet nyújtotta kommunikációs lehetőségek a felek fesztelen, a realitásokat elrejtő érintkezését teszik lehetővé. Különlegessége, hogy egyes kommunikációs módok (e-mail, chat) csak írásbeli alapúak, az észlelés, érzékelés más szenzorai nem kapnak szerepet. A kommunikációk során nincs hang, amelynek ereje, hangsúlya, üteme többlet információt hordozna a közvetített tartalmat illetően, és nem utal a közlő nemére, vagy életkorára. Egy meghatározott személyre jellemző szóhasználattal írt szöveg könnyen tárolható, megszerezhető, többszörözhető.[291] A láthatatlanság szintén megfosztja a fogadó felet a közlő mimikájától, reakcióitól, ezáltal könnyebben befolyásolható, félreérthető a közlés. Az interneten zajló kommunikáció ugyanakkor bizonyos esetekben a szemtől-szemben zajló beszélgetésekkel szemben többletinformációkat is hordozhatnak. Így például egy üzenethez képi, zenei fájlok, linkek csatolhatók, amelyek szintén módosíthatják egy közlés valódi jelentését.[292]

Mindezek a körülmények különböző lehetőségeket biztosítanak a zaklatóknak. A társasági-társadalmi kontroll hiánya azt eredményezi, hogy a társasági szorongás, mint az agresszió egyik legjelentősebb gátja nem létezik. Ezért egyrészt bizonyos, a zaklatókra jellemző érzelmek, indulatok, vágyak – düh, féltékenység, elkeseredettség, birtoklási-irányítás vágy – vagy agresszió közvetlenül a zaklató célpontjára irányíthatók, másrészt a különböző fantáziák kialakulásának lehetőségével az áldozat a zaklató képzelődéseinek fókusza lehet.[293] A közvetlen kapcsolat hiánya emocionális és fizikai távolságot kreál az elkövető és áldozata között, ami egyrészt az áldozat „személytelenítéséhez", és ezáltal az elérhetetlenség tudatában az elkövetés érzelmi megkönnyítéséhez vezet, másrészt az elkövető nagyobb kontroll-lehetőségét eredményezi.[294] Utóbbi körülmény egyik jellemzője, hogy az elkövető az úgynevezett *proxy-stalking* esetén más online résztvevőket befolyásolva érheti el egy személy zaklatását.[295]

Meloy, J. Reid szerint is az internet több tekintetben kaphat szerepet a zaklatás során. Bár gondolatai sok esetben inkább teoretikusak, ezen lehetőségekkel is érdemes pár mondat erejéig számot vetni. Az első esetben az internet olyan eszköz, amit az elkövető a későbbi zaklatás megkönnyítése érdekében az áldozatra vonatkozó személyes információgyűjtés céljából vehet igénybe.[296] Az internethasználat web 2.0 -ként is jelölt trendjének egyik attribútuma a felhasználók közösségépítése – gondoljunk az iwiw, myvip, facebook és a többi szolgáltatásra –, a felhasználók által történő, legtöbbször átgondolatlan adatszolgáltatás. Mindez információs aranybányának tekinthető egy stalker felkészülése során. A második esetben olyan médium, kommunikációs csatorna, amelyen keresztül az áldozatot az elkövető megfenyegetheti, vágyait, érzéseit az áldozata felé tolmácsolhatja.

[291] BARAK, A., Phantom emotions – psychological determinants of emotional experiences on the Internet. In. Joinson, A., McKenna, K., Postmes, T. & Reips, U-D. (ed.), *The Oxford Handbook of Internet Psychology,* Oxford University Press, 2007. pp. 306-307.
[292] BARAK, 2007. p. 307.
[293] MELOY, 1998. p. 11.
[294] BOCIJ, P. & MCFARLANE, L., Cyberstalking: the technology of hate. *The Police Journal,* Vol. 76. (2003.) p. 213.
[295] BOCIJ & MCFARLANE, 2003. p. 213.
[296] MELOY, 1998. p. 10.

Harmadsorban Meloy a meglepetés pszichológiai hatásának tulajdonít komoly szerepet, hiszen elektronikus üzenetet bármikor küldhetünk bárkinek, az üzenet időtől függetlenül létezhet, amíg az áldozat rá nem bukkan, ami az időzítéstől függően azt az érzetet keltheti a kiszemelt személyben, hogy zaklatója bárhol, bármikor a közelében van.[297] Az anonimitás fokozza az áldozat alávetettségét amiatt, hogy nem tudja, ki zaklatja, ekként a környezetében bárkire gyanakodni fog.

Bran Nicol szerint[298] mai kultúránkat többek között az jellemzi, hogy a zaklató magatartások ösztönzői követendő példává erősödtek. Nicol ezalatt a következőket érti: elfogadott és támogatott az a meggyőződés, hogy egyrészt bárkiről, akár idegenekről is minél több információt gyűjtsünk, és velük bensőséges viszonyt építsünk ki, másrészt ennek ellenkezője, azaz hogy önmagunk akár legsötétebb és legbelsőségesebb vágyait is mindenki számára megmutassuk. Olyan világban élünk, ahol az egyén és a mások közötti mezsgye veszélyesen elmosódott, így a zaklatás maga egy ilyen kultúra tüneteként, talán elkerülhetetlen termékeként jelent meg. Az állandó figyelemfelhívás önmagunkra és a hírességekhez való szűnni nem akaró tartozni vágyás mind azt jelzik, hogy a „privacy"-nak tulajdonított felfogásunk megváltozott. A minket teljesen körülölelő digitális kultúra egyfajta folytonos, elfogadott zaklatásba taszít. Maga az internet tehát olyan közvetítő szerepet játszik, amelyen keresztül egyrészt legtöbbször maguk az áldozatok közrehatásaként vagy az általuk közzétett adatok felhasználásával lehet zaklatni, vagy másrészt a Nicol által példaként említett zaklató „szolgáltatásokon" keresztül. Nicol olyan honlapok példáját említi, mint a CelebFanMail.com, vagy a Gawker Stalker, amelyek segítségével szinte bármely híresség e-mail címét és aktuális tartózkodási helyét megtudhatjuk az őket éppen megpillantó „hétköznapi emberek" által közzétett információk alapján. Harmadrészt az internet működésének sajátossága, hogy az általa biztosított anonimitás csupán látszólagos. A felhasználók által igénybe vett szolgáltatások során számtalan nyom keletkezik, amelyeket a hozzáértők képesek összegyűjteni, az adathalászat népszerűségéről ma már nem is érdemes vitába bocsátkozni.

Érdemes e fejezeten belül pár gondolat erejéig az Európai Unió Bizottsága közreműködésével 2009 februárjában tizenhét nagyobb internetes cég által a közösségépítő weboldalak tizennyolc évesnél fiatalabb használóinak biztonságát erősítendő aláírt megállapodással is foglalkozni. A megállapodásban részes felek a következő eszközökkel tervezik visszaszorítani olyan nem kívánt jelenségeket, mint az online zaklatás: a) könnyen használható „visszaélés bejelentése" gomb elhelyezése a kezelőfelületen, amellyel egyetlen kattintással jelezni lehet, ha egy másik felhasználó viselkedését nem tartja kívánatosnak a felhasználó, b) alapértelmezésben ne legyenek publikusak a tizennyolc éven aluli felhasználók személyes adatai, c) a felhasználók személyes adatai keresőprogramokkal által ne lehessenek kereshetők, d) a magánélet védelmét szolgáló funkciók minden időpontban jól látható, könnyen hozzáférhető módon legyenek elhelyezve, e) a 13 évesnél fiatalabb felhasználók regisztrációját meg kell nehezíteni.

Mindezen intézkedések azonban feltételezik a felhasználók személyes adatokra vonatkozó érzékenységét, tudatosságát, amelyet viszont nem támasztanak alá azok a Magyarországon is érzékelhető trendek – amelyeket magyar kifejezések hiányában olyan idegen, új kulcsszavakkal lehet megragadni – mint cyberbullying, sexting.

[297] MELOY, 1998. p. 12.
[298] NICOL, 2006. pp. 8-9.

5. A SZABÁLYOZÁS ÉRTÉKELÉSE

5.1. A Btk. 176/A. § (1) bekezdésébe ütköző zaklatás

Tekintettel arra, hogy a Btk. 176/A. § (1) bekezdésébe ütköző zaklatás tényállása célzatot is tartalmaz, a bűncselekmény kizárólag egyenes szándékkal követhető el. Ez a célzat a) más megfélemlítése, vagy b) más magánéletébe, illetőleg mindennapi életvitelébe történő önkényes beavatkozás. Alapvető problémát okoz, hogy míg a megfélemlítés dogmatikailag letisztult fogalom, addig a magánéletbe való önkényes beavatkozás a büntetőjogi jogalkalmazásban idegen fordulatnak számít a magánélet kifejezés büntetőjogi definíciójának hiánya miatt. A két célzat eltérő absztrakciós szintje pedig még nehezebbé teszi a tényállás alkalmazhatóságát.[299] A célzatra figyelemmel a bizonyítást meglehetősen megnehezítve könnyen sikeresek lehetnek azok az elkövetői védekezések, amelyek a sértett háborgatását eredményező magatartást szándékon túli, mégis valószerű okokkal magyarázzák.[300] Helyesebbnek látom a törvényszövegnek oly módon történő átfogalmazását, amely a célzat mellőzésével büntethetővé teszi az eshetőleges szándékkal történő elkövetést is. Szinte lehetetlenné teszi a bizonyítást az, hogy a sértettel legtöbbször haragos viszonyban lévő elkövető korábbi nézeteltéréseik, elszámolási vitájuk rendezése, haragjának, vagy éppen vonzalmának a sértett felé tolmácsolásának szándékával törekszik olyan kapcsolatfelvételre, amely a sértett háborgatását eredményezi ugyan, de célzata nem a törvényben megfogalmazott célzat.

A magánélet fogalmának bizonytalansága miatt ugyancsak értelmezésre szorul az eset, amikor a gyanúsított a sértett baráti társaságának tagjain keresztül háborgatja a sértettet, és avatkozik be önkényesen magánéletébe úgy, hogy közvetetten, a sértett ismerőseit készteti olyan cselekményekre, amivel önmaguk magánszférája nem sérül, a sértetté viszont igen. A magánszféra fogalmának meghatározására tett kísérletek ismertetése során a magánélet több szintjét vázoltam fel, és azt állítottam, hogy az önkényes beavatkozás mindhárom rendszerelemen keresztül sértheti az egyén jogát a háborítatlan mindennapi életvitelhez. Ezt a gondolatot erősíti a törvény kommentárja is, amely szerint „zaklató jellegű magatartásnak tekinthetőek: az ismétlődő, éjjel-nappali – akár névtelen – telefonhívások otthon és a munkahelyen; üzenetrögzítőn hagyott vagy e-mailen, sms-ben küldött, gyakran sértő, szidalmazó ill. fenyegető üzenetek; az áldozat lakása, munkahelye stb. előtti gyakori jelenlét; az áldozat követése nyilvános helyekre. Mindez kiterjedhet az áldozat közeli hozzátartozóira, barátaira is.”.[301] Erre figyelemmel az (1) bekezdésbe foglalt zaklatás megvalósulhat közvetve is.

Viszonylagos, szubjektív, a sértetti véleményen kívül jogalkalmazói értékelést is igénylő kategória a „háborgatás” fogalma. Példaként említhető, hogy a kizárólag e-mailek küldözgetésében kimerülő zaklatásokban az e-mail nem tekinthető olyan állandó hozzáférhetőséget biztosító szolgáltatásnak, amely minden esetben alkalmas lenne az életminőség tényleges rontására.[302] Korinek Lászlóval egyetértve azért is nehéz empirikus

[299] UJVÁRI Á., A zaklatásról. *Ügyvédek Lapja* 2009/2. p. 18.

[300] Gyakran meg nem cáfolható az a – már nem példa nélküli – terhelti védekezés, amely szerint a gyakori, éjszakai telefonhívásokkal – az állítása szerint lopásra előkészülő – gyanúsított célja kizárólag annak felderítése volt, hogy a sértett otthon tartózkodik-e. Figyelemmel arra, hogy a lopás előkészülete nem büntetendő, és a célzat hiányában a zaklatás (1) bekezdéses alakzata sem tényállásszerű, az ügyésznek a nyomozati szakban a nyomozás megszüntetéséről kell határoznia.

[301] A Complex Dvd Jogtár kommentárja a Btk. 176/A.§-hoz.

[302] Az e-mailt olvasatlanul ki lehet törölni, egyes szolgáltatóknál le lehet tiltani a küldőjét akár a kéretlen elektronikus reklámanyagokat.

kutatásokat folytatni e témakörben, mert az elkövetési magatartások, de különösen a sértettek, az egyének érzékenysége meglehetősen eltérő.[303] Azonban a sértett ért, háborgatásként megélt behatásokról a végső szót a jogalkalmazónak kell kimondania – egyéniesítve ugyan, mégis következetesen – eldöntve azt, hogy mit tekint háborgatásnak.

A törvényszöveg szerint a háborgatásnak rendszeresnek vagy tartósnak kell lennie. Az elkövetés módjától és a kapcsolatfelvétel csatornájától függően kell azonban meghatározni azt, hogy egy adott magatartás annak tekinthető-e. Az ugyanazon a napon megtörténő 4-5 telefonhívás, vagy e-mailküldés nem tekinthető sem rendszeresnek, sem tartósnak, nem eredményezheti a magánszféra sérelmét.

Annak vizsgálatán is el kell gondolkodni, hogy a kizárólag számítástechnikai rendszer útján megvalósuló háborgatás – e-mailek, sms-üzenetek küldözgetése – esetén amennyiben a sértettnek van lehetősége az elkövető behatásának kizárására és ezzel nem él, szükség van-e ultima ratioként büntetőjogi szankciókat alkalmazni.[304] A Btk. más esetben is megkövetel bizonyos óvintézkedéseket a sértettől, és a büntetőjogi védelmet csak annak megléte esetén biztosítja. Ilyen tényállás például a Btk. 300/C. § (1) bekezdésébe foglalt jogosulatlan belépés számítástechnikai rendszerbe, amelyet csak a rendszer védelmét szolgáló intézkedés kijátszásával lehet elkövetni, tehát ha nincs védelem, bűncselekmény nem valósul meg.

Az áldozatra koncentráló profilalkotói kutatások eredményei rámutatnak a bűncselekmény hatásaira is. A számszerűsített kapcsolatfelvételek száraz ténye önmagában visszaélésekre adhat alapot, amennyiben akkor is megállapíthatónak ítéljük a bűncselekményt, ha a háborgatás a sértett magánéletére lényeges kihatással nincsen, nem jár az életminőség megromlásával. Ezért vizsgálni lenne indokolt a zaklatás okozta sérelmeket, amelyek a következők lehetnek: alvászavarok, munkahelyi teherbírás csökkenése, visszahúzódó, bezárkózott életvitel, párkapcsolati problémák az életminőség általános romlása, azaz a kialakuló szorongás kiterjed több, mindennapi általános szokásra, úgymint bevásárlás.[305] Az Egyesült Államokban, az Egyesült Királyságban, Ausztráliában folytatott kutatások alapján a zaklató tevékenységének befejezése után még hosszabb ideig fennmaradtak ezen káros hatások, az életminőség tartósabb romlását eredményezve tehát. A kutatásban részt vett összesen 16.000 ember (nyolcezer nő és ugyanennyi férfi) közül minden harmadik keresett pszichológiai segítséget, egyötödük kimaradt a munkahelyéről, 7% otthagyta a munkahelyét. A megkérdezettek 20 %-a a zaklatásuk befejeződését elköltözésük idejére tette, amely önmagában egy erőteljes lelki megpróbáltatás, 71% az áldozatoknak több szokását is megváltoztatta.[306]

Eddig még nem tisztázott problémát jelent az (1) bekezdésbe ütköző zaklatás esetén a halmazat megállapíthatóságának kérdése, amennyiben az elkövető háborgatása nem csak a kiszemelt áldozatát, hanem például a vele együtt élő családtagjait is érinti.[307] A családtagok magánszféráját külön-külön, avagy a közös magánéletet sérti-e az elkövető ebben az

[303] KORINEK L., Nemek, szexualitás és bűnözés. 12. forrás: http://www.pecshor.hu/periodika/2007/VIII/korinek.pdf [2011-07-31]. Például: ugyanazt a viccelődést, célozgatást másként élhetik meg a sértettek.

[304] Példaként hozható fel az az eset, amikor az iwiw közösségi oldalon szerelmesleveleket küldözgetve hódoló felhasználó levelezését a sértett egy gombnyomással kizárhatja, letilthatja.

[305] PETHERICK, W., Stalking. In. Turvey, B. E. (ed.), *Criminal Profiling – an introduction to behavioral evidence analysis*. Elsenier Inc. 84. Theobald's Road, London 2008. p. 452.

[306] PETHERICK, 2008. p. 453.

[307] A hajnalban történő telefonhívások minden együttlakót zavarnak.

esetben? Ilyen helyzetben minden családtag magánszféráját külön-külön sérti az elkövető, azonban pontosan magánéletük közös részében. Bár több személy joga sérül a behatás következtében, a konkrét személyre irányuló háborgatási célzat és a többek által közösen lakott lakásra elkövetett magánlaksértéshez hasonlóan nem állapítható meg a halmazat.

Az (1) bekezdésbe ütköző zaklatás tartós háborgatást jelent, különböző részcselekményekből tevődik össze, amelyek egységesen jelentik a sértett magánéletébe történő beavatkozást. Kérdésként merül fel, hogy a kettős értékelés tilalmába ütközne-e az a gyakorlat, amely az ugyanazon sértett sérelmére ugyanazon elkövető által korábban elkövetett rongálását, magánlaksértést, lopást – ezek szabálysértési alakzatát is ideértve –, vagy például elutasított feljelentéseket részcselekményeknek értékelve megállapítja a tartós háborgatást.

5.2. A Btk. 176/A. § (2) bekezdés a) pontjába ütköző zaklatás

Különös helyzetet teremtett az a jogalkotói megoldás, ahogyan a zaklatás büntető törvénykönyvbeli tényállását megalkották. A veszélyes fenyegetés szabálysértési tényállása a) pontjának hatályon kívül helyezése, és annak átfogalmazásával történő átemelése a Btk. 176/A. § (2) bekezdésébe, majd a törvényhely ez év elejei hatályba lépése azt jelentette, hogy a 2008. január hó 1. napja előtt elkövetett, a szabálysértési törvény 151. § (1) bekezdés a) pontjába ütköző veszélyes fenyegetés 2008. január hó 1. napjától kezdődően nem volt büntethető. Ennek oka, hogy az 1999. LXIX. törvény 4. §-a szerint a „cselekményt az elkövetés idején hatályban lévő jogszabályok alapján kell elbírálni. Ha a szabálysértés elbírálásakor hatályban lévő új jogszabály szerint a cselekmény már nem minősül jogellenesnek, vagy enyhébben bírálandó el, akkor az új jogszabályt kell alkalmazni”. Mivel a Btk. 176/A. § (2) bekezdésébe ütköző zaklatás vétségének visszaható hatályú alkalmazása szintén kizárt annak nullum crime sine lege elvébe ütközése és a Btk. időbeli hatályáról rendelkező 2. §-a miatt, olyan jogalkalmazási űr született, amely ellehetetlenítette a jogalkotónak a zaklató, fenyegető jellegű magatartások szigorúbb szankcionálására irányuló törekvését, mintegy „átmeneti amnesztiát” hirdetve az adott időben elkövetőknek.

A (2) bekezdésbe foglalt zaklatás esetén az elkövetés legtöbbször verbális környezetben történik, „eszközei” a szavak, nyelvfordulatok, amelyek kultúrától, szubkultúrától, műveltségi foktól függően különböző tartalmat közvetíthetnek. Az egyes szubkultúrákban megtalálható átkozódás, szitkozódás elfogadott szokása sajnálatos módon természetes velejárója lett a szubkultúrához tartozók között zajló kommunikációnak, véleménynyilvánításnak. Jóllehet személy elleni erőszakos cselekmények változatos sorát foglalja magába, ám éppen természetessé válása miatt nem tekinthető minden körülmények között társadalomra veszélyes cselekménynek, nem értelmezhető feltétlenül komoly, veszélyes fenyegetésként. Ilyen átkozódásra utalhat másoknak meglehetősen változatos, mégis „bevett” módszerekkel történő megkínzására utaló, megszokott kifejezések. A kriminalizációt nem előzte meg olyan szociológiai kutatás, amely a mindennapok nyelvhasználatára, a magyar szóhasználatban gyakorta közismert kötőszóként megjelenő káromkodások környezetére irányult volna. Szintén értelmezésre szorul a fenyegetésnek nem verbális, hanem metanyelvi kommunikációval a sértett tudtára adott formája, például nyak előtti vágómozdulat mutatása a sértett felé, vagy a telefonban lejátszott halotti induló, fehér por küldözgetése borítékban.

A tényállás képes ugyan megragadni az egyértelműen kifejezett veszélyes fenyegetést, a határeseteknél azonban egyrészt komoly jogalkalmazói visszaélésekre adhat lehetőséget,

másrészt a jog tekintélyvesztéséhez vezethet a formálisan tényállásszerű, de társadalomra nem veszélyes elkövetés esetén elmaradó jogkövetkezmények miatt. Az új tényállás „népszerűsége" a nyomozó hatóságok erőforrásainak nagy részét leköti, bizonyíthatósága meglehetősen nehézkes figyelemmel arra, hogy a sértetten és a gyanúsítotton kívül más, elfogulatlannak tekinthető tanú legtöbbször nem áll rendelkezésre, a leggyakrabban telefonon elkövetett zaklatás vonatkozásában pedig a szolgáltatóktól beszerzett híváslista a kapcsolatfelvételek időpontja és tartama mellett a beszélgetések tartalmát természetesen nem tartalmazza. Jogosan fogalmazza meg kételyeit Korinek László a szexuális bűncselekmények társadalomra veszélyességéről elmélkedve, amikor azt a kérdést teszi fel, hogy vajon „képes-e egyáltalában a közhatalom bármilyen, tipikusan két ember között és a nyilvánosságtól elzárva megvalósított magatartását a jog érvényesítéséhez szükséges mértékben ellenőrizni, arról büntetőeljárási bizonyítékként is felhasználható adatot szerezni".[308] Ennek kudarca szintén a jog tekintélyvesztését eredményezheti.

6. A STALKING ÉS AZ ALKOTMÁNYOS BÜNTETŐJOG

A fejezet vizsgálatai alapján két problémacsoport körvonalazható. Az első a védendő jogi tárgy meghatározásának kérdése, a második pedig a veszélyes látszatkeltés tényállásának arányossága.

A magánszférához fűződő alkotmányos alapjog – ahogyan az magából az Alkotmány szövegéből is kitűnik – polgári jogi és büntetőjogi védelme az egyes alkotóelemeken keresztül biztosított, például a magánlakás, a testi épség, a személyes adatok védelmén keresztül. A magánélet mint olyan, a maga absztrakciója miatt büntetőjogi szempontból eleve nem kellően körülhatárolt jelenség, jogalkalmazói tekintetben pedig olyan megfoghatatlan kategória, amely a túlzott teret enged a következetlen, jogesetenként eltérő eredményre vezető jogértelmezésnek. Emelett nem szabad elfeledni, hogy a tényállás lényegében a magánélet sérelmét okozó beavatkozás elleni hatékonyabb fellépés jegyében született, azaz a tényállásszerűséghez szükség van az életminőség hátrányos változására. E minőségi változás – legyen az állandó vagy átmeneti – megítélése, mérése természetesen rendkívül kényes jogalkalmazást és jogi szabályozást igényelne, azonban a jogalkotó a személyes adatok megsértése kapcsán is elvárta a jelentős érdeksérelem okozását.

A Btk. 176/A. § (2) bekezdés b) pontjába ütköző zaklatás (veszélyes látszatkeltés) a nyugodt magánélet védelme rendszerében meglehetősen leszállítja a büntethetőség határát. A tényállás célja, hogy büntesse azon magatartásokat, amelyek azt a látszatot keltik, hogy valakit a jövőben sérelem fog érni. Az elkövető szándéka nem irányul a sérelem okozására, annak csupán látszatát kívánja kelteni, amellyel a célszemély nyugalmát megzavarja. A cselekmény bűncselekményi szintű szabályozását indokoló társadalomra veszélyességéhez a következő körülmények miatt fűződik kétely. Egyrészt a büntetőtörvény eleve nem rendeli büntetni valamennyi személy elleni bűncselekmény előkészületi alakzatát, így például a magánlaksértés, személyi szabadság megsértése esetén sem. Másrészt ismert a jogrendszerben egy további, a zaklatáshoz hasonló szabálysértési tényállás is. Az 1999. évi LXIX. törvény 151. § (1) bekezdésének b) pontjába ütköző szabálysértést követ el az, aki mást félelemkeltés céljából, a megfenyegetett személyre vagy annak hozzátartozójára vonatkozó, a becsület csorbítására alkalmas tény nagy nyilvánosság elé tárásával komolyan megfenyeget. A két elkövetési magatartást összehasonlítva azt a következtetést vonhatjuk le, hogy a cselekmények magánéletre gyakorolható nyugtalanító hatása mindkét esetben

[308] KORINEK L., Nemek, szexualitás és bűnözés. 10. forrás: http://www.pecshor.hu/periodika/2007/VIII/korinek.pdf [2012-02-19]

közel azonos mértékű érdeksérelem okozására alkalmas, a jogalkotó ennek ellenére nem adta alkotmányos indokát a hatályos szabályozás megkülönböztető jellegének. A magánélet védelmének büntetőjogi és szabálysértési szabályozási rendszerét vizsgálva tehát az állapítható meg, hogy a veszélyes látszatkeltés nem felel meg az arányosság követelményének.

VIII. FEJEZET: JOGESETEK ELEMZÉSE

Az eddig elemzett tényállások azt a látszatot kelthetik, hogy azok külön-külön könnyen alkalmazhatók, különösebb minősítési problémát nem okoznak. Az infokommunikációs konvergencia azonban igenis érezteti hatását egy-egy tényállás minősítése esetén, hiszen számos olyan élethelyzet alakult ki, amelynek helyes jogi megítélése bizony nem könnyű a több jogterület találkozása miatt. A korábbi fejezetek ismeretében látható, hogy a számítástechnikai bűncselekmények dogmatikája még nem olyan mélységében kidolgozott, mint a klasszikusnak nevezhető deliktumoké. A jogalkalmazó a technológiai fejlődés megállíthatatlan folyamatában gyakran találkozik egy-egy új elkövetési tárgy és módszer okozta értelmezési problémával. A probléma érzékeltetésére a fejezetben egy ilyen fejtörést okozó minősítési kérdéseket járok körbe annak bemutatása érdekében, hogy dogmatikai szempontból milyen nehézségeket vet fel az infokommunikációs konvergencia.

1. A MŰHOLDVEVŐ BELTÉRI EGYSÉGEK ESETE

A vizsgált elkövetési magatartás a következőképpen foglalható össze. Az elkövető kódolatlan műholdas adások vételére alkalmas műszaki berendezéseket vásárol, amiket a megvásárolt készülékekben lévő szoftvert megváltoztatva alkalmassá tesz egy távközlési szolgáltató (a továbbiakban szolgáltató) által sugárzott televíziós műsoradások vételére úgy, hogy a készülékkel nem csak a szolgáltató által sugárzott – egyébként más műsorelosztó szervezeten keresztül is elérhető, kódolatlan adásokat lehetett fogni –, hanem a szolgáltató által külön díj fizetésével elérhetővé tett ún. kódolt adásokat is. A készülék szoftverein az elkövető maga végzi el a szükséges módosításokat, de egyes kódokat (adatokat) és azok bevitelének módját is közli az átalakított készülékeket tőle megvásárlókkal úgy, hogy megadja az interneten elérhető és ott közzétett módszer elérhetőségének címét is, amelynek segítségével a készüléket megvásárló személy elvégezheti akár a szoftver átírását vagy a szolgáltatás igénybevételéhez szükséges frissítését.

A fenti cselekményt lehet egyrészt a Btk. 329/B. § (1) bekezdés b) pontja, de a (2) bekezdés - és az üzletszerű elkövetésre tekintettel - a (3) bekezdés szerint is minősíteni. A módosított készülékek megvásárlóival szemben ebben az esetben eljárás nem indul bűncselekmény hiánya miatt. A minősítés alapja ekkor az, hogy a kódolt adások vételét lehetővé tevő program a szerzői jogi törvényben meghatározott hatásos műszaki intézkedésként értelmezhető. Azonban a távközlés és a média területén alkalmazott számítástechnika jelenléte okán a tényállás minősítése joggal veti fel egy másik lehetséges bűncselekmény megállapíthatóságát, nevezetesen a cselekmény Btk. 300/C. § és a 300/E. § szerinti minősítést is.

1.1. A szerzői jogi szempont

A helyes megoldás kiderítéséhez nem mellőzhető az érintett jogviszonyok vizsgálata, és a törvényi tényállás egyes részleteinek alaposabb értelmezése. A készülékben lévő szoftver és adatok tekintetében a minősítés kérdése vonatkozásában megkerülhetetlen annak eldöntése, hogy mi az elkövető célja, hogy a szerzői jogi törvényben meghatározott hatásos műszaki intézkedésről van-e szó, vagy más jellegű, jelen esetben számítástechnikai rendszer védelmét szolgáló intézkedésről. Ehhez azonban a terjedelmi okok miatt csak a feltétlenül szükséges mértékben, de meg kell ismerni – köznyelvi kifejezéssel élve – a műholdas televíziózás műszaki és jogi hátterét is. A tartalom legtöbbször szerzői jog által védett, de lehet a szerzői jog körén kívül eső is, például sportközvetítés. Amennyiben a

tartalom szerzői jogi oltalom alá esik, a szabályozás elemzésekor a médiajog és a szerzői jog fogalmait meg kell tudni feleltetni egymásnak. Ezért a következő fejezetekben az érintett szabályozási elem értelmezésekor mindkét jogterület fogalmait egyszerre fogom használni. E rövid bevezető után a szerzői jogi alapjogviszonyokat szemügyre véve a következőket állapíthatjuk meg.

1.2. Nyilvánossághoz való közvetítés

Szerzői jogi szempontból a mű nyilvánossághoz való közvetítése, mint felhasználás vonható a vizsgálat körébe. Az Szjt 26. §-ában írt rendelkezések alapján a szerző kizárólagos joga, hogy a művét sugárzással a nyilvánossághoz közvetítse, és hogy erre másnak engedélyt adjon. A sugárzás a mű érzékelhetővé tétele távollévők számára képeknek és hangoknak, vagy technikai megjelenítésüknek vezeték vagy más hasonló eszköz nélkül megvalósuló átvitelével. Sugárzásnak minősül a műhold útján történő sugárzás, ha a sugárzott műsor a nyilvánosság körében közvetlenül fogható.[309] A sugárzás során alkalmazott jel és adat-átalakítási, tárolási és továbbítási technika szerzői jogi szempontból közömbös, lehet akár analóg, akár digitális, annak is csak a szerzői jogi felelősség szempontjából van jelentősége, hogy kódolja-e a műsort eredeztető szervezet (szerzői jogi fogalommal élve rádió- televízió szervezet, médiajogi fogalommal médiaszolgáltató, korábban műsorszolgáltató[310]), vagy a hozzájárulásával más, a műsorhordozó adat továbbításában közreműködő személy a műsorhordozó jeleket, adatokat.[311]

1.3. Kódolt sugárzás

Sugárzásnak minősül a kódolt sugárzás[312] is, amely a nyilvánosság körében csak azt követően fogható közvetlenül, hogy a műsort hordozó jeleket – az eredeti rádió- vagy televízió-szervezettel kötött megállapodás alapján, a tőle vagy a hozzájárulásával mástól beszerzett eszközzel (kódolóval) – a nyilvánossághoz közvetítő szervezet arra alkalmassá teszi.[313] Műholdas sugárzásnak akkor minősül a kódolt sugárzás, ha a kód feloldásához szükséges eszközt vagy maga a műsorszolgáltató, vagy a hozzájárulásával más, rendszerint a műsorelosztó bocsátja a közönség tagja rendelkezésére.[314] A műsorhordozó jelek és adatok többszöri átalakítása a műsor közönségéhez eljuttatásában technikailag szükségszerű, ezért az átalakítások közül csak az számít kódolásnak, azaz titkosításnak, amelynek célja, hogy a műsorhoz való hozzáférést korlátozza, ennek okán az ilyen átalakítás a rádió- televízió szervezet által alkalmazott un. hatásos műszaki intézkedésnek minősül.[315]

A műholdas adások egy részét kódolják, így a műholdas adás nem minősül közvetlenül foghatónak, azaz nem elég a műsor vételéhez egy hagyományos parabolaantenna. A

[309] A műhold útján sugárzott műsor a nyilvánosság körében közvetlenül foghatónak minősül, ha a rádió- vagy televízió-szervezet felelősségével és ellenőrzése alatt műsort hordozó jeleket juttatnak el a műholdhoz, majd onnan a Földre megszakítatlan közvetítés útján azzal a céllal, hogy a jeleket a nyilvánosság vehesse.

[310] ***Médiaszolgáltató****:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező gazdasági társaság, aki vagy amely szerkesztői felelősséggel rendelkezik a médiaszolgáltatás tartalmának megválasztásáért, és meghatározza annak összeállítását. (2010. CIV. törvény 1. § 2. pont.)

[311] LONTAI et al. pp. 71-73.

[312] Kódolt a sugárzás, ha a műsort hordozó jeleket bármilyen módon átalakítják, hogy a hozzáférést a nyilvánosság valamely szűkebb körére korlátozzák.

[313] Szjt. 26. § (3) bek.

[314] LONTAI et al. p. 73.

[315] LONTAI et al. p. 73.

műsorhordozó jeleket a műsorelosztó szolgáltató[316] (szerzői jogi fogalommal továbbközvetítő) fejállomásánál veszik és a kód feloldása után a közönséghez már a műsorként érzékelhető jelek jutnak el. A kódolás másik eljárása során a rádió- televízió szervezet (műsorszolgáltató) a kódolt jeleket eljuttatja a műsorelosztó szolgáltatókhoz, de mivel a fejállomáson a kódot nem lehet feloldani, a műsorhordozó jeleket változatlanul kódolatlan, vagy a műsorszolgáltató által alkalmazott és előírt technológia szerint átkódoltan kell eljuttatni a háztartásokhoz. A kód feloldása tehát a közönség tagjainál a tévékészülékekben, vagy ahhoz csatlakoztatott eszközzel történik olyan kódolóval, amelyet a közönség tagjai vagy csak a műsorszolgáltatótól, illetve közreműködőjétől, vagy a műsorelosztó szolgáltatóktól szerezhetnek be.[317] Ha a kódolás a közönség tagjainál történik, a műsorelosztó úgy tekintendő, mintha műsort eredeztető rádió- televízió szervezet lenne.[318] A mű(sor) megjelenítése a végfelhasználó készülékeiben felveti annak egy szerzői jogi felhasználásként, nevezetesen a többszörözésként történő értelmezésének technológiai lehetőségét is.

1.4. A sugárzott műsorok továbbközvetítése

A nem anyagi formában megvalósuló felhasználási módok között külön felhasználásnak minősül, tehát külön szerzői engedélyezés tárgya a sugárzott műsorok továbbközvetítése.[319] A továbbközvetítés technikai megvalósítási módja közömbös, történhet vezeték útján, vagy másként, a gyakorlatban általában vezeték útján, vagy mikrohullámok segítségével juttatják el a (médiajogi fogalommal élve, mivel a szerzői jogi törvény nem tartalmaz e felhasználókra külön definíciót) műsorelosztók a már sugárzott műsorokat a végfelhasználókhoz.[320]

A továbbközvetítés műsorokra vonatkozik, ezért több jogosult engedélyétől függ. A szerzők, a műsorokban érintett hangfelvétel előállítók és előadóművészek esetében az engedélyt a műsorelosztók az érintett jogosultak egyetértése alapján megállapított jogdíj megfizetésével – kötelező közös jogkezelés keretében – a zenei és irodalmi szerzők közös

---

[316] ***Műsorelosztás:*** olyan műsorterjesztés, amely során az előfizető, vagy felhasználó elektronikus hírközlő végberendezése meghatározott földrajzi helyen csatlakozik a műsorterjesztő átviteli rendszerhez. ***Műsorszórás:*** olyan műsorterjesztés, amelynek során analóg vagy digitális médiaszolgáltatásokat a földfelszínen telepített - az elsődlegesen műholdas szolgálatra rendelt frekvenciák kivételével - rádiófrekvenciát használó, általában egyirányú adatátvitelt lehetővé tevő átviteli rendszerrel továbbítják az előfizetőhöz vagy felhasználóhoz; műsorszórásnak minősül a digitális műsorszóró hálózat (egyidejűleg több frekvenciát használó, több adóval működő hálózat) vagy műsorszóró adó (ugyanazon frekvenciát egyidejűleg, azonos módon használó egy vagy több adó) segítségével végzett műsorterjesztés is. ***Műsorterjesztés:*** az 5/a. pont szerinti bármely átviteli rendszerrel megvalósuló elektronikus hírközlési szolgáltatás, amelynek során a médiaszolgáltató által előállított analóg vagy digitális műsorszolgáltatási jeleket a médiaszolgáltatótól az előfizető, vagy felhasználó vevőkészülékéhez továbbítják, függetlenül az alkalmazott átviteli rendszertől, és technológiától. Műsorterjesztésnek minősül különösen a műsorszórás, a műholddal végzett műsorterjesztés, a hibrid üvegszálas-koaxiális átviteli rendszeren végzett műsorterjesztés, emellett a műsor Internet Protokoll segítségével történő továbbítása valamely átviteli rendszeren, ha a szolgáltatás jellege, illetve feltételei megegyeznek a műsorterjesztéssel, illetve ez helyettesíti a más módon megvalósított műsorterjesztést. Műsorterjesztésnek minősül az olyan műsorterjesztés is, amelyhez az előfizető külön díj ellenében, vagy más elektronikus hírközlési szolgáltatás díjával csomagban értékesített díj ellenében férhet hozzá. (2003. évi C. törvény az elektronikus hírközlésről (Eht.) 188. § 74-77. pont).

[317] LONTAI et al. pp. 73-74.

[318] Szjt. 26. §

[319] Szjt. 28. §

[320] Például: ha az Antenna Hungária az MTV műsorát nyilvánossághoz földfelszíni sugárzás keretében eljuttatja (műsorszórás), akkor e tevékenység az elsődleges nyilvánossághoz közvetítés, az Antenna Hungária ebben az esetben az MTV sugárzási közreműködője. Ha ugyanez a szervezet mikrosugárzással is terjeszti az említett műsort, az már másodlagos az eredeti sugárzáshoz képest, tehát továbbközvetítés.

jogkezelő egyesületétől kaphatják meg. A műsorszolgáltató rádió- televízió szervezetek kizárólagos joga, hogy egyedi joggyakorlás keretében engedélyezzék díj ellenében műsoraik továbbközvetítését, műsorelosztási, vagy jeltovábbítási – jelelosztási szerződés alapján.[321]

1.5. A számítástechnikai szempont: a szolgáltatás és infrastruktúrája

A szolgáltató[322] az Eht. alapján elektronikus hírközlési szolgáltatónak minősül.[323] A szolgáltató a műsorszolgáltatók által előállított műsorjeleknek meghatározott programcsomagban történő egyidejű, változatlan továbbítását vállalja műholdas műsorszóró hálózaton az arra jogosult előfizető vevőkészülékéhez. Másként fogalmazva a szolgáltató műsorelosztóként több különböző műholdról vesz át műsorokat a műsorszolgáltatókkal kötött szerződése szerint, a műsorokat szolgáltatási csomagokba rendezi és ezeket a csomagokat saját vagy akár más szolgáltató eszközeivel teszi hozzáférhetővé az előfizetők számára.[324]

A szolgáltatás igénybevételének feltétele a szolgáltató által az előfizetőnek rendelkezésre bocsátott, a szolgáltatás igénybevételét biztosító berendezés (antenna, műholdvevő beltéri egység). A szolgáltatás igénybevételének további feltétele a beltéri egységhez kapcsolódó előfizetői kártya, melyet a szolgáltató az előfizetői szerződés tartamára az Előfizető használatába ad, azonban az a szolgáltató tulajdonában marad. A kártyán található adatok a szerződés szerinti műsorcsomagok elérhetősége szerint előfizetésenként eltérőek. Az előfizető tehát általában a tetőn elhelyezett parabolaantennát használva azon adott pályaadatú műholdakról való műsorvételre szerez jogosultságot, amelyekről a szolgáltató továbbítja a műsorokat. Mind a szolgáltatások, mind a berendezések számos kiskereskedelmi forrásból elérhetők az előfizetők számára.

A szolgáltatás digitális adattovábbításon alapuló számítástechnikai rendszeren keresztül történik, a műsort (filmet, zeneszámot, stb.) egy számítógép digitális jellé alakítva a műholdra továbbítja, innen digitális jelként érkezik a parabola antennára szerelt vevőfejen keresztül a dekódolást szolgáló vevőkészülékbe, amely azt vagy digitális jelként vagy analóg jellé alakítva továbbítja az azt kezelni tudó televízió készülékhez. Ez az egész tehát egy számítástechnikai rendszert alkot, a dekóder, az abban lévő szoftver és kód rendszerelem illetve adat. Azaz szolgáltatás technikai hátttereként, infrastruktúrájaként a fent részletezett eszközök összessége a Btk. 300/F. § (3) bekezdése alapján – amivel adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés

[321] LONTAI et al.pp. 76-78.
[322] Például: DigiTV, UPC, stb.
[323] ***Elektronikus hírközlési szolgáltatás:*** olyan, más részére általában ellenszolgáltatásért végzett szolgáltatás, amely teljesen vagy nagyrészt jeleknek elektronikus hírközlő hálózatokon történő átviteléből, és ahol ez értelmezhető, irányításából áll, beleértve a távközlési szolgáltatásokat és a műsorterjesztésre használt hálózatokon nyújtott átviteli szolgáltatásokat, de nem foglalja magában az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások felhasználásával továbbított tartalmat szolgáltató vagy ilyen tartalom felett szerkesztői ellenőrzést gyakorló szolgáltatásokat, valamint nem foglalja magában az információs társadalommal összefüggő, más jogszabályokban meghatározott szolgáltatásokat, amelyek nem elsősorban az elektronikus hírközlő hálózatokon történő jeltovábbításból állnak. (2003. évi C. törvény az elektronikus hírközlésről (Eht.) 188. § 13) *Elektronikus hírközlési szolgáltató:* Elektronikus hírközlő hálózat üzemeltetője, valamint elektronikus hírközlési szolgáltatást nyújtó természetes, illetőleg jogi személy vagy jogi személyiséggel nem rendelkező gazdasági társaság. (Eht. 188. § 14.)
[324] A Digi Tv esetében ezek a műholdak az Intelsat 10-02, és a Thor műholdak.

vagy egymással kapcsolatban lévő ilyen berendezések összességéről van szó – számítástechnikai rendszernek minősül.[325]

1.6. A minősítés kérdése

1.6.1. Szerzői jogi törvény szerinti hatásos műszaki intézkedés kijátszása vagy...

Az Szjt 95. §-a alapján műszaki intézkedés minden olyan eszköz, alkatrész vagy technológiai eljárás, illetve módszer, amely arra szolgál, hogy a szerzői jog jogosultja által nem engedélyezett cselekményeket – rendeltetésszerű működése révén – megelőzze, illetve megakadályozza. A műszaki intézkedést akkor kell hatásosnak tekinteni, ha a mű felhasználását a jogosultak a hozzáférést ellenőrző vagy védelmet nyújtó olyan eljárás – különösen kódolás vagy a mű egyéb átalakítása, vagy másolatkészítést ellenőrző mechanizmus – útján ellenőrzik, amely alkalmas a védelem céljának elérésére. Az intézkedés a hozzáférést, vagy a mű felhasználását, rendszerint másolását akadályozza. Azaz a vizsgált esetben az intézkedés vélelmezhetően túlcsordul a szerzői jog által ellenőrzött felhasználás körén.

Az említett jogszabályhely alapján a szerzői jog megsértésének következményeit kell alkalmazni a szerzői jog védelmére szolgáló hatásos műszaki intézkedés megkerülésére, feltéve, hogy az említett cselekményt olyan személy hajtja végre, aki tudja, vagy akinek az adott helyzetben általában elvárható gondosság mellett tudnia kellene, hogy a cselekmény célja a műszaki intézkedés megkerülése. A szerzői jog megsértésének következményeit kell alkalmazni olyan eszköz, termék vagy alkatrész előállítására, behozatalára, terjesztésére, eladására, bérbeadására, eladás vagy bérbeadás céljából történő reklámozására, kereskedelmi céllal való birtoklására, illetve olyan szolgáltatás nyújtására, amelyet a hatásos műszaki intézkedés megkerülése céljából kínálnak, reklámoznak vagy forgalmaznak; amelynek a hatásos műszaki intézkedés megkerülésén kívül nincs számottevő gazdasági jelentősége, illetve célja; vagy amelyet elsősorban a hatásos műszaki intézkedés megkerülésének lehetővé tétele vagy megkönnyítése céljából terveztek, gyártottak, alakítottak át, illetve teljesítettek.

1.6.2. ... számítástechnikai rendszer védelmét szolgáló intézkedés kijátszása?

A számítástechnikai adat megvédése érdekében minden esetben céltudatos, tervszerű emberi magatartás szükséges, amely a kívánt emberi magatartásokat előírások (jogszabályok, szabályzatok, szabványok stb.) formájában rögzíti. Ebben az értelemben a biztonság az információs- és informatikai rendszerekben olyan előírások betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik. Az adatbiztonság megvalósítása védelmi tevékenységek sorozatát jelenti. Más megfogalmazásban az informatikai biztonság alatt valamely informatikai rendszer azon állapota értendő, amelyben a kockázatokat, amelyek ezen informatikai rendszer bevezetésekor a fenyegető tényezők alapján adottak, elfogadható intézkedésekkel elviselhető mértékűre csökkentettük. Az informatikai biztonság két alapterületet foglal magába: információvédelem – amely az adatok által hordozott információk sértetlenségének, hitelességének és bizalmasságának elvesztését hivatott megakadályozni – és az informatikai rendszer megbízható működése területét – amely az adatok rendelkezésre állását és a hozzájuk kapcsolódó alkalmazói rendszerek funkcionalitását hivatott biztosítani. Tehát a fejezet szempontjából azok a

[325] Btk. 300/F. § (3) bekezdés.

műszaki intézkedések relevánsak, amelyek a számítástechnikai rendszer védelmét garantálják.

A szolgáltató által, a szolgáltatás igénybevételéhez szükséges dekóder beállításaival (szoftverével) biztosítja, hogy szolgáltatását illetéktelen személy ne vehesse igénybe. A szolgáltatást jogszerűen igénybe vevő ügyfelek egy, a szolgáltató által rendelkezésükre bocsátott, de nem átruházott készülékbe a szolgáltató által adott kártya alkalmazásával táplálják a szolgáltatást elérését biztosító adatokat, kódokat. Ha az elkövető egy eleve nem a szolgáltató által biztosított szoftverrel üzemeltetett dekódert alakít át, és a szolgáltató által folyamatosan frissített biztonsági kódok jogosulatlan felhasználásával tesz alkalmassá a szolgáltatás élvezetéhez, akkor ebben az esetben a számítástechnikai rendszer védelmét szolgáló intézkedést játsza ki. Az elkövető az adatok bevitelét, módosítását ugyan jogtalan haszonszerzés végett hajtja végre, azonban kárt nem okoz, hiszen az elmaradt haszonként jelentkező, díjfizetés elmulasztása – amelynek csak egy része az ügyfelekre áthárított jogdíj – vagyoni hátrányt eredményez, ezért a Btk. 300/C. § (3) bekezdés b) pontja már nem állapítható meg.

1.7. Az elkövetők és cselekményük minősítése

1.7.1. A „keresleti" oldal, akik az átalakított készüléket megvásárolják

A „keresleti" oldal által a minősítés kérdéskörébe vont cselekmény a következő kérdést veti fel. Miként minősül annak a cselekménye, aki a más által módosított műholdvevő készüléket a megvásárolja, és a szolgáltató szolgáltatását előfizetés nélkül, vagy az előfizetés kereteit túllépve veszi igénybe? Elsőként azt kell eldönteni, hogy szerzői jogi bűncselekmény elkövetése történt-e vagy valamilyen más vagyoni érdekeket sértő cselekmény.

A szerzői jogi minősítés körében a hatásos műszaki intézkedés megkerülésében megnyilvánuló jogsértés jelen esetben a hatásos műszaki intézkedés olyan megkerülése esetén állapítható meg, amikor a változtatás eredményeképpen szerzett haszon mellett a változtatónak nincs a megkerülés lehetővé tételén túl más gazdasági érdeke. Tehát a kódolt adás vételére alkalmas dekóder nem jogosult részére történő értékesítése nem jöhet szóba, továbbá az átalakításnak köszönhetően a szolgáltatás igénybevétele már maga is egy súlyosabb jogsértésnek tekinthető, amelybe az intézkedés megkerülése beleolvad. A saját felhasználás – műérzékelés vagy szolgáltatás igénybevétele – céljára történő megkerülés tehát nem esik a rendelkezés hatálya alá, nem a Btk. 329/B. §-a szerint minősül, hanem a 329/A. §-a szerint.

Másként fogalmazva, ha a saját célú megkerülés felhasználást eredményez, és az nem engedélyezett (pl. szoftver-kód feltörése saját célú futtatásra), akkor szóba kerülhet a szerzői jogsértés, amely azonban már magába olvasztja az intézkedés megkerülését. Ha pedig a megkerülés csak meg nem engedett műérzékeléshez vezet (jelen esetben, ha a néző a kódolt adás kódját feltöri a műsor érzékelése céljából), akkor általános polgári jogi jogkövetkezményekkel lehet számolni, hiszen ebben az esetben az elkövető csak áttételesen sérti a szerzői és szomszédos jogi jogosultak vagyoni érdekeit. Amennyiben elfogadjuk a műsorhordozó jelek tárolását a műholdvevő és televízió készülékekben többszörözésként, akkor is felmerül a magáncélú felhasználás – mint büntethetőséget (jogellenességet) kizáró ok – alkalmazásának lehetősége. Emellett a cselekmény alapvetően polgári jogi kötelem megsértésében áll, egy hasonló példával élve jelen

cselekmény társadalomra veszélyessége ugyanolyan csekély fokú, mint egy művészeti kiállítás belépő díj megfizetésének hiányában történő látogatása.

Számítástechnikai bűncselekményként történő értelmezés esetén a következők állapíthatók meg. Mivel a bűncselekmény elkövetőjének bűnösségét is vizsgálni szükséges a büntetőjogi felelősség megállapítása során, nem mellőzhető az elkövető szándékának szemügyre vétele. A Legfelsőbb Bíróság a BH2002.301 számú eseti döntésben is kifejtette álláspontját, amely szerint a büntetőjogi és polgári jogi felelősség nem azonos fogalmak, az egyik nem szükségszerűen előfeltétele a másiknak. Szándékos bűncselekményről lévén szó, a kérdés az, hogy mire terjed ki az elkövető tudata. A szerzői jogi jogsértésre, vagy a „televíziós" szolgáltatás előfizetői díj ellenében történő igénybevételének lehetővé tételére? A „fogyasztói" oldalt tekintve a szerzői jogi védelem és érdekek meglehetősen áttételesen jelennek meg, mivel – ismételten kiemelendő – az előfizető nem jogdíjat fizet a műsor érzékeléséért, hanem a szolgáltató szolgáltatásának ellenértékét fizeti meg havidíjként, a közös jogkezelőkkel egyébként sincs semmilyen kapcsolatban. A jogdíjat a műsorelosztó szolgáltató fizeti meg a közös jogkezelők vagy a műsorszolgáltatók számára, amely összeg független az előfizetőtől abban a tekintetben, hogy a szolgáltatás igénybevételének nem feltétele a jogdíj előfizető által történő megfizetése. Az elkövető tudata ekként – az átlagos állampolgár médiajogi és szerzői jogi ismereteire is figyelemmel – eshetőlegesen sem terjed ki a szerzői jogi jogsértésre.

A készüléket megvásároló felhasználók, akik az átprogramozott készüléket megveszik és a műsort szolgáltatási díj megfizetése nélkül élvezik, a Btk. 300/E. § (1) bekezdés b) pontja szerinti bűncselekményt követik el. Amennyiben a végfelhasználó az interneten megszerzett kódot saját maga viszi be – pl. a távirányítója segítségével „manuálisan" – akkor viszont a Btk. 300/C. § (2) bekezdés b) pontja szerint minősülő bűncselekményt követ el.

1.7.2. A „kínálati" oldal

A kérdés ebben az esetben az, hogy miként minősíthető annak az elkövetőnek a cselekménye, aki egy nem a rendeltetése szerinti célra kifejlesztett dekódert alakít át a program átírásával úgy, hogy a programot megváltoztatja, majd lehetővé teszi, hogy az internetről letöltött kódokat a készülék távirányítójának segítségével akár ő vagy más „manuálisan" vigye be a készülékbe és nem a szolgáltató megfelelő adatait tartalmazó adatkártyája alkalmazásával. A fenti szerzői jogi és médiajogi ismeretek birtokában az említett cselekmény egyaránt minősíthető a Btk. 329/B. § megfelelő fordulatai és a 300/C. § bekezdései szerint. Amennyiben az elkövető a rendszeres haszonszerzésre törekedve az átalakított készülékeket hirdeti, forgalmazza, szintén megállapítható mindkét szakasz szerinti bűncselekmény megfelelő fordulata (üzletszerűség, kereskedés).

Mindez azért érdekes dogmatikailag, mivel a 329/B. § egy másik – a 329/A. §-hoz – képest sui generis előkészületi és bűnsegédi jellegű bűncselekmény, míg a számítástechnikai vonalon a 300/C. § maga is egy célzott bűncselekmény és a 300/E. § szintén sui generis előkészületi és bűnsegédi jellegű bűncselekménynek tekinthető. Máshogyan fogalmazva, milyen alapon lehet felelősségre vonni egy sui generis előkészületi cselekmény (329/B. §) elkövetőjét, ha maga a célzott cselekmény elkövetője, az átalakított készüléket megvásárló felhasználó nem valósít meg magatartásával a Btk. 329/A. §-a alá eső bűncselekményt?

A jogdíj és szolgáltatási díj kapcsolata és az elkövetés tárgya szerinti érvelés miatt az elkövető cselekménye a haszonszerzés miatt a Btk. 300/C. § (3) bekezdés a) vagy b) pontja

szerint minősülhetne, mert a terhelt szándéka, hogy az átalakított készüléket értékesítve jogtalan haszonra tegyen szert. Azonban az elmaradt haszon büntetőjogilag nem kárnak, hanem vagyoni hátránynak minősül, így csak a (2) bekezdés jöhet szóba. Ha a 300/C. § nem is, a 300/E. § (1) bekezdése megállapítható. Az a személy pedig, aki az interneten a programozási módszert közzéteszi, elköveti a Btk. 300/E. § (2) bekezdését, ha pedig a megváltoztatott program működését biztosító, a szolgáltató által időközönként megváltoztatott és ezt követően kézzel bevihető kódot teszi közzé az interneten, az a Btk. 300/E. § (1) bekezdés c) pontja szerint minősülő cselekményt követi el.

1.8. A szerzői jogi jogsértés

Az értekezésben eddig vizsgált jogeset középpontjában a szolgáltató szolgáltatásainak igénybevétele állt, és a vizsgált jogszabályhelyek értelmezése alapján arra a következtetésre lehetett jutni, hogy egyfajta számítástechnikai bűncselekményként lehet minősíteni a cselekményt, nem pedig szerzői jogi jogsértésként. A jogesetben azonban alaki halmazatként felmerül szerzői jogi jogsértés, de nem a szolgáltató sérelmére, hanem az egyébként kereskedelmi forgalomban beszerezhető dekóder szoftverének jogtulajdonosa vonatkozásában. A jogosultat ugyanis megilleti a mű integritásához való jog, amely sérelmet szenved abban az esetben, ha az elkövető a szoftveren engedély nélküli átalakításokat végez el.

2. A „WI-FI LOPÁS" ESETE

A jogbiztonság kiemelkedően súlyos sérelmét jelentette az 2007. évben történt szabálysértési ügy, amely lopással elkövetett tulajdon elleni szabálysértésnek minősített azt az idegen kifejezéssel élve wardriving-nak nevezett esetet, amikor egy férfi más személy előfizetésében lévő, nem védett, nyitott wifi-hálózatot kutatott fel és arra csatlakozva adatforgalmat bonyolított le, amely az adatforgalmi korlátos kapcsolatra miatt kiszámíthatóan 3,79 megabájtnyi adat volt kb. kilenc forint értékben.

Mivel a lopással elkövetett tulajdon elleni szabálysértés lényegét tekintve a lopás büntetőjogi dogmatikáját veszi alapul, így a döntés az alkotmányos büntetőjogi elvekkel összevethető. Mi volt az alapvető probléma az említett döntésben? Először is lopás tárgya dolog lehet, amelynek fogalmát a Btk. 333. §-a egyfajta törvényi analógia keretében kiterjeszti a villamos- és a gazdaságilag hasznosítható más energiára is. A wifi mikrohullámú alapú, tehát vezeték nélküli kommunikációt megvalósító szabvány (IEEE 802.11) elnevezése, tehát nem energia, ekként nem is dolog. Mivel eleve kiesik a dolog mint elkövetési tárgy fogalma alól, a wifi-re vonatkozóan fogalmilag kizárt a lopás megvalósulása. A Btk. 300/C. § tényállásai sem alkalmazhatók jelen estben, hiszen egyrészt nem történt védelmi intézkedés kijátszása, másrészt a (2) és (3) bekezdéseket illetően szintén nem állapítható meg elkövetési magatartás, mivel nem volt adatokat érintő manipuláció, valamint a számítástechnika rendszer működésének akadályozása sem. Természetes személy megtévesztésének hiányában a csalás sem jöhet szóba. Megállapítható tehát, hogy a magyar büntető- és szabálysértési jog nem szankcionálja a wardriving jellegű cselekményeket.

A cselekmény a korábbi korszakok kriminalizációs tervei között még „szolgáltatáslopás"-ként szereplő deliktumként lenne szankcionálható. A cselekmény ugyan nem minősíthető a Computer Misuse Act 1990. korábban elemzett tényállásainak egyikének sem, azonban a Communication Act 2003. 125. szakasza szerint büntethető. Emlékeztetőül: szolgáltatás jogosulatlan igénybevételét valósítja meg, aki kommunikációs szolgáltatást úgy vesz

igénybe, hogy az adott szolgáltatásra vonatkozó szabályok szerinti ellenszolgáltatás teljesítését elkerülje.

De lege ferenda érdemes megfontolni – természetesen a megfelelő büntethetőségi határok meghúzásával – új tényállás alkotását.

3. A BANKI ÁTUTALÁSOK ESETEI

3.1. A bankautomata-ügy

Egy újabb, minősítési kérdéseket felvető jogesetet a következő cselekmény jelenti. Az elkövető egy hazai pénzintézetnél létesít folyószámlát, amelyre egy, a pénzintézet üzemeltetésében lévő automatán keresztül, bankkártyája felhasználásával százezer forint összeget helyez el. Az elkövető rövid időn belül egy konkurens pénzintézet banki automatájából felveszi a százezer forint pénzösszeget, majd azt a számlavezető bank automatáján keresztül ismét befizeti. Ezt a műveletet rövid időn belül többször – példának okáért négy alkalommal – ismétli meg. Az elkövető haszonszerzési szándéka azon felismerésen alapult, hogy a két különböző pénzintézet által üzemeltetett banki informatikai rendszerek nem írták jóvá azonnal a folyószámlát érintő valamennyi tranzakciót, azaz az elkövető cselekményének végére a számítástechnikai rendszerben a számítástechnikai adatok formájában létező folyószámláján összesen – a példánál maradva – négyszázezer forint létezését igazoló számítástechnikai adat szerepelt. Az ilyen módon generált összeget az elkövető cselekménye végén egyszerre felvette egy automatán keresztül.[326]

A cselekmény természetesen nem minősül készpénz-helyettesítő fizetési eszközzel visszaélésnek, mivel az elkövető a jogszabályoknak megfelelően folyószámla és bankkártya-szerződést kötött a pénzintézettel, azaz a bankkártya használatára jogosult volt.

A cselekmény a Btk. 300/C. § (3) bekezdés a) pontjába ütköző számítástechnikai adatok elleni bűncselekmény bűntettének gyanúját veti fel, hiszen jóllehet mechanikus úton – bankjegyek automatába való betételével – számítástechnikai adatokat vitt be számítástechnikai rendszerbe. Minderre természetesen jogosultsággal bír, azonban rosszhiszeműsége abban nyilvánult meg, hogy a banki informatikai rendszerek egymás felé történő elszámolásában felfedezett hibát felismerve a rendelkezésére álló nagyobb pénzösszeget hívott le. Mindez önmagában egyszerű számlakeret-túllépésnek, hitelnek tűnhet, azonban a kérdés az, hogy másként értelmezve megvalósítja-e számítógépes csalást vagy sem. E másként értelmezés alapja az, hogy az ismételt informatikai műveleteknek minősülő számla-jóváírásokkal és terhelésekkel tudottan hamis számítástechnikai adatokat vitt be és módosított számítástechnikai rendszerben, majd cselekményével kárt okozott.

3.2. A bankkártya-ügy

Egy szintén készpénz-helyettesítő fizetési eszközhöz (bankkártya) köthető elkövetési magatartás során az elkövető a más nevére kiállított bankkártya azonosító számát használja fel akként, hogy online fizetés során a bankkártya sorozatszámát adja meg. A bankkártyához tartozó folyószámláról a fizetést elfogadó online üzlet később lehívja a megfelelő összeget.

[326] Miskolci Városi Ügyészségen B.1482/2011. számon indult büntetőügy.

A cselekmény minősítése azon okból lehet vitatott, hogy valójában mi tekinthető az elkövetés tárgyának. A készpénz-helyettesítő fizetési eszköz a bankkártya, aminek chip- vagy mágnescsíkos része tartalmazza az ügyfél és a kibocsátó tulajdonos, a pénzintézet azonosító adatait. Az elkövető cselekménye mindezeket nem érinti, kizárólag a bankkártya sorozatszáma került felhasználásra. Az eldöntendő kérdés, hogy mi minősül készpénz-helyettesítő fizetési eszköznek és mi annak felhasználásának. Amennyiben a sorozatszám a kártya birtoklásától függetlenül készpénz-helyettesítő fizetési eszköznek minősül, akkor ebben az esetben a cselekmény minősítése is ekként alakul.

Amennyiben egy egyszerű számsorozatot nem tekintünk készpénz-helyettesítő fizetési eszköznek, akkor az online fizetést lebonyolító számítástechnikai rendszerbe a sorozatszám számítástechnikai adatként kerül be, csupán felhasználó személye nem a jogosult. Ebben az esetben a cselekményt a Btk. 300/C. § (3) bekezdés a) pontja alapján kell minősíteni. Szóba kerülhetne a Btk. 318. § rendelkezéseibe ütköző csalás bűncselekménye is, ha úgy értelmezzük, hogy tévedésbe ejtem a megrendelő személyét illetően az eladót és a kár a tényleges kártya, illetve számlatulajdonosnál jelentkezik. Azonban ebben az esetben az elkövető nem az eladó személyét téveszti meg, csupán egy online fizetést lebonyolító szoftvert, ezért a csalás nem jöhet számításba.

4. A LÉZERES TRAFFIPAX-BLOKKOLÓ KÉSZÜLÉKEK ESETE

Számos vitát generált az úgynevezett lézeres traffipax-blokkoló berendezések alkalmazása és annak jogi megítélése. Egy ilyen készülék alkalmazójával szemben a Gyulai Városi Ügyészség emelt vádat 2010-ben a Btk. 300/C. § (2) bekezdés b) pontjába ütköző számítástechnikai rendszer és adatok elleni bűncselekmény vétsége miatt. A továbbiakban egy cselekmény büntetőjogi megítélését vizsgálom arra figyelemmel, hogy mely jogszabályi hiányosság vezetett a fenti minősítéshez.

A gépjárműről és annak hatósági jelzéséről felvételt készítő eszközre vonatkozó követelményekről szóló 18/2008. (IV. 30.) GKM rendelet meghatározza azokat a követelményeket, amelyeknek a köznyelvben csak traffipaxként nevezett ellenőrző készülékeknek meg kell felelniük. A rendelet alkalmazása tekintetében elektronikus közúti ellenőrző rendszernek minősül egy vagy több ellenőrző berendezés és az ezekkel összehangoltan kialakított elektronikus adattovábbító rendszer együtt.[327] Az elektronikus adattovábbító rendszernek minősül az ellenőrző berendezés által dokumentált adatok közigazgatási, szabálysértési és büntetőeljárás során történő felhasználását lehetővé tevő adattároló, illetve adattovábbító rendszer.[328] Az elektronikus közúti ellenőrző rendszer, illetve annak részegységei akkor üzemeltethetők, amennyiben az elektronikus adattovábbító rendszer összekapcsolható a rendőrség által működtetett elektronikus informatikai rendszerrel, valamint megfelel a rendelet mellékletében meghatározott követelményeknek.[329] A rendelet melléklete alapján az ellenőrző berendezés működéséről és működése során keletkezett számítástechnikai adatokat belső adathordozóra rögzíti, majd azokat online kapcsolattal a feldolgozó központba, az ORFK TrafficPoint rendszerébe. A lézeres traffipaxok működésének követelménye tehát a folyamatos (GSM) kapcsolat a TrafficPoint rendszerrel, ahova a kezelő saját felhasználónévvel és jelszóval jelentkezik be. Mindezek alapján megállapítható, hogy a lézeres sebességmérő készülék és

[327] 18/2008. (IV. 30.) GKM rendelet 2. § f) pont
[328] 18/2008. (IV. 30.) GKM rendelet 2. § e) pont
[329] 18/2008. (IV. 30.) GKM rendelet 3. §

a vele összekapcsolt feldolgozó központ számítástechnikai rendszernek minősülnek egyeként és együttesen is.

A berendezés működésének elve alapján a mérő és dokumentáló egység által kibocsátott lézersugár a távolsággal arányosan növekvő átmérőjű kúp alakban szóródik és a gépjárművek sebességét adattárolójában rögzíti, amely adatokat központi feldolgozó rendszerbe továbbítja. A sebességmérő készüléket blokkoló berendezés működésének lényege abban áll, hogy a lézersugarat észlelve a mérőműszer számára értelmezhetetlen választ küld.

Miért vitatott a blokkoló használatának jogi megítélése? Egyes vélemények szerint a készülék használata a Btk. 300/C szakasz (2) bekezdés b) pontjába ütköző számítástechnikai rendszer és adatok elleni bűncselekmény vétségét valósítja meg. Kérdésként merül fel, hogy e vélekedés helyénvaló-e vagy sem. A blokkoló készülék alkalmazása a traffipax számítástechnikai rendszerébe nem visz be adatot, nem töröl adatot, nem változtat meg adatot, egyedüli elkövetési magatartásként az „egyéb művelet végzése" kerülhet szóba. Itt értelmezésre szorulna az egyéb művelet fogalma, hiszen informatikai értelemben a művelet elsősorban a matematikai-logikai alapműveleteket jelöli (igaz-hamis), de a számítástechnikai rendszer egyes funkcióinak alkalmazását, valamint az adatokon, adatokkal végezhető valamennyi tevékenységet is felölelheti (adatok törlése, továbbítása, többszörözése, megváltoztatása, stb.). A művelet tehát a számítástechnikai rendszer működését közvetlenül befolyásoló beavatkozásnak tekinthető. Ezért a Legfőbb Ügyészség álláspontja szerint a blokkoló használata nem a sebességmérés során keletkezett adatokat kezelő és feldolgozó számítástechnikai rendszer, hanem az attól elkülöníthető sebességmérő készüléknek – kizárólag a mérési funkció megzavarása útján történő – működését akadályozza, tehát magát az adatbevitelt zavarja meg.[330] Az a tény azonban, hogy a készülék által mért adatokat digitálisan dolgozzák fel, a bűncselekmény megvalósulása szempontjából irreleváns.

Ezzel az állásponttal ellentétes eredményre juthatunk, amennyiben a sebességmérő készüléket egyfajta hálózatnak, egy egymással kapcsolatban lévő berendezésekből álló számítástechnikai rendszer egyik elemének tekintjük. A korábbi fejezetekben hivatkozott ábra alapján a számítástechnikai rendszer funkcionalitását, működőképességét akadályozhatja valamely rendszerelem elleni támadás is.

Bár a büntetőjogban kizárt az analógia alkalmazása, mégis elgondolkodtató a WLAN (vezeték nélküli hálózatok) működését támadó berendezések alkalmazásának megítélése is. A rádióhullámok fizikai közegében működő WLAN hálózat működésének zavarása legegyszerűbb módon a fizikai, illetve az adatkapcsolati rétegben valósítható meg.[331] A blokkoló berendezések működési elvük szerint a készülék körzetében minden olyan rádiós kommunikációt meggátolnak, ami a működési frekvenciatartományban folyna. Ebben az esetben a számítástechnikai rendszer elleni bűncselekmény csak akkor lenne megállapítható, amennyiben a cselekményt két rendszerelem közötti kommunikációt megakadályozó „egyéb műveletnek" tekintjük. Amennyiben tehát kizárnák számítástechnikai rendszer elemei közötti kommunikáció fizikai közegére irányuló támadást a tényállás keretei közül, az hosszú távon komoly hátrányokhoz vezetne. A két eset közötti különbség, illetőleg az utóbbi érvelés gyengeségét az jelenti, hogy a traffipax működése során nem valamely más rendszerelemmel törekszik kommunikálni.

[330] A Legfőbb Ügyészség Kiemelt Ügyek Főosztályának állásfoglalása. (KF.1036/2011/2-6.)
[331] GYÁNYI S., Informatikai WLAN-hálózatok zavarása. *Bolyai Szemle* 2009/4. p. 124.

Megállapítható tehát, hogy a jelenlegi szabályozás alapján a traffipax blokkoló készülékek alkalmazása nem valósítja meg a számítástechnikai rendszer és adatok elleni bűncselekmények bűntettét, azonban az „egyéb művelet" kifejezés elég bizonytalan és pontatlan ahhoz, hogy a büntethetőség kereteit egyértelműen, a jogbiztonság elvárásainak megfelelően jelölje ki.

Egy további probléma, hogy a szenzorok működésének akadályozása a tényállás értelmezése szerint nem büntethető, mivel azok a környezetből származó ingereket érzékelik és azokat számítástechnikai adatokba átalakítva továbbítják a számítástechnikai rendszerbe. A környezet és a szenzor közötti fizikai közeg megzavarása viszont kívül esik magán a rendszeren, a rendszer működését nem akadályozza, az ilyen cselekmény egyszerűen értelmezhetetlen adattal látja el a szenzoron keresztül a rendszert, vagy az adatoktól megfosztja. Jóllehet a rendszer működését nem akadályozza a cselekmény, azonban a rendszer funkcionalitását igen. Ezért a jövőre tekintettel mihamarabb rendezni indokolt a szenzorok működésére vonatkozó szabályozást.

5. A FEJEZET ÖSSZEFOGLALÁSA

Az említett jogeseteken kívül még számos okoz fejtörést a gyakorlat számára, például a már korábban említett játékautomaták működésének befolyásolása, vagy a gépjárművek fedélzeti számítógépének átprogramozása a gépkocsi eltulajdonítása céljából, amely értelmezhető dolog elleni erőszakkal elkövetett lopásként éppúgy mint a lopás és számítástechnikai bűncselekmény halmazataként. Úgy tűnhet, hogy a fejezetben felhozott jogesetek egyenként nem jelentenek komoly értelmezési gondot, azonban összességükben véve látható, hogy az IKT általános elterjedése okán számos bizonytalansági elemet hordoznak magukban. Gondoljunk arra, hogy például a beltéri egységek ügyében a különböző értelmezési lehetőségek révén más-más, egyik esetben szűkebb, másik esetben szélesebb elkövetői kör vonható a büntetőeljárás keretei közé, amely az érintett számára igenis súlyos következményekkel jár éppúgy, mint a halmazat büntetéskiszabási szabályaiban rejlő súlyosabb szankció lehetősége. A számítástechnikai rendszerek elleni különböző támadások, behatások célja sok esetben nem maga a rendszer működésének akadályozása, az csak járulékos, szükségszerű eszközcselekmény egy másik jogtárgy sértése érdekében, önmagában ezen körülmény azonban nem teszi meg nem állapíthatóvá a bűncselekményt valamely más deliktummal halmazatban. Egy következtetés kétséget kizáróan megállapítható a fejezet alapján, mégpedig az, hogy a technológiai fejlődés, a konvergencia bizony olyan új jogi helyzeteket teremt, amit a büntetőjog a maga tradicionális kategóriáival és helyesen merev alapelvekre épülő dogmatikájával jelenleg még nehezen tud feloldani, az újabb és újabb tényállások kreálása pedig szintén nem vezet jóra.

IX. FEJEZET: ELJÁRÁSI KÉRDÉSEK

Az informatikai bűncselekmények nyomozását számos olyan körülmény nehezíti, amelyek legyőzéséhez a bűnüldöző hatóságok nagy része még nem rendelkezik megfelelő technológiai, tudásbeli, vagy jogszabályi háttérrel. A következő pontokban a teljesség igénye nélkül sorolok fel olyan tényezőket, amelyek a nyomozást hátráltathatják.

Ilyenek körülmények például, hogy az elkövetéskor nem a klasszikus értelemben vett tárgyi jellegű nyomok keletkeznek, a számítástechnikai hálózaton folytatott kommunikáció biztosít egyfajta anonimitást az elkövetőnek, az elkövetés gyakran több államot is érint, nehezen értelmezhető az elkövetés helye, ugyanakkor lassítja a nyomozást a nemzetközi büntetőjogi együttműködés folyamata is. Kétséges lehet a bűncselekmény észlelése, de a sértettnek is lehetnek a felderítéssel ellentétes érdekei, amennyiben számítástechnikai rendszerén olyan adatokat tárol, amelyek nyilvánosságra kerülése gazdasági tevékenységében károsítaná.[332] Nem jelentéktelen nehézséget jelent az állam bűnüldözési érdekének és a polgárok személyi szabadságának ütközése a nyomozás és adatszerzés során. A minőségileg új típusú bűncselekmények eltérő módszerű nyomozását nehezíti továbbá sok esetben a jogalkotás lemaradása is, hiszen a korábbi eljárási szabályok a fizikai világ normáihoz igazodtak, egyes szabályok nem alkalmazhatók, sőt egyszerűen értelmezhetetlenek a virtuális térben.[333] A felsorolt nehézségek miatt a büntetőjogi felelősségre vonáshoz szükséges és beszerezhető bizonyítékok száma, fajtája szűkös, noha a digitális bizonyítékokon kívül legtöbbször aligha áll rendelkezésre más eszköz.

Az informatikai bűncselekmények nyomozásának problematikáját a bűnüldöző hatóságok együttműködésének tükrében megoszthatjuk a nyomozás belföldi és nemzetközi aspektusainak elemzésére.

1. A BIZONYÍTÁS CÉLJA ÉS ALAPELVEI

1.1. A bizonyítás

A bűncselekmény által a külvilágban okozott változás elemeinek felkutatása, azoknak az okozattól kiindulva egy logikai láncra történő felfűzése, majd az ok felismerése, és mindezeknek az előírt hatóság előtt történő próbára tétele jelenti a bizonyítás folyamatát. Bizonyításon a bíróság, az ügyész, a nyomozó hatóság és más alanyok cselekményeinek sorát értjük, amelyek arra irányulnak, hogy ismereteket nyújtsanak, illetve szerezzenek arról, történt-e bűncselekmény, és annak ki az elkövetője.[334] A fejezet a bizonyítás előbb idézett tág felfogása mellett csupán a nyomozó hatóság által végzett bizonyítékgyűjtés és az ügyészség nyomozás-felügyeletére koncentrál.

A Be. 75. § (1) bekezdése alapján a bizonyítás azokra a tényekre terjed ki, amelyek a büntető és a büntetőeljárási jogszabályok alkalmazásában jelentősek, és a bizonyítás során a tényállás alapos és hiánytalan, a valóságnak megfelelő tisztázására kell törekedni. A Be. 76. § (1) bekezdése szerint a bizonyítás eszközei a tanúvallomás, a szakvélemény, a tárgyi bizonyítási eszköz, az okirat és a terhelt vallomása.

---

[332] LACZI B., A számítógépes környezetben elkövetett bűncselekmények nyomozásának és nyomozás felügyeletének speciális kérdései. *Magyar Jog*, 12/2001. p. 727.
[333] PARTI K., Az internetes bűncselekmények nyomozásának egyes kérdései. *Kriminológiai tanulmányok*, 41. szám. 2004. p. 249.
[334] KIRÁLY T., *Büntetőeljárásjog.* Osiris Kiadó Budapest, (Negyedik kiadás) 2008. p. 240.

1.2. A bizonyítás és a bizonyítékok összegyűjtésének alapelvei

1.2.1. A bizonyítás alapelve: a törvényesség

A Be. 77. §-a fogalmazza meg a bizonyítás törvényességének alapelvét. A törvényhely alapján a bizonyítási eszközök felderítése, összegyűjtése, biztosítása és felhasználása során e törvény rendelkezései szerint kell eljárni. Jogszabály elrendelheti a bizonyítási cselekmények teljesítésének, a bizonyítási eszközök megvizsgálásának és rögzítésének, valamint a bizonyítási eljárások lefolytatásának meghatározott módját. A bizonyítási cselekmények végzésekor az emberi méltóságot, az érintettek személyiségi jogait és a kegyeleti jogot tiszteletben kell tartani, és biztosítani kell, hogy a magánéletre vonatkozó adatok szükségtelenül ne kerüljenek nyilvánosságra.

A bizonyítás törvényességének elve szorosan illeszkedik a dolgozat alkotmányos büntetőjoggal foglalkozó fejezetének rendszerébe, annak főképp anyagi jogi vonala mellett, kiegészítéseként szerepel. A bizonyítékokat a Be. rendelkezései szerint kell tehát beszerezni, azonban figyelemmel kell lenni az eljáró hatóság működését meghatározó normarendszerre is. Amennyiben például egy szakértő szegi meg a rá vonatkozó előírásokat, a nyomozó hatóság vét a törvényesség elve ellen, ha nem észleli a hibát, és ha nem teszi meg a hatáskörébe tartozó intézkedéseket az észlelt hiba kiküszöbölése érdekében.[335]

1.2.2. A bizonyíték-megszerzés kriminalisztikai alapelvei: tárgyilagosság, teljesség, szakszerűség, hitelesség

A tárgyilagosság elve alapján a nyomozás során sem az eljárás lefolytatásának módjában, sem a tények feltárásában nem engedhető meg az elfogultság.[336] Az elfogulatlan eljárás jogi hátterét biztosítják többek között a Be. kizárásra vonatkozó szabályai, de az ártatlanság vélelme és az eljárási szerepek megosztása is. A teljesség elve alapján a nyomozás feladatait – ide értve a határidőhöz kötött és utólagos tennivalókat is – maradéktalanul el kell végezni, valamennyi bizonyítékot össze kell gyűjteni, és azok lefoglalása esetén az utólagos ellenőrzésükről és kezelésükről is gondoskodni kell.[337] A bizonyítékok beszerzése, rögzítése során szakszerűen, az alkalmazott technika szabályszerű alkalmazásával kell eljárni.

A hitelesség elve alapján a bizonyítékról kétséget kizáróan meg kell tudni állapítani származását, forrását, minta esetén annak eredetiségét, azonosságát, azaz biztosítani kell a bizonyíték visszavezethetőségét. A hitelesség olyan akkreditálási, minőségbiztosítási és minőség-ellenőrzési rendszerek fenntartását igényli, amelyek biztosítják az érvényes és megbízható módszerek alkalmazásának körülményeit.[338] A házkutatás, lefoglalás és bűnjelkezelés során hitelesség biztosításával a hatóságoknak azt kell mindent kétséget kizáróan igazolniuk, hogy a számítástechnikai adatok a megszerzést közvetlen megelőző állapotukat a büntetőeljárás során mindvégig megőrizték. A hiteles adatokon végzett

[335] LAKATOS J., A nyomozás – kriminalisztikai szempontból. In. Bócz E. (ed.), *Kriminalisztika.* BM Duna Palota és Kiadó Budapest, 2004. 131.
[336] LAKATOS, 2004. p.133.
[337] LAKATOS, 2004. p. 133.
[338] KERTÉSZ I., A szakértői bizonyítás. In. Bócz E. (ed.), *Kriminalisztika.* BM Duna Palota és Kiadó Budapest, 2004. p. 233.

vizsgálatok bármikor megismételhetők, a vizsgálat eredménye reprodukálható.[339] A hitelesség biztosítása érdekében számos intézkedésre van szükség. A szakértők tevékenységét illetően például gondoskodni kell kiképzésükről, továbbképzésükről, a vizsgálati módszerek, szabványok, útmutatók készítéséről, előírásáról és alkalmazásuk ellenőrzéséről. A hitelesség biztosítását célozza a bizonyítékok beszerzése (lefoglalás, házkutatás) során jegyzőkönyv felvétele, amelyben valamennyi, a bizonyítási eszközre vonatkozó információt rögzíteni kell. Példaként említve számítástechnikai adathordozó lefoglalása esetén a jegyzőkönyvben fel kell tüntetni annak egyedi azonosításra alkalmas jelzését, egy számítógépes hálózat vizsgálata esetén annak hálózati rajzát, felépítését, és minden lényeges műveletet, amit a bizonyíték rögzítése során az eljáró személy végez. A hitelesség megőrzése érdekében részletes szabályok vonatkoznak a bizonyíték tárgyi védelmére, a bűnjelkezelésre is.

1.3. Nyomozás célja

Bár a bűnösségről és a jogkövetkezményekről a végső szót a bíróság mondja ki, mindez nem jelenti a nyomozás másodrendűségét a tárgyaláson felvett bizonyítással szemben, hiszen számos – a tárgyaláson felhasznált – bizonyítási eszköz a nyomozás során nyeri el erejét, amennyiben szakszerűen, a törvényeknek megfelelően történt a beszerzése. A Be. 164. § (1) bekezdése szerint a büntetőeljárás első szakasza a nyomozás, a büntetőeljárás – ha e törvény eltérően nem rendelkezik – nyomozással kezdődik. A nyomozás feladata a (2) bekezdés szerint, hogy annak során fel kell deríteni a bűncselekményt, az elkövető személyét, fel kell kutatni és biztosítani kell a bizonyítási eszközöket. A tényállást oly mértékben kell felderíteni, hogy a vádló dönthessen arról, vádat emel-e.

2. KÜLÖNLEGES BIZONYÍTÉKOK

2.1. A digitális bizonyítékok

A számítógépes környezetben elkövetett bűncselekmények nyomozásának elemzésénél mindenekelőtt azt kell tisztázni, hogy hol és milyen formában találhatók a különböző bizonyítékok, ezek után kerülhet sor a lehetséges bizonyítékok törvényes beszerzésének tárgyalására. Az informatikai bűncselekmények nyomozásának és nyomozás-felügyeletének nehézségeit elkövetésük sajátosságai mellett a klasszikus bűncselekményektől eltérő bizonyíthatóságuk alapján érthetjük meg. Tekintettel arra, hogy az informatikai bűncselekmények elkövetéséhez legtöbbször számítógépet használ az elkövető, jelen fejezetben csupán a digitális bizonyítékokat majd azok megszerzésének törvényi feltételeit mutatom be, a klasszikus bizonyítási eszközöket – tanúvallomás, szemle, stb. – nem részletezem. Maga a nyomozás a technológia fokozott jelenléte ellenére nem bír olyan különleges sajátossággal, ami egy hatékony tanúkihallgatás metodikáját vagy az adatgyűjtést más bűncselekményekhez viszonyítottan eltérő módon befolyásolná.[340]

A digitális bizonyítékok alatt valamilyen elektronikus formában megjelenő, számítástechnikai eszközön tárolt, feldolgozott adatot értünk. Peszleg Tibor csoportosítása

[339] MATUS M., Kutatás, lefoglalás, bűnjelkezelés számítástechnikai környezetben. In. Bócz E. (ed.), *Kriminalisztika.* BM Duna Palota és Kiadó Budapest, 2004. p. 292.
[340] NEWVILLE, L. L., Cyber Crime and the Courts - Investigating and Supervising the Information Age Offender. *Federal Probation* [Vol. 65. No. 2], September 2001. p. 12.

alapján ezek az adatok lehetnek: digitális dokumentumok, digitális nyomok, valamint napló és regisztrációs adatok.[341]

A digitális dokumentumok lehetnek szöveges dokumentumok, könyvelési adatok, kép-fájlok, videó-fájlok, programok, stb.[342] Ezen adatok megismeréséhez legtöbbször különösebb szakismeret nem szükséges, az átlag számítógéphasználók körében könnyen felismerhetők, a számítógép háttértárán vagy hordozható adattárolón találhatók.

Speciális ismeret, szakértői tudás kell viszont a digitális nyomok felkutatásához. A kriminalisztika a nyomon olyan fizikai elváltozást ért, amely a bűncselekmény elkövetésével bármilyen kapcsolatban áll, és így lehetővé teszi, hogy a bűncselekmény megtörténtének tényére, vagy a tettes személyére nézve következtetéseket vonjanak le.[343] A bűnügyi nyomtan (traszológia) azonban ennél szűkebb jelentést tulajdonít a fogalomnak. A nyom a nyomképző külső felépítésének, szerkezeti, funkcionális tulajdonságainak a vizsgált eredmény során bekövetkezett eredményeként létrejött kölcsönhatások visszatükrözése.[344] Másként fogalmazva a nyom olyan elváltozás, amelyik visszatükrözi a nyomot létrehozó tárgy alakbeli és felületi sajátosságait és így nyújt lehetőséget a nyomot létrehozó eszköz vagy tárgy fajtájának megállapítására, illetőleg azonosítására.[345] A digitális nyomok a számítástechnikai eszköz, program működése közben keletkezett, a számítástechnikai eszközök által rögzített adatok, amelyek a működés közben ideiglenesen létrehozott, törölt és felülírt adat-állományokból állíthatók vissza. A digitális nyomok a számítógépek háttértárolóin vagy esetleg perifériáin találhatók. Ha traszológiai értelemben nyomként nem is értelmezhető, az általános kriminalisztikai nyom fogalomkörébe mégis beilleszthető a digitális nyom. Ezen bizonyítékok megtalálásához, kimentéséhez megfelelő, magas szintű informatikai ismeretek és megfelelő eszközrendszer szükséges.

A napló és regisztrációs adatok a számítástechnikai rendszerek működése és kommunikációja során keletkeznek. Az úgynevezett napló adatok *(logok)* törvényi kötelezettség, gazdasági ésszerűség, vagy rendszerbiztonsággal kapcsolatos követelmények alapján jönnek létre, ilyen adatok például a különböző szerverek fel- és letöltését naplózó adatállományok, a levelező szerverek postafiókokhoz kapcsolódó ki- és bejövő leveleket, valamint a postafiók elérését regisztráló adatállományok, vagy az egyes hálózatbiztonsági programok, tűzfalak naplóadatai is.[346] A regisztrációs adatok egy-egy szolgáltatónál keletkeznek, amikor valaki igénybe veszi szoláltatásukat. Ezek lehetnek valós, ellenőrzött adatok, de lehetnek nem ellenőrzött adatok, amikor valaki regisztrálja magát egy szolgáltatás igénybevételénél, és az adatok hitelességét nem ellenőrzi senki.[347] A regisztrációs adatokból ismerhető meg, hogy a feltételezett elkövető milyen adatokat adott meg a regisztráció során, a napló adatokból pedig, – amelyek a belépésekre, fel- és sokszor

[341] PESZLEG T., A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük. Ügyészek Lapja 2010/2. pp. 23-32.
[342] Például az adathordozókon tárolt programok, gazdasági bűncselekményeknél a számítógépes könyvelés adatai, tiltott pornográf felvétellel való visszaélésnél képek, videó anyagok, okmányhamisításoknál az eredeti okmányok digitalizált változatai, de más bűncselekményeknél is a kapcsolattartásra utaló levelezés, vagy egyéb adat található a számítógépes adattárolókon.
[343] GARAMVÖLGYI V. & VISKI L. (ed.), *Kriminalisztika.* Belügyminisztérium Tanulmányi és Módszertani Osztálya, Budapest, 1961. p. 116.
[344] BÍRÓ Gy., *Kriminalisztika.* Debreceni Egyetem ÁJK. Lícium-ART Könyvkiadó Kft. Debrecen, 2007. p. 46.
[345] GARAMVÖLGYI & VISKI, 1961. p.116.
[346] PESZLEG, 2010. p. 30.
[347] PESZLEG, 2010. p. 30.

a letöltésekre is tartalmaznak adatokat, – kideríthető, hogy az internet mely számítógépéről léptek be arra az oldalra, töltöttek fel vagy le adatállományokat arról az oldalról.

2.2. A digitális bizonyítékok megszerzésének forrásai

A bizonyítékok beszerzésének törvényessége akkor állapítható meg, ha a nyomozó hatóság törvényben meghatározott módon, törvényben meghatározott körbe tartozó és kezelt, feldolgozott, a büntetőeljárásban bizonyítékként felhasználható elektronikus adatokat szerez be. Az előző cím alatt részletezett digitális bizonyítékok – ahogy már említettem – részben a bűncselekmény sértettjének vagy elkövetőjének számítógépén vagy a szolgáltatók birtokában van. Utóbbi forrás vonatkozásában meg kell vizsgálni azokat a jogszabályokat, amelyek bizonyos adatvédelmi megfontolások miatt a digitális bizonyítékoknak tekinthető, mégis személyes adatoknak minősülő adatok kezelésére engedélyt és lehetőséget biztosítanak.

A vonatkozó uniós jogforrás a hírközlési hálózatokban keletkezett adatok tárolásáról szóló 2006/24/EK európai parlamenti és tanácsi irányelve (adat-visszatartási irányelv), amely többek között az egységes, bűnüldözési célú adatmegőrzés sztenderdjeit határozza meg. Az irányelv alkalmazásában adatok a forgalmi és helymeghatározó adatok, valamint az előfizető vagy felhasználó azonosításához szükséges kapcsolódó adatok (pl.: telefonszám, az előfizető neve, címe, cellaazonosító).

Az irányelv rendelkezéseit a jogalkotó a hazai jogszabályok közül az elektronikus hírközlésről szóló 2003. évi C. törvényben (a továbbiakban Eht.) implementálta, amely a hírközlési szolgáltatóktól vár el bizonyos adatkezelési és szolgáltatási kötelezettséget szolgáltatásuk teljesítése vonatkozásában. Az Eht. értelmező rendelkezései szerint elektronikus hírközlési szolgáltatás: olyan, más részére általában ellenszolgáltatásért végzett szolgáltatás, amely teljesen vagy nagyrészt jeleknek elektronikus hírközlő hálózatokon történő átviteléből, és ahol ez értelmezhető, irányításából áll, de nem foglalja magában az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások felhasználásával továbbított tartalmat szolgáltató vagy ilyen tartalom felett szerkesztői ellenőrzést gyakorló szolgáltatásokat, valamint nem foglalja magában az információs társadalommal összefüggő, más jogszabályokban meghatározott szolgáltatásokat, amelyek nem elsősorban az elektronikus hírközlő hálózatokon történő jeltovábbításból állnak.[348] Míg az elektronikus hírközlési szolgáltató: az elektronikus hírközlő hálózat üzemeltetője, valamint elektronikus hírközlési szolgáltatást nyújtó természetes, illetőleg jogi személy vagy jogi személyiséggel nem rendelkező gazdasági társaság.[349] A törvény tehát azokra a szolgáltatókra ró kötelezettséget, akiknek az infrastruktúráján az internetes adatforgalom folyik.

A szolgáltatók bűnüldözési, nemzetbiztonsági és honvédelmi célú adatmegőrzési kötelezettsége az Eht. 159/A. §-án alapul, amely szerint az elektronikus hírközlő hálózat üzemeltetője, illetve az elektronikus hírközlési szolgáltatás szolgáltatója – az adatkérésre külön törvény szerint jogosult nyomozó hatóság, ügyészség, bíróság, valamint nemzetbiztonsági szolgálat törvényben meghatározott feladatai ellátásának biztosítása céljából, a kérelmükre történő adatszolgáltatás érdekében – megőrzi az elektronikus hírközlési szolgáltatás előfizető, illetve felhasználó általi igénybevételével kapcsolatos, az érintett elektronikus hírközlési szolgáltatás nyújtásával összefüggésben a szolgáltató által

[348] Eht. 188. § 13. pont
[349] Eht. 188. § 14. pont

előállított vagy kezelt meghatározott adatokat.[350] A szakaszban felsorolt adatokat a szolgáltató azok típusától függően az előfizetői szerződés megszűnését követő, azok keletkezését követő egy évig, a sikertelen hívások során előállított vagy kezelt adatokat azok keletkezését követő fél évig köteles megőrizni.

Ami a dolgozat tárgya szempontjából releváns e szabályozásban, az a megőrzésnek az adatkezelés célhozkötöttsége elvének való megfelelése, az adatok hitelessége és az adatok megszerzésének törvényessége. Az adatmegőrzés ellen érvelők szerint a kérdés az, hogy a „készletező", előre meghatározott cél nélküli adatgyűjtés, amelynek indoka csak utólagosan – az elkövető felelősségének bizonyításakor – igazolható, megfelel-e az alkotmányos követelményeknek.[351] Alkotmányossági szempontból tehát az vizsgálandó, hogy valamennyi polgár alapvető jogának a korlátozása mennyiben adhat alapot a kevesek feltételezett és még el nem követett jogsértéseinek esetleges felderíthetősége.[352]

Az információs önrendelkezési joggal szemben azonban szintén védelmet igénylő alapjogok követelnek védelmet. Egyrészt minden polgárt megilleti jogainak védelme, ennek egyik részelemeként a sérelmére elkövetett bűncselekmény esetén az elkövető kilétének felderítése és megbüntetése, sérelmének orvoslása. Másrészt a polgárok kollektív érdeke nyilvánul meg a stratégiai jelentőségű közművek, az államszervezet működésének, a nemzetbiztonság védelmében. Az egymásnak feszülő érdekek közötti egyensúly megtalálása a folyamatos technológiai fejlődés tudatában még talán megoldható volna, azonban a globális trendek, a 2001. szeptember 11. után megerősödött nemzetközi nyomás ismeretében a hazai alkotmányos probléma rendezéséhez fűződő érdeket jelentősen túlnövik az egyes nagyhatalmak hatékonyan érvényesített érdekei.

Másrészről a szolgáltatók nem kizárólag bűnüldözési, nemzetbiztonsági célból tárolnak kötelező érvénnyel adatokat, hanem más megfontolások miatt is, például üzleti vagy számviteli kötelezettségek teljesítése miatt, amely adatkörök átfedést mutatnak a bűnüldözési célból őrizendő adatokkal.[353] A bűnüldözési célú, az Eht. 159/A. §-a alapján előírt egy éves adatmegőrzési kötelezettség tehát úgy értelmezendő, hogy a szakaszban felsorolt adatokat a szolgáltatóknak mindenképpen meg kell őrizniük legalább 1 illetőleg fél év időtartamig. Következésképpen a szolgáltatóknak a Be. 71. §-a alapján az adatok keletkezését követő 1 év után küldött megkeresés a nem kifejezetten bűnüldözési de egyéb törvényes célból kezelt adatok szolgáltatása érdekében törvényes, a szolgáltatók részéről a megkeresés nem teljesítésének okául megjelölt 1 éves határidő túllépése tehát nem

[350] Ezek az adatok a teljesség igénye nélkül a következők lehetnek az Eht. 159/A. § (2) bekezdése alapján: az előfizetői állomás száma vagy egyéb azonosítója, az előfizető címe és az állomás típusa, a hívás vagy egyéb szolgáltatás típusa, iránya, kezdő időpontja és a lefolytatott beszélgetés időtartama, illetőleg a továbbított adat terjedelme, mobil rádiótelefon szolgáltatásnál a szolgáltatást nyújtó hálózat és cella, valamint a szolgáltatás igénybevételekor használt készülék egyedi azonosítója (IMEI), IP hálózatok esetén az alkalmazott azonosítók, a hívás vagy egyéb szolgáltatás dátuma.

[351] A 15/1991. (IV. 13.) AB határozat szerint a célhoz kötöttség elvéből következik, hogy a meghatározott cél nélküli, készletre, előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és tárolás alkotmányellenes. A felmerülő kérdés pontosabban az, hogy a jövőbeni, bűnüldözési, nemzetbiztonsági célú adatgyűjtás alkotmányos-e vagy sem.

[352] HÜTTL T., JOVANOVICS E., SZABÓ M. D. & VISSY B., Alkotmánybíróságok az adatmegőrzésről – Adalékok az Alkotmánybíróság számára az adatmegőrzési irányelvet átültető magyar szabályok alkotmányossági felülvizsgálatáról szóló eljáráshoz. *Infokommunikáció és Jog*, 2010. április (37. szám) p. 73.

[353] Az Eht. 157. § (5) bekezdése külön törvények által előírt adatkezelés lehetőségét is felveti. Például a számvitelről szóló 2000. évi C. törvény 169. § (2) bekezdése alapján a könyvviteli elszámolást közvetlenül és közvetetten alátámasztó számviteli bizonylatot (ideértve a főkönyvi számlákat, az analitikus, illetve részletező nyilvántartásokat is), legalább 8 évig kell olvasható formában, a könyvelési feljegyzések hivatkozása alapján visszakereshető módon megőrizni.

elfogadható, amennyiben az adtok elkülönülten de rendelkezésre állnak.[354] Az Eht. 157. § (10) bekezdése a bűnüldöző szervek ezen adatkérési lehetőségét külön is nevesíti.

Az adatok hitelességére vonatkozóan a 2006/24/EK irányelv 6. és 7. cikke alapján az Eht 159/A. § (4) bekezdése úgy rendelkezik, hogy a forgalmi adatok hitelességéért, teljeskörűségéért és időszerűségéért a szolgáltató felel, azonban a gyakorlatban a tényleges kontrol nem ismert, nem tapasztalt. A jogalkalmazás során viszont előfordulnak olyan esetek, hogy a különböző szolgáltatókhoz rendelt telefonszolgáltatások egymás irányában történő hívásainak adatai nem egyeznek meg a két szolgáltatónál, vagy egy megtörtént hívásnak nincs nyoma.[355] A szolgáltatóktól beszerzett adatok tehát önmagukban nem mindenekfelett állók, természetesen további megerősítésekre szorulnak.

A 2001. évi CVIII. törvény (továbbiakban E-ker. törvény) az elektronikus kereskedelmi szolgáltatást és az információs társadalommal összefüggő szolgáltatást nyújtókra ró kötelezettségeket. Az E-ker. törvény nem határoz meg egyértelmű szabályokat a hatálya alá tartozó szolgáltatókra. Ezen törvény hatálya alá az „elektronikus úton, távollevők részére, rendszerint ellenszolgáltatás fejében nyújtott szolgáltatás, amelyhez a szolgáltatás igénybe vevője egyedileg fér hozzá", vagyis az információs társadalommal összefüggő szolgáltatások tartoznak, és azok a természetes-, vagy jogi személyek, illetve jogi személyiség nélküli szervezetek, akik ilyen szolgáltatást nyújtanak. A szolgáltatók a szolgáltatás teljesítése, a szerződés megkötése, módosítása, számlázás és az azzal kapcsolatos követelések érvényesítése céljából kezelheti a szolgáltatást igénybe vevő személyes adatait, de csak annyit, amennyi elégséges és szükséges az azonosításához. Kezelheti továbbá azokat a személyes adatokat is, melyek a szolgáltatás nyújtásához technikailag elengedhetetlenül szükségesek. A technológia megválasztásánál úgy kell eljárnia, hogy azonos feltételek esetén azt kell választania, mely kevesebb személyes adat kezelésével jár. Az így kezelt adatokat is csak addig őrizheti meg, míg a szerződés meg nem szűnt, illetve a számlázás meg nem történt. A törvény részletesen foglalkozik a szolgáltató és a közvetítő szolgáltató felelősségével, de nem ír elő adatmegőrzési és adatszolgáltatási kötelezettséget az Eht-ban megfogalmazottakhoz hasonlóan.

3. A BIZONYÍTÉKOK BESZERZÉSÉNEK LEHETŐSÉGEI, MÓDSZEREI

3.1. Megkeresés

A Be. 71. § (1) bekezdése alapján a megkeresés során a bíróság, az ügyész és a nyomozó hatóság állami és helyi önkormányzati szervet, hatóságot, köztestületet, gazdálkodó szervezetet, alapítványt, közalapítványt és társadalmi szervezetet kereshet meg tájékoztatás adása, adatok közlése, átadása, illetőleg iratok rendelkezésre bocsátása végett. A megkeresések során a fenti szolgáltatóktól a szervereiken megtalálható honlapok, tárhelyek tartalmát kéri meg a nyomozó hatóság, valamint az ezekhez az oldalakhoz és tárhelyekhez tartozó regisztrációs adatokat és az oldal elérését dokumentáló napló adatokat, arra vonatkozóan, hogy egy bizonyos IP cím egy bizonyos időben kinek volt kiosztva, azaz a

[354] Az Eht. 157. § (6) bekezdése alapján az e törvény, illetve más törvények által lehetővé tett, illetve előírt különféle célú adatkezeléseket az elektronikus hírközlési szolgáltatónak el kell különítenie egymástól. Az elkülönítés történhet *a)* kezelési cél szerint fizikailag elkülönített adatkezelési rendszerekben, amelyekben egymástól függetlenül vannak eltárolva az eltérő kezelési céllal kezelhető adatok; *b)* logikailag elkülönített adatkezelési rendszerben, amelyben a különféle céllal kezelhető adatok közös rendszerben vannak eltárolva, azonban az adatokhoz való hozzáférések az adatkezelés célja szerint elkülönülnek egymástól.

[355] Például a Budapesti IV. és XV. Kerületi Ügyészség B.4241/2008. számú ügye. Az adatok hiányának oka lehet pl. az értekezésben meg nem nevezett mobilszolgáltató technológiaváltása miatt átmeneti üzemzavar.

szervert az adott időben mely számítógép használta, mely előfizetői névvel, honnan és milyen összeköttetésről érték el az internetet. A megkeresés útján kapott adatokat a büntetőeljárás során már okiratként használja fel a hatóság. Ennek kriminalisztikai furcsaságát az adja, hogy a bizonyítékot magát (az adatot), annak fizikai valóját, az adatmegőrzésre vonatkozó szabályok szigorú rendelkezései miatt az adatkezelő keletkezését követő legkésőbb egy év elteltével törli, megsemmisíti.

A nyomozás tervezésekor figyelemmel kell lenni arra, hogy a szolgáltatókkal való kapcsolattartás lassítja a nyomozást, a bűncselekmény késedelmes észlelése, a megkeresés késedelmes megküldése esetén a kívánt adatok elveszhetnek. Célszerű éppen ezért a szakértelmet nem igénylő kérdésekben a nyomozó hatóság tagjának magának intézkednie, így például egy-egy IP-cím tartományt a bárki számára hozzáférhető internetes adatbázisok segítségével meg lehet állapítani, ezután célirányosan, a megfelelő szolgáltatóhoz küldeni a megkereséseket.[356] Arra is figyelni kell, hogy a megkereséseket időben kell alkalmazni, hiszen az internet tartalomszolgáltatói nem tekinthetők hírközlési szolgáltatóknak, így az egyéves adatmegőrzési kötelezettség sem terjed ki rájuk.[357] Egy további, a gyakorlatban már több esetben előfordult probléma, hogy a szolgáltatóktól megkért adatok nem voltak hitelesek.[358] A megkeresésre adott válasz hitelességét az is gyengítheti, hogy egyes programokkal az is elérhető, hogy a szolgáltató IP-állományának egy részét vagy teljes mennyiségét használja az elkövető.

A 2006. évi LI. törvény eltörölte a Be. 178/A §-a szerint ügyészi jóváhagyás szükségességét, amikor a nyomozó hatóság a gyanúsítottról (feljelentettről, illetőleg az elkövetéssel gyanúsítható személyről) a tényállás felderítése érdekében adatok szolgáltatását igényelheti a hírközlési szolgáltatást nyújtó szervezettől. Mindezzel jelentős tehertől nem szabadult meg az ügyészség, ugyanakkor gyorsíthatta a nyomozás folyamatát. Felmerül a kérdés azonban, hogy valóban biztosítható-e maradéktalanul a magánszemélyek információs önrendelkezési jogát érintő nyomozás során a törvényességi felügyelet, avagy a nyomozó hatóság szabad kezet kap a szolgáltatóktól történő teljes körű adatgyűjtésre azzal az egyetlen, a Be. 178/A. § (8) bekezdésébe foglalt garanciával, hogy ügyészi vádemelés hiányában az így beszerzett adatokat törölni kell. Úgy gondolom, hogy az elkövető gyanúsítottkénti kihallgatása után, illetve akkor, ha gyanúsítotti kihallgatására még nem került sor ugyan, de a megfelelő mennyiségű adat már rendelkezésre áll, akkor az így konkréttá vált személy adatainak beszerzéséhez már nincs szükség ügyészi engedélyre. Ennek hiányában azonban az ügyész általános jogvédelmi feladatára tekintettel minden esetben vizsgálnia kell, hogy a nyomozó hatóság által beszerzett adatokra a nyomozás érdekében valóban szükség van-e, mert amennyiben nincs, azok haladéktalan megsemmisítésére kell utasítania a nyomozó hatóságot.

A megkeresésben fel kell tüntetni annak jogalapját, azonban mind a mai napig előfordul, hogy egyes kisebb rendőrőrsön helytelenül, korábban az ORFK és a távközlési szolgáltatók között kötött megállapodásra hivatkozva kérik a fent felsorolt adatok közlését és nem a Be. vonatkozó rendelkezéseire.

[356] Ilyen például a centralpos.net szolgáltatása.

[357] A népszerű iwiw-közösségi oldal adatvédelmi szabályzata alapján csak 6 napig tárol a nyomozás szempontjából lényeges adatokat, amelyek bizonyító erejük szempontjából erősebbek lehetnek, a határidő eltelte után már csak az üzemeltető hírközlési szolgáltatójához lehet fordulni.

[358] Két különböző mobiltelefon szolgáltatóhoz tartozó készülék egymás közötti kommunikációjára vonatkozóan feltett kérdésre a két különböző szolgáltató nem adott egymással megegyező híváslistát.

3.2. Lefoglalás

A lefoglalás az egyik legtöbbet vitatott kényszerintézkedés a nyomozások során. A Be. 151. §-a alapján a lefoglalás a dolog birtokának elvonása a birtokos rendelkezése alól. A bíróság, az ügyész, illetőleg a nyomozó hatóság elrendeli annak a dolognak, illetőleg számítástechnikai rendszernek vagy ilyen rendszer útján rögzített adatokat tartalmazó adathordozónak a lefoglalását, amely a) bizonyítási eszköz, b) a törvény értelmében elkobozható, vagy amelyre vagyonelkobzás rendelhető el.

Bizonyítási eszköz lefoglalásakor az adott bűncselekményekre utaló nyomok és a bizonyítás sikerességének biztosítása miatt van szükség. Lefoglaláskor tehát azokat az adathordozókat kell lefoglalni, amelyek a digitális bizonyítékokat tartalmazhatják, és amelyek a későbbi szakértői vizsgálatok tárgyai lehetnek.

A lefoglalás által okozható vagyoni és nem vagyoni károk miatt különös figyelmet kell tulajdonítani ezen kényszerintézkedés elrendelésekor és foganatosítása során. A lefoglalt számítástechnikai eszközön – legyen az egy szolgáltató szervere vagy egy magánszemély személyi számítógépe, vagy annak adathordozója – sok esetben olyan tartalmak is találhatók, vagy olyan szolgáltatások működnek, amelyek a bűncselekmény elkövetőitől független személyek érdekkörébe tartoznak, a lefoglalással azonban ezen személyek gazdasági vagy privát érdekei sérülnek.

Bár az informatikai bűncselekmények elkövetésének bizonyítása során a lefoglalással szerezhető bizonyítékok mellett gyakran más bizonyíték nem áll rendelkezésre, figyelemmel kell lenni a lefoglalással érintett személyek érdekeire is. Így teljes szerver lefoglalásához nem elegendő az a tény, hogy a bűncselekmény elkövetésére utaló adatokat tartalmaz, hanem a szerver üzemeltetője, tulajdonosa és a bűncselekmény között kell valamilyen kapcsolatot találni.[359] Az említett érdekvédelmet már számos technikai eszköz biztosítja amellett, hogy alkalmazásuk megalapozhatja a későbbi szakértői vizsgálatok hiteles eredményét is azáltal, hogy a lefoglalással megszerezni kívánt adat hordozóját nem vonjuk el birtokosától, hanem a bizonyíték forrásával mindenben megegyező, változatlan, hiteles másolatot hoz létre.[360] Amennyiben mégis lefoglalásra kerül sor, abban az esetben is csak a szükséges mértékben foganatosítható, értem ezalatt azt, hogy sok esetben – kivéve, ha elkobzásra is sor kerülhet – nem indokolt a teljes konfiguráció lefoglalása, hanem elegendő a winchesterre vagy más adathordozóra szorítkozni.

Egyetértve Peszleg Tibor észrevételével nem szerencsés a 11/2003. (V. 8.) IM-BM-PM együttes rendelet 67. §-nak meghatározása, mely szerint az elektronikus úton rögzített adatot a hatóság adathordozóra történő rögzítés (átmásolás) útján foglalja le. Ez a megfogalmazás arra enged következtetni, hogy a lefoglalást nem eredetben, nem a konkrét adathordozó (dolog) birtokostól történő elvonásával kell foganatosítani, hanem másolással, vagy megkereséssel. A jogszabályhelyek egymásnak ellentmondó fogalmi nyelvezetére is

[359] PARTI K., Gondolatok a szerver-lefoglalásokról. *Infokommunikációs és Jog* 2004/3. p. 98.

[360] Az egyik legyakrabban alkamazott technikával az eredeti adathordozón változás végrehajtása nélkül készíthető másolat, amin a rögzített digitális nyomok a továbbiakban vizgálhatók. Az eljárással egyben hitelesíthetők az így biztosított digitális nyomok, mert egy matematikai műveleten alapuló úgynevezett „hash" kulcsot (például az MD5 rendszerrel) generálnak az eredeti adathordozóról, mely valamilyen változtatás esetén már más eredményt ad. A „hash" kulcs olyan karaktersorozat, amelyet csak a számítógépes program értelmez, és amit akár kinyomtatva is tárolhat a nyomozó hatóság az ügyiratban, illetve megőrizheti a szakértő, valamint az a személy, akitől a digitális nyomokat rögzítették. Az eljárással nem szükséges az eredeti adathordozó lefoglalása.

visszavezethető a nyomozó hatóságok lefoglalást előnyben részesítő hozzáállása. A Be. 158/A § (8) bekezdése az adat lefoglalását említi, a 11/2003. (V. 8.) IM-BM-PM együttes rendelet 67.§-a csak másodlagosan említi meg a számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés jogintézményét. A lefoglalás mellett szól az is, hogy a bizonyíték kétséget kizáróan csak lefoglalással szerezhető be, egyes esetekben gyorsabb megoldás, és az információ kevésbé van kitéve változásoknak.

Nem szabad azonban azt sem elfelejteni, hogy a lefoglalás célja lehet a bűncselekmény elkövetéséhez eszközül használt dolgok későbbi elkobzásának biztosítása. Egy számítástechnikai eszköz, berendezés valamennyi tartozéka együttesen eszköze lehet az elkövetésnek (például egy interneten elkövetett bűncselekmény eseten egy laptop), ebben az esetben az elkobzás a Btk. 77. § (1) bekezdés a) pontja alapján nem mellőzhető, ekként a lefoglalás sem tehető mérlegelés tárgyává.

3.3. Számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés

A Be. 158/A.§ (1) bekezdése alapján a megőrzésre kötelezés a bűncselekmény felderítése és a bizonyítás érdekében a számítástechnikai rendszer útján rögzített adat birtokosának, feldolgozójának, illetőleg kezelőjének a számítástechnikai rendszer útján rögzített meghatározott adat feletti rendelkezési jogának ideiglenes korlátozása. Ez a jogintézmény ideiglenesen kívánja biztosítani a nyomozó hatóságok részére a számítástechnikai rendszer útján rögzített adatok átvizsgálásának lehetőségét, amennyiben az eljárás során ezek közül az adatok közül szükség lenne valamely adatra a bizonyításhoz vagy a felderítéshez, akkor azt lefoglalással kell megszerezni. Ez az ideiglenes intézkedés csak azt biztosítja a nyomozó hatóságnak, hogy ezeket az adatokat vizsgálni tudja. Ebből következik, hogy ezt a jogintézményt akkor alkalmazhatja a nyomozó hatóság, ha nagyobb terjedelmű adathalmazt kell átvizsgálnia (például több terra-bájtnyi adatot tartalmazó szervereket), és nem lehet meghatározni, hogy pontosan mely adatokra van szükség, így az egész adathalmazra vonatkozóan se megkereséssel, se lefoglalással nem tud élni. Az adatok sérthetetlenségét az elrendelő szerv olyan módon is biztosíthatja, hogy az adatot fokozott biztonságú elektronikus aláírással láthatja el.

Ezzel az intézkedéssel biztosítható, hogy akár az ország különböző területein bűncselekmény felderítése során szükséges különböző szerverek adatai a nyomozó hatóság rendelkezésére álljanak. Az adatokat összevetve, „összefésülve” és kigyűjtve a releváns adatokat, csak a szükséges adatokat kelljen lefoglalni a bizonyítás érdekében. A kényszerintézkedés másik lehetséges alkalmazása, amikor egy olyan számítógépen tárolt adatokat megőrzésére van szükség, ami nem érintett a bűncselekményben, azonban az adathordozóján tárolt adatok a nyomozáshoz szükségesek. A számítógép adathordozójának lefoglalása túlzó és felesleges terhet róna a tulajdonosra, hiteles másolata viszont szükségtelen költséget keletkeztetne. A megőrzésre kötelezés ebben az esetben helyénvaló megoldásnak tűnik, mivel a lefoglalásnál enyhébb intézkedés, és a vétlen birtokosnak is kisebb joghátrányt okoz, ugyanakkor a kényszerintézkedés célja, hogy a számítástechnikai eszközön lévő adatokat a nyomozó hatóság átvizsgálhassa, biztosított.

A kényszerintézkedés hatékony, és megfelelő időben történő alkalmazása megoldást kínálhat az elektronikus hírközlési szolgáltatóknak nem minősülő – ekként az adatmegőrzési kötelezettség hatálya alá nem tartozó – szolgáltatóknál rövid ideig tárolt

forgalmi adatok vizsgálatára.[361] A gyors reagálással természetesen a helyes kérdéseket tartalmazó, adaszolgáltatásra irányuló megkeresés jóllehet azonnal megfelelő választ biztosít, viszont a gyakorlatban mindez gyakran nem tapasztalható.

A kényszerintézkedést korlátozó garanciális szabály, hogy az adatok feletti korlátozás csak három hónapig tarthat. Ennek indoka az, hogy az intézkedés a megőrzésre kötelezettre akár komoly anyagi terheket is róhat, üzemszerű működését akadályozhatja az a körülmény, hogy gondoskodnia kell az adatok tárolásáról, és hozzáférhetetlené tevéséről mások számára.

A kényszerintézkedésnek természetesen kritikája is ismert, mivel a jogszabály csak később került be a büntetőeljárásról szóló törvénybe, nem egészen illeszkedik annak rendszerébe. A Be. nem határozza meg az adat fogalmát, és mivel lényegében egy új, előzmények nélküli jogintézményről van szó, alkalmazásának gyakorlata még nem alakult ki.

3.4. A szakértői bizonyítás

A Be. 99. § (1) bekezdése alapján, ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges, szakértőt kell alkalmazni. A Be. 105. § (1) bekezdése alapján a szakértő a vizsgálatot a tudomány állásának és a korszerű szakmai ismereteknek megfelelő eszközök, eljárások és módszerek felhasználásával köteles elvégezni. Ez alapján a büntetőeljárási törvény kötelező erővel fogalmazza meg azt az igényt, hogy a szakértő legjobb tudomása szerint, a legfejlettebb technikai színvonalon lássa el szakmai feladatát.

A számítástechnikai, vagy számítógéppel kapcsolatos bűncselekmények nyomozása során a technológia erőteljes jelenléte miatt gyakori a szakértő alkalmazása, ami azonban több visszásságot hordoz magában. Jellemző, hogy informatikai kérdésekben a kirendelő hatóság az informatikai szakmai kompetencián túlmutató kérdésekre is választ vár.[362] Illési Zsolt szerint további probléma, hogy nincs olyan képzés, ami például az informatikai igazságügyi szakértés alapismereteivel függ össze, az olyan ismereteket egyetlen magyar felsőoktatási intézmény nem ad, amelyek az igazságügyi szakértés speciális követelményeivel foglalkoznának, nem ismertetik a rendelkezésre álló technológiákat, hardver és szoftver eszközöket, módszereket.[363] A Magyar Szakértői Kamara Informatikai Szakértői albizottsága pedig nem egységesíti a szakértők képzését.[364] Egyes szerzők szerint a technológiai képzés mellett nem elhanyagolható szempontot jelent az informatikai szakértők etikai felkészültsége is, hiszen előfordulhatnak olyan esetek, amikor dönteniük kell, milyen adatokat és milyen mélységben vizsgálnak.[365]

---

[361] Például a közösségi oldalak üzemeltetői nem elektronikus hírközlési szolgáltatók, ezért rájuk nem vonatkozik az adatmegőrzés kötelezettsége, jellemzően rövid ideig (az iwiw esetében 6 napig) tárolják a bűncselekmény elkövetőjének felderítésére alkalmas forgalmi adatokat (milyen IP-címről léptek be az elkövetés napján a felhasználói fiókba, profiloldalra).

[362] ILLÉSI Zs., Az igazságügyi informatikai szakértés modellezése. *Hadmérnök* IV. évfolyam 4. szám (2010. december) p. 123.

[363] ILLÉSI, 2010. p. 126.

[364] PARTI K. & VIRÁG Gy., Beszámoló a Számítógépes bűnözéssel foglalkozó kormányközi munkacsoport (Intergovernmental Expert Group on Cybercrime) üléséről, (Bécs, 2011. január 1721.) és az ennek kapcsán felmerült kérdésekről. p. 8.

[365] IRONS, A. & KONSTADOPOULOU, A., Professionalism in digital forensics. *Digital Evidence and electronic signature law review*. 2007. p. 46.

Az informatikai szakértők eljárásának egy további, nem csak hazai részproblémája, hogy a számítógéppel érintett bűncselekmények felderítése során a szakértők nem sztenderdizált eljárásokkal folytatják a vizsgálatot.[366] Nem egységes szabályzat alapján végzik az elektronikus adatokat tároló eszközök vizsgálatát, felszereltségük nem egyforma, ekként az egyes szakértők munkája eltérő minőségű lehet, azaz a bizonyítékok hitelessége esetenként megkérdőjelezhető. E körben kiemelendő, hogy az informatikai szakértők eljárására vonatkozóan – szemben más igazságügyi szakértői ágazatokkal – nem született ez idáig olyan módszertani levél, amely egységesítené, szabványosítaná a szakértői vizsgálatot, biztosítva ezáltal az eredmények megbízhatóságát. A módszertani levelek többek között lehetővé tennék a hatóságok laikus tagjai számára, hogy egy szakmai katalógusra épülve szakszerű kérdéseket tegyenek fel illetve, segítenének abban is, hogy a laikusok értelmezni tudják a kérdéseikre adott szakmai válaszokat.[367]

Egy másik, joggal feltehető kérdés, hogy miért kerül olyan gyakran sor informatikai szakértők kirendelésére. A jogalkalmazók elektronikus bizonyítékokhoz való viszonya még bátorításra szorul, a technikai eszközök és a szakértelem hiánya miatt döntéshozók még idegenkednek a szakértőket kiváltó technikai eszközök beszerzésétől, vagy a bizonyítékszerzés bűnügyi technikusok igénybevételével történő biztosításától.

A büntető eljárás során a szakértők kirendelésére jellemzően rövid szakaszokban kerül sor, így például számítástechnikai eszközök lefoglalásakor, vagy a már lefoglalt bizonyítékok vizsgálatakor. Azonban egyes bonyolultabb esetekben már a nyomozási terv kidolgozásához is szükség lehet informatikai szakértelemmel rendelkező személy közreműködésére, aki a nyomozás kezdetétől fogva segítséget nyújt a bűncselekmény hatékony felderítéséhez.[368]

Természetesen nem várható el egy bűnügyi elemzőtől, hogy az informatika valamennyi területén járatos legyen, és kiemelkedő tudással rendelkezzen az informatikai biztonság és valamennyi típusú számítástechnikai rendszer működését illetően, azonban megfelelő állami intézet alkalmazottaiként felállítható lenne egy quasi szaktanácsadókból álló, informatikai bűnügyi technikus csoport. A már megszerzett bizonyítékok tárolása, a bűnjelkezelés is a lehető legnagyobb fokú biztonsággal lenne biztosítva egy kifejezetten számítástechnikai bűnjelek elemzésére létrehozott laboratóriumban, intézetben.

4. A BIZONYÍTÁS HATÉKONYSÁGÁNAK JAVÍTÁSA

A hatékony bűnüldözés alapelemei a szakképzett személyi állomány és a megfelelő eszközpark. Nincs ez másként a számítástechnikával érintett bűncselekmények nyomozása esetén sem. Mivel a korábbi fejezetekben írtak alapján jelentősen felértékelődött a speciális tudás birtoklásának értéke, valamint átalakult a különleges ismeretek és szakkérdések megítélése, egyértelmű, hogy az információs társadalom bűncselekményeit hatékonyan csak a megfelelő tudással rendelkező személyek képesek felderíteni és bizonyítani. Mindez első pillantásra pusztán krimináltechnikai és szervezéstani problémának tűnhet. Addig azonban, amíg a büntetőeljárásról szóló törvényben a különleges szakkérdéseknek tekintett valamennyi informatikai vonatkozású ténymegállapítás problémája szakértő kirendelésével rendeződik, addig a korábban felmerült, szakértőket érintő anomáliák sem fognak eltűnni.

[366] JONES, N., Training and accreditation – who are the experts? *Digital Investigation,* 2004. Vol. 1. No. 3. pp. 189-194.
[367] ILLÉSI, 2010. p. 124.
[368] LUEHR, P. H., Real evidence, virtual crimes – The role of computer forensic experts. *Criminal Justice 2005*. p. 18.

El kell fogadnunk, hogy az információs társadalomban felmerült információ- és jogszabálytömeg kezelése nem mindig várható el a jogalkalmazótól. Az viszont sehol sincs megtiltva, hogy a tudást ne lehetne kollektívan, az ismereteket külön-külön birtokolva hasznosítani. Azaz a felderítés során a számítástechnikával, szerzői joggal érintett bűncselekmények nyomozását olyan csoportoknak kell folytatniuk, amelyek a különböző szakismeretekkel rendelkező személyekből állnak. A megfelelő szakembereket természetesen ki kell képezni, és megfelelő fejlesztésű eszközöket kell biztosítani számukra.

A szakértői bizonyítás és a bűnügyi költségek túlburjánzásának megakadályozása érdekében az informatikai szakképzettséggel rendelkező bűnügyi technikusok *(computer forensic experts)* alkalmazása mellett egy lehetséges másik megoldás az állam által fenntartott igazságügyi laboratóriumok, szakértői intézetek rendszerének kialakítása. Példaként említhető az *USA PATRIOT Act* 816. szakasza *(Development and Support of Cybersecurity Forensic Capabilities)*, amely előírja az Egyesült Államokban regionális informatikai laborok felállítását, amiknek a vizsgálatok végrehajtása mellet az is célja, hogy az állami és szövetségi számítástechnikai bűnüldözés személyi állományát képezze, oktassa.[369] Figyelemreméltó, hogy a hatékony bűnüldözés koncepciója nem merül ki kizárólag az eszköz-rendszer biztosításában, hanem a személyi állomány differenciált kiképzését is célul tűzte ki, a tréning – akár a titkosszolgálatok bevonásával – egyes speciális bűncselekmény-típusonként történik.[370]

Például a zaklatások (cyberstalking) felderítésénél az informatikai tudás mellett a bűncselekménytípusra jellemző elkövetői és áldozati viselkedésminták ismerete is szükséges lehet. A nyomozás során a tanúk kihallgatása mellett olyan adatok gyűjtése is szükséges, amelyek az elkövető indítékára, az áldozatával való kapcsolatára utalhatnak, ennek során a tanúk, sértette kioktatása is fontos a későbbi, akár digitális bizonyítékok beszerzése miatt: azaz ne dobják el a zaklatótól kapott tárgyakat, leveleket, ne töröljék az smst.[371] A zaklatások időtartama – amíg az áldozatok feljelentéssel élnek, vagy segítséget kérnek – változó, átlagosan 3-4 hónap, a legtöbben addig várnak, amíg már nem tudtak megbirkózni a problémával, ezért a digitális bizonyítékok beszerzésére rendelkezésre álló időtényezőt is figyelembe kell venni.[372]

5. A SZERZŐI JOGI BŰNCSELEKMÉNYEK BIZONYÍTÁSÁNAK ANOMÁLIÁI

5.1. Az információs táradalom, a különleges tudás és a szakértők kérdése

A technológia fejlődése jelentősen növelte a társadalom reakciójának gyorsaságát az új életviszonyokkal szemben, mivel az információk mind nagyobb arányú áramlása fokozatosan csökkentette a napra kész tudás elsajátításának tartamát, a folyamatos tanulás alapvető követelménnyé vált.

A vagyoni értékkel bíró információ termelése és innovatív felhasználása tehát a gazdasági élet egyik új erőforrása. Ugyanakkor az információtömeg megjelenésével párhuzamosan megnövekedett az azt kezelni képes tudás birtoklásának értéke is. Ezért az információs

[369] PODGOR, E. S., Computer Crimes and the USA PATRIOT Act. *Criminal Justice*, 2002. Summer. p. 62.
[370] PODGOR, 2002. p. 62.
[371] PETHERICK, W., Stalking. In. Turvey, B. E. (ed.), *Criminal Profiling – an introduction to behavioral evidence analysis*. Elsenier Inc. 84. Theobald's Road, London 2008. p. 454.
[372] PETHERICK, 2008. p. 470.

társadalmat szokás „tudásalapú társadalomnak” is nevezni, amelyben a változások legfőbb alapját a társadalom tudásában bekövetkező fejlődésben láthatjuk.[373]

Mindez a büntetőjogi jogalkalmazásra levetítve a következőket jelenti. Az élet és jogviszonyok bonyolultabbá, összetettebbé válásával a jogalkalmazók számára elkerülhetetlen a bűncselekményenkénti specializálódás, másrészt átértékelődik a különleges szakértelem, és a hatóságok jogismeretének jelentése. A digitális környezetben megjelenő, szerzői jogi oltalom alá eső művekre elkövetett jogsértések büntetőjogi vonatkozásai többszörösen interdiszciplináris területnek mondhatók.[374] A dolgozat első részében az informatikai vonatkozású tények szakértői megállapításának és értékelésének egyes kérdéseivel, második felében a jogkérdések és a szakvélemény kapcsolatával foglalkozom. Utóbbi vonatkozásában ismét két, klasszikus részproblémát kell újraértelmezve megvizsgálni, mégpedig elsőként megengedhető-e a szakértőnek, hogy jogkérdésben nyilatkozzék, a második kérdés pedig, hogy megengedhető-e a jogi szakértő alkalmazása.[375]

5.1.1. Problémafelvetés

A digitális környezetben elkövetett szerzői jogi jogsértések elbírálása során a nyomozások nagy részében szakértő, mégpedig a vizsgálandó számítástechnikai adathordozók jellege okán informatikai szakértő kirendelésére kerül sor. Egy, a Hamisítás Elleni Nemzeti Testület megbízása alapján készült, a szellemitulajdon-jogokat sértő bűncselekmények nyomozására vonatkozó kutatás eredményei alapján a nyomozások mintegy 90%-ban történt szakértő kirendelése, aki ebből, a Btk. 329/A. §-a miatt folyamatban lévő büntetőeljárások 69 %-ban informatikai szakértő volt.[376]

A szakértő bevonására a legtöbb esetben a következő kérdések megválaszolása miatt kerül sor: a lefoglalt adathordozón található-e szerzői jogot sértő tartalom, a lefoglalt adathordozón milyen szerzői jogi védelem alatt álló művek, műpéldányok találhatok, azoknak ki a jogosultja, és milyen vagyoni értéket képviselnek?

Mi a felsorolt kérdések fő problémája? Elsőként az a körülmény, hogy az informatikai szakértő fogalma önmagában nehezen értelmezhető, az informatika széleskörű alkalmazhatósága miatt az informatikán belül is többféle specializálódás létezik, ekként számos informatikai szakterület és arra épülő szakértői kompetencia között kell különbséget tenni.[377] Másrészt az elektronikus adathordozón található szerzői jogi tartalmak jogsértő voltának megállapítása jogkérdés, nem informatikai szakértelmet, sokkal inkább alapos jogszabályi ismereteket igényel. A szakértő feladata kizárólag az lehet, hogy olyan utaló bizonyítékokat keressen, amik a szerzői jogsértést valószínűsítik. Így például a zenei- és filmalkotások többszörözésére vonatkozóan szakértői kérdés lehet az, hogy a számítógép adathordozóján található-e, vagy korábban található volt-e olyan program, vagy annak korábbi létére utaló adat, amelynek működése eleve a szerzői jogi

[373] FARKAS J., Úton az ipari társadalomból az információalapú társadalom felé. In: Balogh G. (ed.), *Az információs társadalom dimenziói*. Gondolat/Infonia, Budapest, 2006. p. 97.
[374] Például a szoftveresen módosított műholdvevő beltéri egységek forgalmazásának minősítése médiajogi, szerzői jogi, informatikai, polgári jogi és büntetőjogi ismereteket igényel.
[375] ERDEI Á., *Tény és jog a szakvéleményben.* Közgazdasági és Jogi Könyvkiadó, Budapest, 1987. p. 37.
[376] KÁRMÁN G., NAGY L. T., SZABÓ I. & WINDT Sz., A szellemitulajdon-jogokat sértő bűncselekmények kutatása. *Kriminológiai tanulmányok*, 2011. 48. szám. p. 58.
[377] Ilyen szakterületek lehetnek például: informatikai biztonság, szoftverfejlesztés, adatbázisok tervezése, digitális műsorterjesztés, és az azzal összefüggő elektronikus hírközlés, stb.

szabályok megsértésével történik. Itt például elsősorban a torrent-alapú[378] vagy a DC++[379] elvein működő fájlcserélő, fájlmegosztó kliensprogramok telepítésére kell gondolni, amelyek alkalmazása, ha nem is szükségszerűen, de jellemzően szerzői jogi tartalmak megszerzésére és megosztására irányul, működésük viszont már szükségszerűen – a DC++ esetében a felhasználási feltételek teljesítése miatt – a szerzői jogok sérelmével jár. Szintén szakértői kérdés lehet egy számítógépes programalkotás jogtisztaságára vagy jogsértő voltára utaló felhasználói kód, vagy programtörés keresése és rögzítése. Annak kiderítése, hogy a szerzői művek kiskereskedelmi ára mennyi, kik a sértettek, szintén nem tekinthető informatikai szakkérdésnek. Az eljáró hatóság sok esetben ugyanolyan, nem szakértői módszerekkel meg tudná a szükséges választ szerezni az adott kérdésre[380]

Miért is jelentenek a fent sorolt észrevételek jogi szempontból problémát? A szakvélemény elkészítésének, a szakértő kirendelésének a büntetőeljárásról szóló 1998. évi XIX. törvény rendelkezései alapján kell történnie, azaz a bizonyítási eljárásnak törvényesnek kell lennie. A szakvéleménynek meg kell felelnie a törvényben meghatározott feltételeknek, amennyiben nem így lenne, kétségbe vonható a bizonyítási eszközből származó bizonyító erő maga. További anomália, hogy a szakértői vélemények elkészítésének költsége jelentős mértékben növeli meg az eredményes büntetőeljárás végén a terheltre hárított bűnügyi költséget, amely sok esetben nagyobb terhet ró a terheltre, magasabb összeget képvisel, mint a szerzői jogi jogsértések esetén a büntetőeljárások nagy részében alkalmazott pénzbüntetés, vagy egyéb szankció.[381] Mindez a büntetőeljárás belső arányainak felborulásával és a büntetőjogi szankciórendszer átértékelődésének veszélyével járhat.

Mindezek mellett más jellegű problémát okozhat egy-egy jogeset megoldása kapcsán egy szerzői műre vonatkozó jogi szabályozás értelmezése is. A számítástechnikai eszközökkel érintett bűncselekmények szabályozása – korábbi minták hiányában – gyakran nem megfelelően kiérlelt, a büntetőjogi dogmatika a legújabb kori kommunikációs forradalom előtti fogalomkészletével és jogi alapjaival még nem mindig képes megfelelően kezelni az új bűncselekményeket, ami gyakran vezethet egyes büntetőjogi értékek feloldásához. Mégis e veszélynek tudatában kell arra keresni a választ, hogy a növekvő kihívásoknak való megfelelés érdekében az információs társadalom jogszabályi környezetének és társadalmi viszonyainak változásában milyen módon változtathatók meg a szakértői véleményhez fűződő elvárásaink.

5.1.2. Tények és a szakvélemény értékelése

A büntetőeljárásban folytatott bizonyítás során a jogalkalmazó egyik legfontosabb feladata a bizonyítékok és a bizonyítási eszközök mérlegelése, értékelése. Erdei Árpád szerint a

[378] A torrent alapú fájlcserélő rendszereken a felhasználók adják egymásnak a tartalmat, és a rendszer lényege és hatékonysága abban rejlik, hogy már a letöltők is egyidejűleg feltöltővé válnak. Ahogy egy felhasználó gépére megérkezett egy adatcsomag, az a program működése okán azonnal megosztásra kerül.

[379] A DC++ egy úgynevezett „peer-to-peer" (P2P) hálózat, amiben nem egy centralizált szerveren keresztül folyik a fájlok átvitele, mint például egy webszerver, egy FTP szerver esetén, hanem a két felhasználó egymással áll közvetlen kapcsolatban. A kapcsolatok szervezésének központja az ún. HUB, ami lehetővé teszi kapcsolódást, beszélgetést, a megosztani kívánt tartalmak keresését. Mivel mindez egy közösségnek tekinthető, sok esetben a használat feltétele, hogy a felhasználó előírt mennyiségű vagy terjedelmű tartalmat tegyen hozzáférhetővé. Ezen mennyiségi elvárások teljesítése legtöbbször csak digitális formában létező szerzői művek megosztása útján lehetséges. Ezért a DC++ hálózat alkalmazása sok esetben szükségszerűen jár együtt a szerzői jogok megsértésével.

[380] Például a Microsoft Magyarország Kft. megkeresésével tisztázható egy Microsoft operációs rendszer telepítése során használt telepítőkód eredetisége.

[381] KÁRMÁN et al. 2011. p. 65.

bizonyítékok mérlegelése olyan hatósági gondolkodási tevékenység, amelynek során a bizonyítékok sokoldalú ellenőrzésére, hiteltérdemlőségük, bizonyító erejük megállapítására kerül sor.[382] Mindez a szakvélemények esetében sincs másként, azzal a nem lényegtelen különbséggel, hogy a vizsgált tények szakvéleményben megjelenő szakértői, majd jogalkalmazói értékelése különböző mérce szerint történik. A két fél viszonyát úgyis körvonalazhatjuk, hogy míg a szakértő feladata a tényállás valamely részének természettudományos módszerekkel történő vizsgálata, amely során – szemben a bizonyítékok értékelése során a jogalkalmazóval, aki a kétséges tényeket a vádlott javára kell, hogy értékelje – feladata a vizsgálati leletek lehetőség szerinti tárgyilagos közlése. Az ebbe foglalt bizonytalanság értékelése viszont már a jogalkalmazó kompetenciájába tartozik.[383]

Ez utóbbi értékelés problémája tömören úgy foglalható össze, hogy a jogalkalmazó azért vesz igénybe szakértőt, mert a kérdés megítéléséhez különös szakértelemre van szüksége, de végül olyan szakvéleményt kap, amely különös szakismeret nélkül nem értelmezhető. A szakértő ezzel szemben azzal a nehézséggel küzd, hogy megállapításait hogyan tudja a jogász számára is érthető formába önteni anélkül, hogy a kényszerű egyszerűsítés a szakszerűség rovására menne.[384] Egy látszólagos kitérőt téve, a szakvélemény véleményrésze lehet kategorikus, valószínűsítő és lehetőségi. Ha a leletből minden kétséget kizáróan lehet egy bizonyos vonatkozásban állást foglalni, akkor kategorikus szakvéleményről beszélünk.[385] A jogalkalmazó azonban gyakran quasi „bizonyíték-automataként" tekint a szakértőre, azaz díjának kifizetése után vásárolt termékként egzakt, kategorikus, egyértelmű választ vár feltett kérdésére. A természettudós viszont a rá kötelező, a tudományterület paradigmái szerint hozza meg állásfoglalását, amely a valószínűségszámítási és tudományelméleti megfontolások alapján legtöbbször tartalmaz valószínűségi elemet, ami kizárja a kategorikus megállapítás lehetőségét, utóbbi az ügy összes körülményének figyelembevételével a bíróság dolga.[386]

A probléma gyakorlati megjelenése többek között az, hogy – a fenti bizonytalansági elemekre is figyelemmel – melyek azok a ténykérdések, amelyeket fel lehet tenni a szakértőnek, és ezek közül is melyek azok, amiket érdemes?[387] Ennek eldöntéséhez már a bizonyításhoz és a bűncselekmény minősítéséhez szükséges előfeltevések birtokában kell lennie a kirendelőnek, ami lehetetlen a különleges szakértelem határait érintő tudás nélkül. Márpedig a tudást definiálhatjuk úgy is, hogy az információk olyan szervezése, amely lehetővé teszi az előrelátást, az oksági viszonyok megállapítását vagy az előírt döntéseket.[388]

---

[382] ERDEI, 1987. p. 231.
[383] KATONA G., Kriminalisztikai elméletek. In. BÓCZ E. (ed.) *Kriminalisztika*. BM Duna Palota és Kiadó Budapest, 2004. p. 79.
[384] KERTÉSZ I., A szakértői bizonyítás. In. Bócz E. (ed.), *Kriminalisztika.* BM Duna Palota és Kiadó Budapest, 2004. p. 225.
[385] GARAMVÖLGYI V. & VISKI L. (ed.), *Kriminalisztika.* Belügyminisztérium Tanulmányi és Módszertani Osztálya, Budapest, 1961. p. 548.
[386] KERTÉSZ, 2004. p. 225.
[387] A korábbiakban felvetett ilyen ténykérdések lehetnek: Található-e az adathordozón olyan számítógépes programalkotás, amelyet felhasználása érdekében megváltoztattak, ha igen, mennyi az értéke? Található-e az adathordozón fájlmegosztó vagy fájlcserélő kliensprogram? E segédprogramokkal történt letöltésekre (többszörözésekre) utaló adat található-e az adathordozón? Ha igen, melyek azok a zenei és filmalkotások műpéldányai, fájljai, amik azokkal kapcsolatba hozhatók?
[388] FARKAS J., Úton az ipari társadalomból az információalapú társadalom felé. In. Balogh G. (ed.), *Az információs társadalom dimenziói.* Gondolat/Infonia, Budapest, 2006. p. 97.

A felvetett problémákra visszautalva, a szakvélemények határainak kijelölése érdekében, figyelemmel arra is, hogy a jogalkalmazó munkájának hatékony segítését biztosítsuk, megfontolandó lenne olyan, törvény által előírt, időszakonként frissített, a közös jogkezelők által kezelt adatbázisok létrehozása, amelyek a jogdíjakat, kiskereskedelmi árakat, a jogosultakat tételesen és kereshető módon rögzítik. Ezzel a megoldással a jelentős munkaidőt igénylő, de nem szakkérdést képező ténykérdések megválaszolása gyorsabbá, és költségkímélőbbé válna. Szintén elgondolkodtató a szakértők helyett olyan szaktudással rendelkező, de a nyomozó hatóság állományába tartozó bűnügyi technikusok alkalmazása is, akik egyes szoftverek vizsgálatára, segédprogramok felkutatására, leírására megbízhatóan képesek. A felsorolt vizsgálatok nem tekinthetők olyan különleges szakértelmet igénylő kérdéseknek, amelyeket egy megfelelően kiképezett, a megfelelő eszközökkel ellátott bűnügyi technikus vagy szaktanácsadó jelenlétében a nyomozó hatóság tagja ne tudna megválaszolni, hiszen a bizonyítékok ereje nagy részben a vizsgálathoz igénybevett számítástechnikai eszközök megbízhatóságából ered.

5.1.3. Jogkérdés a szakvéleményben

A szakvéleményekkel kapcsolatban aggályosnak tekinthető az a szokás, hogy a – tipikusan a szerzői jogot sértő tartalmak, illetve azok szerzői jogot sértő megszerzésére vonatkozó – szakvélemények olykor jogkérdésben is állást foglalnak.[389] A Be. 99. (1) bekezdése alapján szakértőt akkor kell alkalmazni, ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges, ezért abban mind a szakirodalom, mind a bírói gyakorlat egységes, hogy jogkérdésben a szakértő nem foglalhat állást. A BH2007/397. számú eseti döntésben is megfogalmazott bírói gyakorlat szerint jogkérdésben a büntetőeljárásban szakértői vélemény nem szerezhető be, az ilyen kérdésben véleményt nyilvánító szakértő a szakértői kompetenciáján túlterjeszkedik. A hatóság – tehát nem csak a bíróság – nem bízhatja a jogi kérdések eldöntését a szakértőre, mert ez saját feladatainak átruházását jelentené. A kérdés a továbbiakban az, miként viszonyuljunk a jogkérdésben állást foglaló szakvélemény értékeléséhez. Két válasz lehetséges, az egyik szerint ebben az esetben a szakvélemény nem felel meg a Be-ben előírt feltételeknek, ezért szakvéleményként nem vehető figyelembe, és mivel legtöbbször a büntetőeljárási fő kérdésekben formál véleményt, elfogultság miatt a ténymegállapításokra szorítkozó okirati bizonyítékként sem alkalmazható, azaz ki kell zárni a bizonyítékok közül. A másik szerint a szakvélemény jogkérdésekre vonatkozó részét figyelmen kívül kell hagyni, egyebekben bizonyítékként felhasználható.

5.1.4. A jogi szakértők megengedhetőségének kérdése

A jogi szakértők megítélése már összetettebb vizsgálatot igényel. A jogszabályok tartalmát illetően az eljáró hatóságnak kell megfelelő szakértelemmel rendelkeznie. Egy jogkérdésben sem alapozhatja meg a büntetőjogi felelősséget az ítélkező bíróságon kívüli fórum döntése, mivel a jogértelmezés egyértelműen előzetes érdemi döntésnek tekinthető a kerettényállások esetén. Érdemes tehát e problémakört egy manapság már ritkán értelmezett alapelv, a *„jura novit curia”* vélelmének felelevenítésével kezdeni.

A jura novit curia tétele alapján az eljáró hatóságot – ideértve a bíróságot, ügyészséget és a nyomozó hatóságot is – többek között az emeli a jogeset elbírálására kompetenciával

[389] Például a szakértő a szakvéleményében kijelenti, hogy a számítógép adattárolóján talált művekkel a gyanúsított szerzői jogról szóló törvénybe ütköző magatartást valósított meg, vagy egy adott műpéldány megszerzése nem esik a szabad felhasználás esetkörébe.

rendelkező jogalkalmazói szintre, hogy birtokában van a társadalmi viszony megítéléséhez szükséges jogszabályi ismereteknek. Éppen ezért – figyelemmel a Be. 75. § (3) bekezdésére, amely alapján nem kell bizonyítani azokat a tényeket, amelyekről az eljáró bíróságnak, ügyésznek, illetőleg nyomozó hatóságnak hivatalos tudomása van – a jogszabály nem tárgya a bizonyításnak. Amennyiben mégis lehetővé tennénk a jogértelmezés átengedését valamennyi más esetben folytatott hatósági jogalkalmazásban, az természetszerűen vonhatná maga után a teljes igazságszolgáltatási rendszer legitimációjába vetett társadalmi bizalom megrendülését, etekintetben a hatósági jogismeret illúziója túlmutat az adott ügy elbírálásán.[390]

A hatályos jog szerint több módja is van az eljáró hatóság segítésére érdemi döntésének meghozatalában. Először tehát ezeket szükséges sorra venni, azt megvizsgálva, hogy ezen keretek közé beilleszthető-e a büntetőjogi felelősséget megalapozó, előzetes érdemi döntésként felfogható szakvélemény. A Be. lehetőséget ad az eljárás felfüggesztésére azokban az esetekben, amikor az eljáró fórum kompetencia és hatáskör hiányában szenved, azaz valamely előzetes kérdésben kell dönteni, előzetes döntéshozatali eljárást kell lefolytatni, vagy amikor a bíró észleli valamely jogszabály alkotmányellenességének lehetőségét, és ezért az Alkotmányírósághoz fordul.[391] Ezen lehetőségek alapja az, hogy adott kérdés megválaszolására az eljáró szervnek nincs hatásköre, tehát nem osztja meg, nem ruházza át eljárási, döntési jogosultságát és kötelezettségét más szervre.

A külső testület általi jogértelmezés egy másik, komoly jogtörténeti múltra visszatekintő formája a római jogi gyökerű, a császárkorban quasi jogforrásként működő jogtudósok véleménye, a ius respondendi. A jogtudomány (iurisprudentia) fejlődésének részeként a jogtudósok – később egyre inkább a császári hatalom támaszaiként – egyedi ügyekben vagy egy-egy jogkérdésben adtak ki véleményeket, amelyeket azután más, hasonló esetekben is alkalmaztak.[392]

A jogérvényesítés ezen módszerének egyik ma is továbbélő lehetősége a „bíróság barátainak” *(amicus curiae)* levelei. Az amicus curiae latin eredetű kifejezés, a jogtudósok egy-egy bonyolultabb ügy kapcsán a bírósághoz intézett véleménye, amely eredetileg egyik peres fél érdekét sem szolgáló tudományos állásfoglalásnak volt tekinthető. Simon Zoltán megfogalmazása szerint az amicus curiae levél még ma is olyan szakértői véleménynek tekinthető, amely egy-egy bonyolultabb jogi, társadalmi, politikai vagy szaktudományos kérdésben igyekszik a bíróság számára információt közvetíteni, illetve az ítélkező testület figyelmét felhívni olyan fontos vonatkozásokra, amelyek a felek perbeli cselekedetei és nyilatkozatai alapján egyébként rejtve maradnának.[393] Ahogy azt Simon kiemeli, az amicus curiae levelek érdeksemlegessége mára megszűnt. Eredeti formájukban a bíróság barátainak felszólalását jelentették, aminek egyedüli célja az ítélkező testület segítése volt az igazság keresésében, ma azonban inkább a háttérben álló érdekcsoport üzenetének „eladását” szolgálják. Azt lehet mondani, hogy a jogkérdésben állást foglaló amicus curiae levél a politikai, azaz jogalkotó színtéren működő lobbi tevékenységet kiegészítő, jogalkalmazói területen működve az ítélkezés befolyásolására irányuló törekvések egyik formája lehet. Könnyen felismerhető, hogy a bíróságon kívüli

[390] SZATHMÁRY Z., A szerzői vagy szerzői joghoz kapcsolódó jogok megsértése nyomozásának jogalkalmazási anomáliái. *Magyar Jog*, 2010/3. p. 155.
[391] Be. 188. § és 266. §
[392] FÖLDI A. & HAMZA G. (Brósz-Pólay): A római jog története és instituciói. Nemzeti Tankönyvkiadó, Budapest, 1996. pp. 84-91.
[393] SIMON Z., Érdekérvényesítés a bírói hatalmi ágban: az amicus curiae levelek http://jesz.ajk.elte.hu/simon15.html [2011-07-31]

testületektől származó, amicus curiae jellegű szakvélemények a technológiai és rendkívüli szaktudást igénylő szerzői jogi viták körében alkalmasak lehetnek a fenti helyes és helytelen érdekek érvényesítésére egyaránt.

Az életviszonyok bonyolultabbá válása, a technológia fejlődése okán a jogszabályok száma jelentősen megnövekedett a korábbi korszakokhoz képest. Egy-egy jogterület összetettsége már nemcsak természet- és társadalomtudományi kontextusban okozhat komoly fejtörést egy adott jogeset megítélésénél, hanem magán a büntető jogtudományon belül is egyre gyakrabban találkozhatunk interdiszciplináris területekkel, ilyen példának említhető a szerzői jog, amelyet kerettényállás integrált a Büntető Törvénykönyvbe. A szerzői jogi jogkérdések önálló eldöntése elkerülhetetlen a Btk. 329/A. § alkalmazhatóságánál, azonban a szerzői jog összetettsége és a technológiai fejlődés eredményeként megújuló, több jogterületet érintő elkövetési magatartások miatt a folyamatos, magas szintű hatósági felkészültség nehezen érhető el. Az EBH2000.188. számú, elvi jellegű eseti döntésében a Legfelsőbb Bíróság azonban egyértelműen kifejezésre juttatja álláspontját, amikor a következőképpen fogalmaz: szerzői és szomszédos jogok megsértésének bűncselekménye miatt emelt vád esetén a büntetőbíróságoknak önállóan kell vizsgálni, hogy a büntetőjogi felelősséget megalapozó szerzői vagy szomszédos jogi jogsértés megvalósult-e. E jogkérdések eldöntése más (polgári) eljárástól nem tehető függővé. A megváltozott jogszabályi környezet miatt ennek ellenére megfontolandó, hogy egyes jogkérdések tisztázásánál az eljáró hatóság segítséget vegyen igénybe, a továbbiakban ennek reális lehetőségét veszem sorra.

Nem büntetőeljárás jogi területen, mégis működő gyakorlatként példának tekinthető a Gazdasági Versenyhivatal azon tevékenysége, amelynek során egy-egy versenyjogi egyéni jogsérelem orvosolására indított eljárásban a versenyügy elbírálása során a bíróságot segíti az üggyel kapcsolatos szakmai álláspontjának kifejtése révén.[394]

Erdei Árpád szerint a „jogi szakértő" igénybevétele bizonyos korlátok között igenis elfogadtatható, összeegyeztethető a büntetőeljárási jog szellemével. Elképzelése alapján a jogi szakértő nem a jogi kérdést döntené el, hanem bizonyos jogszabályok létezését, és azok tartalmát bizonyítaná. Mindez nem a jogszabály hatálya alá tartozó jogi kérdés elbírálása lenne.[395] Erdei elméletének első részével egyet lehet érteni, lényegében a korábban részletezett amicus curiae levelekkel egyező tartalmú tájékoztatásnak tekinthető eljárási segédmunkát vázol, azonban a jogszabály tartalmának bizonyítása már nehezen értelmezhető. Egy jogszabály értelmezése nem lehet független a nyomozás vagy vád tárgyává tett konkrét jogviszonytól, élethelyzettől, különben megmarad az absztrakció olyan szintjén, amely hipotetikus volta miatt az adott helyzetre való alkalmazhatóságát lehetetlenné teheti. Egy jogszabály alkalmazhatóságának eldöntése a hatályossággal kezdődik, az pedig csak az adott jogviszonynak a vizsgálat körébe vonásával érhető el, amely művelet már szükségszerűen vonja maga után az egyébként elkerülni szándékolt kérdéses jogi helyzet megítélését. Erdeivel egyetértve a jogi szakértő működésének megengedhetősége garanciákkal még mindig jobban körülbástyázott jogintézmény lenne, mint jogi kérdésben a szaktanácsadó igénybevétele, vagy a hatóság informális tudakozódása.[396]

[394] http://www.gvh.hu/gvh/alpha?do=2&st=1&pg=84&m5_doc=4243&m57_act=22 [2011.07.31.]
[395] ERDEI, 1987. p. 54.
[396] ERDEI, 1987. p. 57.

A kérdéskör tárgyalása felveti még egy jogelv értelmezésének szükségességét, amelynek komoly kihatása lehet a büntetőjogi felelősség megállapításában. Amennyiben a megfelelő jogi szakértelem birtokában lévő, hatáskörrel rendelkező jogalkalmazó hatóság döntéséhez jogi szakértőre van szükség, megdől a „jog nem tudása nem mentesít" elv is. Jogosan fogalmazódhat meg a terheltben a következő: Hogyan várható el az egyszerű állampolgár jogkövető magatartása, ha a hatóság nyíltan elismeri azt a körülményt, hogy ő maga sincs birtokában a jogi felelősséget megalapozó jogszabályi ismereteknek? A válasz erre a kérdésre is az, hogy természetesen nem várható el. A büntetőjogi tényállásoknak meg kell felelniük a normavilágosság követelményének ahhoz, hogy minden állampolgár tisztában lehessen cselekménye törvényi korlátaival. A fent részletezett körülmények alapján a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének kerettényállása, a magas szintű szerzői jogi jártasságot igénylő volta és a technológia fejlődése okán, nem felel meg az említett jogbiztonsági elvárásoknak. Az elkövető „rosszhiszeműségére" nagyobb értékre történő, üzletszerű elkövetéseknél joggal lehet következtetni az alsó büntethetőségi határral nem rendelkező tényállás elemeinek megvalósulásánál, azonban a mindennapi, csekély értékekre történt elkövetésnél a komoly jogi és technológiai ismeretekkel nem rendelkező elkövető felelősségét nem minden esetben lenne indokolt megállapítani, még a társadalomra veszélyességének hiánya vagy igen csekély volta okán sem.

5.2. Egyéb bizonyítási anomáliák

A szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének fordulatai a Btk. 329/A. §-ban kerettényállásként szerepelnek, tehát az értelmezésükhöz a szerzői jogi törvény rendelkezéseit kell alapul venni. A technológiai fejlődés, valamint a számítógép és az internethasználat általánossá válásával ezen bűncselekményeket nagyszámban és tipikusan számítástechnikai úton követik el. E két körülmény a következő problémákat veti fel. A kerettényállás-jelleg azt a látszatot keltheti, hogy a büntetőjogi jogalkalmazásnak vajmi kevés szerepe van az egyes esetek, elkövetési magatartások megítélésénél, és egyfajta automatizmus érvényesülhet ezen a területen.[397] Mindezt erősíti a technológia jelenléte miatt alkalmazott informatikai szakértők szerepének felértékelődése és a különböző jog- és tudományterületek egymásra hatása miatt a büntetőjogtól idegen jogintézmények megjelenése a bizonyítási eljárásban. A dolgozat ezeket az anomáliákat igyekszik feltárni, rámutatva azok elutasításának okára és a lehetséges megoldásokra.

5.2.1. A bizonyítási teher sérelmei

Az első problémahalmazt a bizonyítási teher körüli anomáliák képezik. Aggályosnak tekinthető az a gyakorlat, amely polgári ügyben alkalmazott vélelmekkel pótolja a büntetőeljárásban alapelvként elvárt kétséget kizáró bizonyítás hiányosságait. Ilyen büntetőeljárási bizonyításba beszivárgó vélelem található a BH1992.98 szám alatt közölt jogesetben. A polgári per lezárásaként született fenti határozatában a Legfelsőbb Bíróság úgy foglalt állást, hogy a vendégek számára rendelkezésre álló helyiségekben üzemképes állapotban elhelyezett televíziós készülék esetén vélelmezhető, hogy a készüléken keresztül zeneszolgáltatás is történik, mivel köztudomású, hogy a televízió zenét is sugároz. Az IP-alapú televíziózás fejlődésével és terjedésével ráadásul a szerzői jogi védelem alá eső művek tömege válik majd elérhetővé. A probléma a következő módon

[397] OTT I., A büntetőjogi felelősség önálló elbírálása és a bizonyítási teher kérdésköre a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének egyes eseteiben. *Ügyészek Lapja* 2008/6. p. 11.

jelentkezik a gyakorlatban. Az Artisjus[398] által az egyes vendéglátóhelyeken végzett ellenőrzések során a kiállított jegyzőkönyv sok esetben nem tartalmazza a zeneszolgáltatás tényleges megtörténtének észlelését és a készülék üzemképes állapotát sem. Számos vendéglátóhely, jóllehet jövedelemfokozás céljából helyez el televízió készüléket egyik, vendégek számára nyitva álló helyiségében, azon mégis szerzői vagy szomszédos jogi oltalom alá nem eső műsorsugárzás történik, tipikus esetben közszolgálati adón keresztül történő futballmérkőzés közvetítése. A sporteseményekkel kapcsolatos vagyoni jogokról a sportról szóló 1996. évi LXIV. törvény rendelkezik, azok tehát nem tartoznak a szerzői jogi törvény hatálya alá.[399] A zeneszolgáltatásra alkalmas készülék elhelyezése önmagában nem alapoz meg jogsértést a zeneszolgáltatás megtörténtének bizonyítása nélkül, ezért ezt megkerülendő az Artisjus büntetőeljárás során is előszeretettel hivatkozik az említett polgári perben született bírósági határozatra, figyelmen kívül hagyva azt a már a BH2002.301 számú eseti döntésben is kifejtett elhatárolást, hogy a büntetőjogi és polgári jogi felelősség nem azonos fogalmak, és az egyik nem szükségszerűen előfeltétele a másiknak.

A vélelmek alkalmazása emellett a következő büntetőeljárási normába ütközik. Míg a polgári eljárásjogi bizonyítás lehetővé teszi vélelmek alkalmazását, addig a büntetőeljárásról szóló 1998. évi XIX. törvény (a továbbiakban Be.) – az in dubio pro reo elvének szellemében – egyértelműen elutasítja azt, amikor úgy rendelkezik a 4. § (2) bekezdésében, hogy a kétséget kizáróan nem bizonyított tény nem értékelhető a terhelt terhére. A vélelem nem tekinthető kétséget kizáró ténymegállapításnak, az pusztán a mindennapi életben rendszeresen együtt járó körülményekből levont tapasztalat, amely az ítélkező bíró meggyőződését alakíthatja, azonban büntetőjogi felelősséget nem alapozhat meg, bizonyítékot nem pótolhat. A megdönthető vélelem alkalmazása ugyanakkor megfordítja a bizonyítási terhet, amely a büntetőeljárás alapelveivel szintén összeegyeztethetetlen, mivel a Be. 4. § (1) bekezdése alapján a vád bizonyítása a vádlót terheli. A Be 75. § (1) bekezdése tovább erősíti a vélelem alkalmazását tiltó érveket, amikor a bizonyítás szabályainál úgy rendelkezik, hogy a bizonyítás során a tényállás alapos és hiánytalan, a valóságnak megfelelő tisztázására kell törekedni. A vélelem természetében rejlő legcsekélyebb kétely már nem jelenthet kétséget kizáró, valóságnak megfelelő megállapíthatóságot. Ahogy Király Tibor hangsúlyozza „Az igazság követelménye tehát a bűnösség megállapításához kötődik; a felmentéshez elegendő az afelőli kétség, hogy tényleg a vádlott követett-e el bűncselekményt, vagy hogy egyáltalán elkövetett-e bűncselekményt.”[400] Amennyiben a tágabb értelemben vett büntetőjog lehetővé tenné a vélelem alkalmazását a büntetőjogi bizonyítás során, arról külön rendelkezne, ahogyan azt a Be. teszi az ártatlanság vélelménél, vagy a Btk. a tizenkettedik életét be nem töltött gyermek védekezésre képtelen állapotának vélelmezésénél. A Be. a 75. § (3) bekezdésében csak az ott felsorolt körülményekre szorítja a bizonyítás mellőzésének lehetőségeit, azaz nem kell bizonyítani azokat a tényeket, amelyek köztudomásúak, vagy amelyekről az eljáró bíróságnak, ügyésznek, illetőleg nyomozó hatóságnak hivatalos tudomása van. A contrario, a vélelem alkalmazása megengedhetetlen, mivel arról az eljárási törvény nem szól. Fontos még kiemelni, hogy az ártatlanság vélelme nem tekinthető a „klasszikus” értelemben vett praesumtionak, valójában egy jogviszonyokat meghatározó norma, amely processzuális személyek egymáshoz való

[398] Az Artisjus Magyar Szerzői Jogvédő Iroda Egyesület a zenei és irodalmi szerzői jogok közös jogkezelő szervezete. Az Artisjus fő tevékenysége a közös jogkezelés jogdíjak beszedése és felosztása a zenei és irodalmi művek bizonyos felhasználása után a szerzők és örököseik részére.
[399] Szerzői Jogi Szakértő Testület 31/2000. számú szakvéleménye
[400] KIRÁLY, 2008. p. 23.

viszonyát határozza meg.[401] Hiányzik belőle a vélelmező tény, mert nincs szükség ártatlanságra mutató tényekre ahhoz, hogy az ártatlanság vélelme éljen, nem kell bizonyítani semmilyen megelőző tényt, amiből majd a törvény az ártatlanságra való következtetést megengedné.[402] A gondolatsort ismételten Király Tibort idézve zárom: „A büntetőjogban és a büntetőeljárási jogban a vélelemnek nincs nagy jelentősége, minthogy a törvény a vélelmet a vélelmező és a vélelmezett tény valószínűségi (statisztikai) kapcsolatára alapítja. ... A bírói döntést azonban nem valószínűségre, hanem bizonyosságra kell alapítani."[403]

5.2.2. Az Szjt. hatálya és a hozzá kapcsolódó problémák

Vélelemként jelenhet meg a szerzői jogról szóló 1999. évi LXXVI. törvény (a továbbiakban: Szjt.) hatályának alkalmazása is a következők miatt. Nagyszámú zenei mű vizsgálata esetén – amelyek közül több 30-40 éve jelent meg – nehezen adható jogszerű válasz azon védői bizonyítási indítványokra, amelyek az Szjt. hatályának a művekre való kiterjedésével kapcsolatosak. Ahogy a Szerzői Jogi Szakértő Testület[404] (a továbbiakban SZJSZT) többek között a szerzői jogi törvény hatályáról értekező 1/2003. számú szakvéleményében az Szjt 2. §-val kapcsolatban kifejti, hogy a törvény hatálya az olyan műre, amely először külföldön került nyilvánosságra, a törvényben meghatározott védelem csak akkor terjed ki, ha a szerző magyar állampolgár, vagy ha a szerzőt nemzetközi egyezmény vagy viszonosság alapján a védelem megilleti. A szerzői műveknek az egyes országok szerzői jogi törvényeinek területi hatályán túllépő védelmét az 1886. évi Berni Egyezmény (BUE) biztosítja, amelynek Magyarország 1922. óta tagja, és amelynek felülvizsgált szövegét az 1975. évi 4. tvr. hirdette ki.[405] A BUE-nak jelenleg 150 tagországa van, ezért az internetről letöltött műről alappal feltételezhető – tehát vélelmezhető –, hogy származási helye valamely BUE-hez tartozó állam, azaz kiterjed rá az Szjt. hatálya.[406] A védői indítványok elutasítása pusztán a nagy valószínűség miatt érezhetően támadható álláspont, a művek jogosultjainak egyenkénti kiderítése, majd a művek értékének meghatározása jelentős szakértői munkaórát generálva növeli az eljárás költségét, elhúzhatja magát a bizonyítási eljárást. Mindez azonban a mai zenei trendek tudatában csak szélsőséges eset, a szakértői vizsgálat nagy valószínűséggel minden zenei műre megállapíthatóvá teszi az Szjt. hatályát, azonban a kétséget kizáró bizonyítást megkövetelő jogszerű eljárás az említett folyamatot szükségessé teheti.

5.2.3. Az elkövetés időpontja

A számítógépes programalkotások kérdésében nem egységes még a gyakorlat abban a kérdésben, hogy a nem jogtiszta szoftverekkel visszaélés vajon állapot-bűncselekménynek tekinthető-e vagy sem. A kérdés számos bizonyítási problémát vet fel, hiszen gyakran

[401] KIRÁLY, 2008. p. 129.
[402] KIRÁLY, 2008. p. 129.
[403] KIRÁLY, 2008. p. 248.
[404] A Szerzői Jogi Szakértő Testületet 1970-ben hozták létre. Feladatait, szervezeti és működési rendjének keretszabályait a szerzői jogról szóló 1999. LXXVI. törvény (Szjt.) állapította meg újra. Az Szjt. 101. § (1) bekezdése szerint a Testület a Magyar Szabadalmi Hivatal mellett működik. Az Szjt., illetve a Szerzői Jogi Szakértő Testület szervezetéről és működéséről szóló 156/1999. (XI. 3.) Korm. rendelet alapján, a Testület szerzői jogi jogvitás ügyekben felmerülő szakkérdésekben a bíróságok és más hatóságok megkeresésére, illetve a felhasználói jog gyakorlásával kapcsolatos kérdésekben peren kívüli megbízás alapján jár el. Forrás: http://www.mszh.hu/testuletek/szjszt/ [2011-07-31]
[405] A BUE 5. cikk (1) bekezdése kimondja, hogy a BUE bármely tagországában először nyilvánosságra hozott műre a többi tagországban a nemzeti elbánás elvét kell biztosítani.
[406] SZJSZT 1/2003. sz. szakvéleménye

nehéz megállapítani az elkövetés időpontját, ami például az elévülés kérdésében fontos szempont. Egyes jogalkalmazók az elkövetési magatartást görcsösen a többszörözéshez kötve úgy foglalnak állást ebben a kérdésben, hogy az elkövetés ideje a programalkotás nem jogszerű megszerzése (letöltése, felmásolása a számítógépre) vagy feltelepítése. A másik – helyes – álláspont a szerzői jogi törvény következő rendelkezéseiből indul ki. Az Szjt 17. §-a példálózó jelleggel sorolja fel a mű felhasználásának eseteit, azaz nem kimerítő jelleggel. Egy számítógépes programalkotáson a törvény sajátos jogvédelmi rendszere okán a felhasználó nem tulajdonjogot, hanem jogdíjfizetés ellenében használati jogot szerez. A szoftver felhasználása tehát kiterjed az adattárolón elhelyezett szoftver birtoklására, tárolására is. A jogdíj fizetése nélkül tárolt, futtatott, alkalmazott szoftver esetében a jogellenes állapot mindaddig fennáll, amíg az az adattárolón „használható" formában megtalálható.[407] Meglehetősen problémás ugyanakkor az első esetben az elkövetés időpontjának meghatározása is, mert ahogy azt a témában a Somogy Megyei Főügyészségen számos különböző területről érkezett jogalkalmazó részvételével rendezett kerekasztal-beszélgetésen cserélt tapasztalatokból is megállapítható, a szakértők általában a számítógép belső órájának beállítására hivatkozva csak hozzávetőleges letöltési időpontot tudnak megállapítani.[408]

5.2.4. Az egyéni felelősség bizonyítása

Egyetértve Ibolya Tibor álláspontjával az audiovizuális művek letöltésével elkövethető szerzői jogi bűncselekmények bizonyítása számos büntetőjogi alapelvbe ütközik. A torrent technológia használata során a szabad felhasználás esetkörébe tartozó „letöltés", azaz többszörözés mellett a folyamat „feltöltéssel", az Szjt. 26-27. §-a szerinti *nyilvánossághoz történő közvetítéssel* is jár.[409] A gyakorlatban azonban mindez puszta vélelemnek tekinthető, hiszen a felhasználó magában a kliensben vagy a tűzfalon le is tilthatja a seedelést, másrészt pedig azért, mert egy sokak által seedelt fájl letöltésénél hiába kínálja fel a már letöltött fájldarabot a program, ha az nem tartozik a leggyorsabb kapcsolatok közé, nem jön létre a kapcsolat és ekként a feltöltés sem, továbbá abban az esetben sincs feltöltés ha például a letöltő olyan bolyhoz csatlakozik, ahol rajta kívül nincs más letöltő, azaz mindenki seedel.[410]

Egy következő értelmezésre szoruló, technológiai gyökerű probléma, hogy a seedelés fájlszeletekre vonatkozik, ami nem képezi a szerzői mű egészét. Jóllehet a szerzői jogi védelem a Szjt. 16.§ (1) bekezdésében foglaltak alapján a szerzői mű valamely azonosítható részét is megilleti, ami a SzJSzT 7/2008. számú szakértői véleménye szerint a felhasználó általi „érzékelhetőséget" jelenti, Ibolya Tibor szerint azonban a fájlszeletek egyes felhasználók általi feltöltése ennek nem felel meg. Érvelése szerint az egyes fájlszeletek nem érzékelhetők, mert önmagukban nem játszhatók le, nem nézhetők és hallgathatók meg, az azonosíthatóság (érzékelhetőség) csak a folyamat végén, az akár több százezer forrásból (egyéni felhasználótól) származó adatmennyiség összeillesztése után következik csak be, a letöltő számítógépén.[411] Hangsúlyozandó, hogy a büntetőjogi felelősség ezzel szemben individuális, az egyéni felhasználót a Btk. 329/A §. (1)

[407] Ezt az álláspontot képviseli a Legfőbb Ügyészség, amelyet Nf.6625/2007. számú, eseti jellegű állásfoglalásában fejtett ki.
[408] DR. JÁVORSZKI–DR. RONGÁNÉ DR. SRAKTA, A szerzői vagy szerzői joghoz kapcsolódó jogok megsértése bűncselekményének jogalkalmazási kérdései. *Ügyészek Lapja* 2008/5. p. 39.
[409] A *seed* egy olyan *peer* (másik számítógépen futó kliens), amely rendelkezik az összes darabkával, és azt megosztja, vissza-, illetve feltölti a fájlt. Minél több *seed* van, annál nagyobb az esélye a gyors letöltésnek.
[410] IBOLYA T., A torrentrazziák büntetőjogi megítélése. *Belügyi Szemle*, 2011. (59. évf.) 2. sz. pp. 49-59.
[411] IBOLYA, 2011. pp. 49-59.

bekezdésében foglalt bűncselekmény elkövetésének megalapozott gyanúja esetén is csak a saját tevékenysége miatt lehet felelősségre vonni.

6. A FEJEZET ÖSSZEFOGLALÁSA

A jog mint a társadalom egyik funkcionális rendszere olyan közvetítő folyamatok eszközével fogadta be magába az új tudást, mint oktatás, szakértők meghallgatása, valamint a kutatás és gyakorlat kombinálása az egyetemeken, így alakítva ki a tudománnyal szembeni igényeit, azonban a tudás többközpontúvá válásának elterjedésével e munkamegosztás gyengülése vehető észre.[412] Az információtömeg – benne a társadalmi viszonyok és jogszabályok tömegével – megfelelő kezelésének elvárása már nem csak a más tudományterülethez tartozó szakértői vélemények kontrolálását nehezíti meg, hanem a több jogágat és jogterületet érintő kérdések megoldására irányuló jogalkalmazást is.

A fejezetben felelevenített problémákon keresztül jól érezhető az a tudásbeli határvonal, amelyet az adott jogi probléma megoldása érdekében a jogalkalmazónak és a szakértőnek – egymás felé ugyan – egyaránt át kell lépnie. Mivel mindez olykor a büntetőjogi alapelvek megsértésével érhető csak el, érdemes megfontolni olyan új büntető eljárásjogi intézmények bevezetését, amelyek kellő garanciák mellett a jogalkalmazó munkáját megkönnyítik.

[412] FARKAS, 2006. pp. 121-122.

X. FEJEZET: A NEMZETKÖZI EGYÜTTMŰKÖDÉS EGYES PROBLÉMÁI

1. A JOGHATÓSÁG KÉRDÉSE

A nemzetközi elemmel bíró bűncselekmények elkövetőivel szembeni eljárás alapja a nullum crimen sine lege alapelvének nemzetközi büntetőjogi vetülete, a kettős inkrimináció. Az egységes jogi alap megteremtése után a következő kihívást az érintett államok joghatósági összeütközésének feloldása jelenti és az eljárás hatékony lefolytatásának biztosításában történő együttműködés.

Az EU Igazságügyi Tanácsa a 2011. április 12. napján tartott ülésén a kiberbűnözés elleni új irányelv-tervezet vitáját folytatta le. Az *„Európai Parlament és Tanács irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat hatályon kívül helyezéséről”* című javaslat célja, hogy korszerűsítse a korábbi, 2005-ös kerethatározatot többek között a „botnet”-alapú elkövetések büntethetőségének megalapozásával, és az úgynevezett személyazonosság lopás *(identity theft)* bűncselekménnyé nyilvánításával. A javaslat az információs rendszerek elleni támadásokról szóló, 2005. február 24-i 2005/222/IB tanácsi kerethatározat felváltására irányul, amely kerethatározat célkitűzése a preambulum szerint a tagállamok igazságügyi és egyéb hatóságai – beleértve a rendőrséget és egyéb bűnüldöző szakszolgálatokat – közötti együttműködés javítása a tagállamok büntetőjogszabályainak az információs rendszerek elleni támadások területén történő további közelítése révén. Ezen új irányelv tervezete meghatározza a bűncselekményi tényállásokat az informatikai rendszerek elleni támadások területén, létrehozza az ilyen bűncselekményekre vonatkozó büntetési tételekhez kapcsolódó szabályozási minimumokat. További célja, hogy külön rendelkezéseket vezessen be ezen a területen az említett támadások megelőzése, az európai büntetőjogi együttműködés javítása érdekében.

Utóbbi vonatkozásában kiemelésre érdemes az irányelv-tervezet 13. Cikke, amely a joghatóság kérdéskörével foglalkozik. A cikk alapján a tagállamok joghatóságát megalapozza az irányelvben meghatározott bűncselekmények elkövetése, amennyiben a bűncselekményt a) egészben vagy részben az érintett állam területén követték el, vagy b) az elkövető személy az érintett tagállam állampolgára vagy szokásos tartózkodási helye az adott tagállamban van, vagy c) olyan jogi személy javára követték el, amelynek az érintett tagállam területén van a székhelye.

Önmagában az elkövetés helye nem jelent nagy segítséget a bűnüldözés hatékonyságának javításában, azonban a cikk (2) bekezdésének értelmezése szerint minden tagállam biztosítja, hogy a joghatóság kiterjedjen azokra az esetekre is, amikor a) az elkövető a bűncselekmény elkövetésekor fizikailag jelen van az érintett tagállam területén, függetlenül attól, hogy a bűncselekmény a területén található informatikai rendszer ellen irányul-e, vagy b) a bűncselekmény az érintett tagállam területén található informatikai rendszer ellen irányul, függetlenül attól, hogy az elkövető a bűncselekmény elkövetésekor fizikailag jelen van-e az adott tagállamban.

E rendelkezés egy európai szintű joghatósági összeütközés rendezésére alkalmas ugyan, azonban a jelenlegi és várható problémák megoldására önmagában nem elegendő. Egyrészt a büntetőeljárás egyik lényeges eleme a bűncselekmény elkövetőjének felkutatása és a bűnösség bizonyításához szükséges bizonyítékok beszerzése. A hatékony bizonyítás gyakorlati problémáját a joghatóság kérdésének elméleti rendezése még nem oldja meg. Másrészt az internet virtuális fejlődése okán a „hollét” akár egyszerre több állam területén

is lehetséges, vagy éppen „sehol” (pl.: nemzetközi vizek, bukott államok), továbbá az automatizáltható elkövetési magatartások megjelenése miatt a kérdés sokszor nem is csak a hol, hanem a „mikor”.

2. A BŰNÜGYI EGYÜTTMŰKÖDÉS EGYES KÉRDÉSEI

A nemzetközi bűnügyi együttműködés kiépítése érdekében számos nemzetközi egyezmény született és megannyi nemzetközi szervezet jött már eddig is létre, sokuk egy-egy bűncselekmény-csoport hatékonyabb üldözésére. Ilyen általános, a részes tagállamok bünügyi hatóságai között egyfajta koordinációs tevékenységet folytató, jogsegélyeket és információcserét bonyolító, együttműködést segítő szervezetnek tekinthető például az Interpol, az Europol, az Eurojust, amely szervezetekre vonatkozó jogszabályok, egyezmények ismertetésére egyrészt terjedelmi okok miatt nem kerül sor, másrészt a dolgozat témája szempontjából egyedi attribútummal nem rendelkeznek.

Európai szinten – a shengeni együttműködés részletes szabályainak ismertetését mellőzve – a bűnügyi együttműködés egyszerűsítésére a Tanács 2006/960/IB kerethatározata is tett már lépéseket a pontos és naprakész információkhoz, köztük a bűnüldözési operatív információkhoz való gyors hozzáférés biztosítására törekedve. Az említett kerethatározat 1. Cikk (4) bekezdése azonban még mindig határozottan védi a tagállamok szuverenitását, amikor a következőképpen rendelkezik. A kerethatározat a tagállamokat semmiféle módon nem kötelezi arra, hogy az igazságügyi hatóságok előtt bizonyítékként felhasználható információt és bűnüldözési operatív információt szolgáltassanak, és nem jogosít fel az ilyen információ vagy bűnüldözési operatív információ e célra történő felhasználására. Amennyiben valamely tagállam az e kerethatározatnak megfelelően beszerzett információt vagy bűnüldözési operatív információt bíróság előtt bizonyítékként fel kívánja használni, be kell szereznie az információt vagy bűnüldözési operatív információt szolgáltató tagállam beleegyezését, szükség esetén az információt vagy bűnüldözési operatív információt szolgáltató tagállam nemzeti joga szerint, a tagállamok között hatályban lévő, az igazságügyi együttműködésre vonatkozó eszközök alkalmazása útján. E beleegyezés beszerzése nem szükséges, amennyiben a megkeresett tagállam az információ vagy bűnüldözési operatív információ átadásakor beleegyezését adta annak bizonyítékként történő felhasználásához.

A Magyarországon a 2007. évi CXII. törvénnyel kihirdetett prümi egyezmény további kezdeményezéseket tartalmaz a bűnügyi együttműködés javítására például automatizált adatkeresés rendszerének kiépítésével a DNS-profilok területén. Azonban az egyezmény is általános együttműködés dokumentumának tekinthető, az informatikai bűncselekményekre vonatkozóan nem tartalmaz érdemleges rendelkezést.

Az EU bel-és igazságügyi politikájának a 2011-2015. közötti időszakára vonatkozó programja (Stockholmi Program)[413] előirányozza az európai bizonyítékgyűjtési rendszer kidolgozását, tehát e területen jelentős javulásra lehet számítani. A program számítástechnikai bűnözéssel foglalkozó 4.4.4. pontjának tervei szerint a tagállamoknak mielőbb meg kell erősíteniük az Európa Tanács számítástechnikai bűnözésről szóló, 2001. évi egyezményét. Ez az egyezmény szolgálhatna globális szinten a számítástechnikai bűnözés elleni küzdelem jogi referenciakeretéül, míg az Europol pedig az európai forrásközpont szerepét tölthetné be azáltal, hogy az észlelt bűncselekmények jelzésére

[413] Európai Tanács: A Stockholmi Program – A polgárokat szolgáló és védő, nyitott és biztonságos Európa EU HL (2010/C 115/01)

szolgáló európai fórumot hoz létre, amely segíti a tagállamok nemzeti figyelmeztető platformjait a legjobb gyakorlatok cseréjében.

Még mindig a Cyber-crime Egyezmény tekinthető a legátfogóbb nemzetközi jogi alapnak, amely tartalmazza az információs rendszerek elleni támadások miatt indult büntetőeljárások ügyében folytatott bűnügyi együttműködésre vonatkozó speciális szabályokat. Egyrészt elrendeli egy a hét minden napján, napi 24 órában működő, úgynevezett 24/7 elnevezésű hálózat felállítását. Az Egyezmény 35. Cikke alapján minden szerződő fél kijelöl egy éjjel-nappal, a hét minden napján elérhető kapcsolattartási pontot, annak érdekében, hogy lehetővé tegye a számítástechnikai adatokkal és rendszerrel összefüggő bűncselekményekre vonatkozó nyomozásokkal vagy a bűncselekményekre vonatkozó elektronikus bizonyítékok összegyűjtésével kapcsolatos azonnali segítségnyújtást. Ez a segítségnyújtás felöleli a következő intézkedések megkönnyítését vagy, ha azt a belső jog és a gyakorlat lehetővé teszi, közvetlen foganatosítását: *a)* technikai tanácsok átadása; *b)* adatok megőrzése a 29. és 30. Cikk szerint; *c)* bizonyítékok összegyűjtése, jogi információk átadása és a gyanúsítottak tartózkodási helyének meghatározása. A Fél kapcsolattartási pontja számára biztosítani kell azokat az eszközöket, hogy késedelem nélkül tarthassa a kapcsolatot a másik Fél kapcsolattartási pontjával. *b)* Ha a Fél által kijelölt kapcsolattartási pont független a Fél nemzetközi jogsegélyért vagy kiadatásért felelős hatósága(i)tól, a kapcsolattartási pontnak alkalmasnak kell lennie ezen hatóság(ok)kal történő késedelem nélküli együttműködésre.[414] A hálózat működtetésének megkönnyítése érdekében minden Szerződő Fél biztosítja a képzett és megfelelően felszerelt személyzetet. Az Egyezmény emellett számos, a digitális bizonyítékok beszerzését lehetővé tevő kényszerintézkedés határokon átívelő – jogsegély eljárás keretében történő – alkalmazásának alapjait is megteremti.

Az együttműködés javítására a már tárgyalt, a 2005/222/IB kerethatározat felváltását tervező, EU Parlamenti és Tanácsi irányelv tervezete szerint a tagállamok továbbra is üzemeltetik a napi 24 órában működő információs szolgálatot, amelynek közreműködésével minden tagállam kötelezettséget vállal a sürgős kérdések 8 órán belüli megválaszolására.

3. A FEJEZET ÖSSZEFOGLALÁSA

Az internet, a virtuális világ életterében elkövetett jogellenes cselekmények szankcionálására elméletileg létezik alkotmányosan igazolható módszer: egy, valamennyi állam által elfogadott, ha úgy tetszik nemzetközi szerződésben rögzített tényállásokból összeállított büntetőkódex, amelynek végrehajtására valamennyi állam kötelezettséget vállal. Az ördög azonban a részletekben rejtőzik, hiszen a büntetőeljárás lefolytatására az univerzalitás elve alapján eddig is bármely állam rendelkezett joghatósággal a kérdéses bűncselekmények üldözésére, azonban a konkrét eljárási cselekmények foganatosítása, a bizonyítékok felkutatása, hiteles beszerzése, biztosítása olyan kihívás, amelynek jelenleg egyetlen nemzetközi egyezmény sem tud megfelelni.

A virtuális jövőre figyelemmel a hatékony megoldás nyilván egy univerzális, szupranacionális bűnüldöző szerv létrehozása lenne, amely joghatósággal rendelkezne valamennyi, virtuális térben elkövetett bűncselekmény üldözésére, azonban mindez költséghatékonysági szempontból aránytalan lenne a csekélyebb súlyú bűncselekmények

[414] Magyarországon ez a kapcsolattartási pont az ORFK Bűnügyi Főigazgatóság Nemzetközi Bűnügyi Együttműködési Központja (NEBEK), amely az i-24/7 hálózatot működteti.

felderítése esetén, másrészt további komoly szuverenitási kérdéseket vetne fel. Amennyiben az állami szuverenitás klasszikus elemeire, a meghatározott (föld)területre és az ott élő lakosságra a virtuális tér szempontjából tekintünk, be kell látnunk, hogy a világháló területi szerkezete kikezdi az állami főhatalom, azon belül az állami büntetőhatalom érvényesítésének formáit.[415] A nemzetközi kapcsolatokkal érintett jogi problémák rendezése egy kisebb állam részéről a legtöbb esetben felveti az érdekérvényesítés hatékonyságának kérdését, mindez hatványozottan igaz az internet szabályozása körül folytatott szüntelen vitákra vonatkoztatva is, amelyben a magyar alkotmányos szempontok játszák a legkevesebb szerepet. Erre a következtetésre juthatunk, amikor például az Európai Gazdasági és Szociális Bizottságnak (EGSZB) az Európai Unió Bizottságának a kritikus informatikai infrastruktúrák védelméről szóló COM(2009) 149 számú közleményéhez fűzött véleményezését olvassuk. Az EGSZB szerint[416] a biztonság érdekében az EU-nak úgy kellene tovább erősítenie az internet jövőbeli szabályozására vonatkozó álláspontját, hogy közben az Egyesült Államok nemzeti prioritásait is tiszteletben tartja, ám egyben az Európai Unió érdekeit is tükrözi.

[415] Az egyik legismertebb, a szuverenitás érvényesítésével kapcsolatos eset a *Yahoo!*-ügy volt. Az amerikai székhelyű *Yahoo!* honlapján náci tárgyakat árvereztek a felhasználók, és emiatt két francia szervezet (a LICRA és az UEJF) 2000-ben pert indított, arra hivatkozva, hogy a *Yahoo!* aukcióin eladásra kínált náci relikviák forgalmazása a francia törvények szerint jogellenes. A francia Legfelsőbb Bíróság ítéletében kimondta, hogy a *Yahoo!* köteles olyan szűrési rendszert kialakítani, ami kizárja a francia internetezőket a náci relikviák árveréseiből, ellenkező esetben napi százezer frank büntetést kell fizetnie. A *Yahoo!* – bár megváltoztatta aukciós gyakorlatát – az ítéletet nem ismerte el magára nézve kötelezőnek és a kaliforniai bíróságtól kérte annak megállapítását, hogy egy amerikai székhelyű cégre nem érvényes a Franciaországban hozott ítélet. 2001-ben az amerikai bíróság kimondta, hogy a *Yahoo!* nem köteles betartani a tartalomkorlátozó francia ítéletet: az Amerikából üzemeltetett weboldalakra az amerikai törvények vonatkoznak, és az alkotmány első kiegészítése értelmében a tulajdonosnak joga van a szólásszabadsághoz, a külföldi bíróságok ítéletei nem hajthatók végre.

[416] Az EGSZB 2009. december 16. napján elfogaott 2010/C 255/18 számú véleménye 2.12. pont.

X+1. FEJEZET: AZ ÚJ BTK. TERVEZETE

A felvetett anyagi jogi problémák időszerűsége miatt szükséges egy rövid fejezet erejéig kitérni a büntetőjogi kodifikáció eredményeként megjelent Btk. tervezet egyes elemeire.

A számítástechnikai bűncselekmények vonatkozásában a tervezet azon álláspontra helyezkedik, hogy észlelve a jelenleg hatályos 300/C. § összetettségét feldarabolva, két fejezetben helyezi el a jelenleg a gazdasági bűncselekményekről szóló fejezetben található tényállásokat. A számítógépes csalás (jelenleg 300/C. § (3) bek.) a vagyon elleni bűncselekmények közé kerülne, míg a jogosulatlan belépés (jelenleg 300/C. § (1) bek.), a számítógépes szabotázs (jelenleg 300/C. § (2) bek) és technikai intézkedés kijátszása (jelenleg 300/E. §) önálló fejezetet kapna. Emellett a számítástechnikai rendszer működésének jogosulatlan akadályozása a konkrét elkövetési magatartások példálózó felsorolásának elhagyásával nyitott törvényi tényállásként élne tovább az informatikai rendszer működésének jogosulatlan akadályozását eredményként meghatározva.

Jelentős és helyes irányú változást hozhat azon jogalkotói szándék megnyilvánulása, amely a jelenleg hatályos 329/A. § alapesetét akként módosítaná, hogy egyrészt a „más *vagy mások*” szerzői vagy szerzői joghoz kapcsolódó jogának megsértése, másrészt az elkövetés célzataként a *rendszeres* haszonszerzés kerülne be új tényállási elemként. E megoldással egyszerűsödnének a halmazati kérdések, hiszen a rendszeres haszonszerzésre törekvés és a több jogosultat érintő jogsértés meghatározása lényegében az üzletszerűség tényállásba emelésének feleltethető meg. A tényállás e változtatással közelebb kerülne a Cyber-crime Egyemény szerzői jogi jogsértésekre vonatkozó ajánlásához is, amely elsősorban a kereskedelmi méretekben történő jogsértések kriminalizációját tartotta szükségesnek. A tényállás módosítása mellett az új Btk. 100.000.- forintot meghaladó összegben határozná meg a bűncselekmény alsó értékhatárát, tehát biztosítva lenne a tényállás arányossága.

Ami azonban külön figyelmet és értékelést érdemel az magának a jogalkotó szándéknak a nyilvánosságra kerülése. A korábbi fejezetek alapján egyértelműen alkotmányellenesnek tekinthető tényállásnak az ilyen jelentős mértékű módosítása (pontosabban annak reménye), a cselekmény társadalomra veszélyességének megítélését érintő jogalkotói hozzáállás ily mértékű változása két további megfontolást vet fel. A tényállásnak a büntetőjogi szigort érintő ily jelentős módosítására irányuló és a (jogász)társadalom értékítéletével várhatón egybehangzó jogalkotói szándék nyilvánosságra kerülése miatt joggal volna elvárható, hogy a jogalkotó az új Btk. elfogadása előtt már módosítsa a tényállást, hiszen az érintett alapjogoknak a tervezet megjelenésével már deklaráltan is elismert alkotmányos sérelme nem várhat további politikai vagy jogalkotási vitákra, figyelemmel a Btk. utóbbi időben történt gyakori, csekélyebb vonatkozású módosításira is.

Az új Btk. hatályba lépését megelőző módosítások elmaradása esetén viszont a jogalkotó sem vonatkoztathat már el a cselekmény társadalomra veszélyességének jogalkotói megítélését érintő változástól az egyes jogesetek megítélése során.

MEGÁLLAPÍTÁSOK, KÖVETKEZTETÉSEK ÉS JAVASLATOK

1. MEGÁLLAPÍTÁSOK ÉS KÖVETKEZTETÉSEK

Az információs társadalom által életre hívott új életviszonyok változásait vizsgálva az értekezés célja annak feltárása volt, hogy miként hatott a kiérlelt alapelvekkel, szilárd dogmatikával rendelkező büntetőjogi jogalkotásra és jogalkalmazásra a szabályozási környezet változása, és milyen újabb kihívásokat támaszt feléjük az információs társadalom fejlődése. Az értekezés további két kérdésre kereste a választ: Miként adható helyes válasz az információs társadalom társadalmi és gazdasági rendet sértő cselekményeire? A hatályos magyar büntetőjogi jogszabályok adta válaszok megfelelnek-e a magyar alkotmányos büntetőjog elveinek?

Az értekezés Általános Része alapján megállapítható, hogy az információs kommunikációs technika alapvető hatással van a közösségi együttélésre, a társadalom szinte valamennyi alrendszerét érintő befolyással rendelkezik. Az IKT kihat a felhasználói szokásokra, szerepe van a felhasználók értékrendjének átalakulásában, egyes új devianciák megjelenésében, ugyanakkor hozzáférésükhöz és megbízható működésükhöz új társadalmi érdekek társulnak, ami büntetőjogi szempontból az új jogi tárgyak megjelenéséhez vezetett. A technológiai környezet által életre hívott társadalmi viszonyok a büntetőjogi dogmatika korábbi kategóriáival azonban nehezen kezelhetők, a kizárólag megszorító értelmezéssel opráló büntetőjogi fogalmak, normák kereteit sok esetben szétfeszíti a technológiai fejlődés és a vele együttjáró változás az élethelyezetek megítélésével kapcsolatban, gondoljunk a magánszféra határainak alakulására, az ember és a technológiai környezet kapcsolatára vagy a virtuális tér földrajzi-joghatósági vonatkozására. Az információs társadalom fejlesztési programjai és az infrasruktúra biztonságának megteremtésére irányuló szabályozás elemei részben olyan új kihívásokra adott válaszok, amelyek hozadéka az egyre szorosabb, szuverenitást is érintő államok közötti együttműködés. Ekként az információs társadalom szabályozási környezete alapvető befolyással bír a magyar alkotmányos büntetőjogi jogszabályok kialakításában. Világossá vált, hogy az infokommunikációs konvergencia hatásaként olyan új jogi helyzetek alakulnak ki, amelyek helyes minősítése a büntetőjogi fogalomrendszertől idegen, túlnyomó részt más tudományterületek ismeretinek birtokában oldható meg. Azaz az elemzett bűncselekmények elbírálását illetően jelentősen felértékelődik az interdiszciplináris tudás alkalmazása mind a jogalkotás, mind a jogalkalmazás során. Az alkotmányos büntetőjogi elvárásoknak megfelelő szabályozás megteremtéséhez ezért a szabályozandó környezet önálló fogalmi rendszeréből szükséges építkezni, amely figyelemmel van a technológiai fejlődés irányaira is. Csak így biztosítható a kellően pontos, meghatározott normatartalom, amely hosszabb távon képes megőrizni a tényállás alkalmazhatóságát a jogbiztonság elvárásának megfelelve.

A Különös Részben az egyes tényállásokat érintő vizsgálatok, elemzések alapján kijelenthetjük, hogy a hatályos szabályozás bizony sok tekintetben nem teljesíti az alkotmányos követelményeket. A Btk. 300/C. § és 300/E. §-okban meghatározott számítástechnikai bűncselekményi tényállások rendszertani elhelyezése és a 300/C. §-on belüli több tényállás egybeszerkesztése alapvetően elhibázott, amely jogértelmezési problémák mellett a bűnüldözési munkatehert torzító, indokolatlan illetékességi koncentrációhoz is vezet. A tényállások megfogalmazása részben megfelel az alkotmányos büntetőjog követelményeinek, kellően rugalmasnak és az „egyéb művelet végzése” fordulat kivételével pontosnak tekinthető, azonban koncepcióját illetően nincs figyelemmel az IKT általános és számos jogtárgyat érintő elterjedtségére. Az is észrevehető

ugyanakkor, hogy az egyes jogesetek minősítésekor gyakran vezet látszlólagos alaki halmazathoz a számítástechnikai rendszer működésének járulékos vagy szükségszerű megzavarása valamely más jogtárgy elleni támadás során, amely már túlmutat a tényállás eredeti célján.

A szerzői jogi bűncselekmények vizsgálatának eredményeképpen egyrészt megállapítható, hogy a Btk. 329/A. §-a egyértelműenb az alkotmányos büntetőjog elveibe ütközik. Másrészt – részben az infokommunikációs konvergencia hatására – a szerzői jog összetett szabályozási rendszerének jogi helyzeteit a büntetőjogi dogmatika nehezen – sok esetben egyáltalán nem – képes a jogbiztonságnak megfelelően kezelni. A tényállás gyakorlati alkalmazásának problémáira nem csak az anyagi jogi minősítés területén, a halmazati kérdések eldöntését és a sértettek meghatározását illetően derült fény, hanem a minden büntetőeljárás lényegét jelentő bizonyítás eljárás anomáliáinak felfedése során is. A szerzői jogi tényállás következésképpen nem egyeztethető össze az alkotmányos büntetőjog elveivel.

A hazai büntetőjog egyik legfiatalabb – hagyományok nélküli – tényállása, a zaklatás híven tükrözi életkorának sajátosságait: fejletlen, bizonytalan jogértelmezést tesz lehetővé és nincs kialakult gyakorlata. Az információs társadalom új trendjei, a kommunikáció környezetének változásai, a védett jogi tárgy, a magánszféra átalakulása mind-mind olyan körülmények, amelyek a büntetőjogi fogalomrendszerben nehezen értelmezhetők, ekként nemcsak a tényállás megfogalmazása és értelmezése, hanem a vitás élethelyzetekhez való vonatkoztatása is hordoz magában visszaélésekre lehetőséget, hiszen az egyének magánszférához fűződő érzékenysége sem egyforma.

A nemzetközi bűnügyi együttműködés területén folytatott vizsgálatok alapján megállapítható, hogy a Cyber-crime Egyezmény megkötése óta igazán jelentős előrelépés nem történt a számítástechnikával érintett bűncselekmények elleni fellépés területén. A nemzetközi bűnügyi együttműködés alapját képező közös anyagi jogi alap megteremtése megtörtént, valójában a komolyabb eljárásjogi kihívások jelentik továbbra is a fő problémát, amely területen érehető az EU részéről a szabályozási szándék, azonban az csupán a problémák ismertetésére szorítkozó dokumentumokban jelenik meg. A nemzethatárokon átnyúló operatív rendőri tevékenység, az egységes bizonyítási eljárás (ideértve a bizonyítékok felkutatását, összegyűjtését, cseréjét, stb.) kialakítása, a joghatósági összeütközések feloldása olyan állami szuverenitást alapjaiban érintő politikai kérdés, amelynek rendezése nem alkotmányos büntetőjogi kérdés, ezért részletesebb boncolgatására az értekezésben nem került sor.

2. JAVASLATOK

2.1. A számítástechnikai bűncselekmények vonatkozásában

Mivel a jelenleg a Btk. 300/C. § és 300/E. §-okban meghatározott számítástechnikai bűncselekményi tényállások nem kizárólag a gazdasági élet védelmére korlátozódnak, hanem annál sokkalta szélesebb társadalmi értékek, érdekek védelmére hivatottak, ezért a Btk. rendszertani felépítésének való megfelelés miatt is érdemes fontolóra venni a lehetséges társadalmi érdekeket megtestesítő minősített esetekkel kiegészített tényállásokat összegyűjtve a Btk. önálló, számítástechnikai bűncselekményeket magába foglaló fejezetének megalkotását.

Egy önálló büntető törvénykönyvi fejezet, a tényállások szétbontásával és a megfelelő minősített esetek kiegészítésével cizelláltan, és a lehetséges jogi tárgyakra érzékenyen lenne képes e bűncselekményi kör dogmatikailag is helyes szabályozására, és ezáltal a hatályos büntetőeljárási törvény szerinti illetékességi visszásságokat is könnyebben rendezni lehetne.

Az önálló büntető törvénykönyvi fejezet a következőképpen épülne fel. A fejezet tartalmazná a jelenlegi 300/C. § bekezdéseit szétbontva, önálló szakaszokban megfogalmazva, a jelenlegi 300/E. §-t, valamint a fogalom-meghatározásokat tartalmazó 300/F. §-t, kiegészülve a számítástechnikai bűncselekmények fogalmával.

2.2. A szerzői jogi bűncselekmények vonatkozásában

Mivel a Btk. 329/A. §-a a magyar alkotmányos büntetőjog elveinek nem felel meg, az Alkotmány rendelkezéseibe ütközik, azaz erre irányuló alkotmánybírósági normavizsgálat kezdeményezése esetén meg kell semmisíteni. A Cyber-crime Egyezmény ajánlására is figyelemmel a tényállás olyan átfogalmazása szükséges, amely a kereskedelmi mértékű, vagy üzletszerű elkövetést teszi a bűncselekmény alaptényállásának elemévé, de egy alsó elkövetési érték-határ meghatározása is már biztosítaná a tényállás arányosságát.

Be. képviselőkre vonatkozó rendelkezéseit olyképpen szükséges átfogalmazni, hogy abba a közös jogkezelő ipso iure be tudjon illeszkedni, vagy képviselőként, egyértelműen sértetti jogok gyakorlásával ruházná fel e szervezeteket. Ez a megoldás jelentős munkaterhet vonna el a nyomozásban résztvevő hatóságoktól, és azzal párhuzamosan a sértetti érdekek hatékonyabb képviseletéhez is hozzájárulna.

A rendbeliség kérdésében a szellemi alkotások jogának sajátságos felépülése okán, az egymással párhuzamos jogok megsértése miatt megállapítható halmazati kérdések alapjaként a mű és annak felhasználása lenne okszerű. A sértettek számához ragaszkodó elméletek elfogadásával a tényállás hiánytalan, valóságnak megfelelő felderítésének kötelezettsége a hatóságot aránytalan munkateherrel sújtaná, ráadásul a gyakorlatban tapasztalható, sokszor praktikussági megfontolások szerint ad hoc változó halmazati és sértetti szempontok helyett egységes, a jogállami elvárásoknak megfelelő, kiszámítható és következetes joggyakorlatot eredményezne egy mű- és felhasználás-központú elmélet.

A szerzői jogi bűncselekmények felderítése vonatkozásában kiemelt problémakör a szakértők kérdése. Megfontolandó olyan új büntető eljárásjogi intézmények bevezetése, amelyek kellő garanciák mellett a jogalkalmazó munkáját megkönnyítik, így például szükség lenne a szerzői jogi jogosultakat, a jogdíjak, a művek időszakonkénti nyilvántartó és frissítő, a közös jogkezelők által fenntartott adatbázis létrehozására.

2.3. A zaklatással kapcsolatban

A zaklatás bűncselekményének elemzése során kiderült, hogy az angolszász eredetű tényállás nehezen illeszthető be a magánszféra hazai jogvédelmének rendszerébe, mégpedig a védett jogi tárgy nehéz behatárolhatósága és az elkövetési magatartás pontos megfogalmazása miatt. E területen tehát a tényállás nem felel meg minden tekintetben a jogbiztonság követelményeinek, nem hordoz egyértelmű tartalmat arra vonatkozóan, hogy a bűncselekmény mikor követhető el.

Btk. 176/A. § (1) bekezdését illetően helyesebbnek látom a törvényszövegnek oly módon történő átfogalmazását, amely a célzat mellőzésével büntethetővé teszi az eshetőleges szándékkal történő elkövetést is, a magánszféra fogalmának mielőbbi dogmatikai meghatározását, akár értelmező rendelkezésként is. Az információs társadalom oly új életszférákkal gazdagította a személyek magánéletét, amelyek nehezen definiálhatók, azonban ugyanúgy magas szintű jogvédelmet igénylenek.

Megfontolandó emellett a Btk. 176/A. § (2) bekezdés b) pontjába ütköző zaklatás felülvizsgálata és kiegészítése olyképpen, hogy az elkövető cselekménye jelentős érdeksérelmet okoz. Enélkül a cselekmény társadalomra veszélyességének bűncselekményi szintű szabályozást igénylő fokához kétség fér, a tényleges jogsérelem bekövetkezése előtt, pre-pre-előkészületi jellegű magatartásként alacsony szinten húzza meg a felelősségre vonhatóság határát. A tényállást elegendő lenne szabálysértésként szabályozni, lévén, hogy a jogalkotó a tényleges sérelemmel járó bűncselekmények közül sem rendeli büntetni az előkészületet.

2.4. A büntetőeljárással kapcsolatban

A digitális bizonyítékokra vonatkozó szemléletváltás mellett, a szakértői bizonyítás visszaszorítása érdekében megfontolandó a nyomozó hatóság állományában informatikai szaktudással rendelkező bűnügyi technikusok (computer forensic) alkalmazása, akik az egyszerű megítélésű ügyekben az egyes adathordozók, szoftverek vizsgálatára, segédprogramok felkutatására, és vizsgálatuk leírására megbízhatóan képesek. A nyomozások nagy részében elvégzett informatikai vizsgálatok nem tekinthetők olyan különleges szakértelmet igénylő kérdéseknek, amelyeket egy megfelelően kiképezett, a megfelelő eszközökkel ellátott bűnügyi technikus vagy szaktanácsadó jelenlétében a nyomozó hatóság tagja ne tudna megválaszolni, hiszen a bizonyítékok ereje nagy részben a vizsgálathoz igénybevett számítástechnikai eszközök megbízhatóságából ered. E megoldás által a nyomozások idejét nagy valószínűséggel csökkenteni lehetne, emellett nem elhanyagolható pozitív eredményeket érnénk el a bűnügyi költségek csökkentésének célterületén is. Jóllehet a megfelelő szakemberképzés, a szükséges eszközrendszer beszerzése, az esetlegesen felállítandó laboratóriumok létrehozásának költségei magasra rúgnának, azonban ezen alkalmankénti beruházások relatíve hamar megtérülnének, hiszen a szakértők díjára kifizetett összegek sem tekinthetők éppen kevésnek.

SUMMARY

By examining the changes of new living conditions created by information society, my aim was to discover how the change of regulatory environment influenced criminal legislation, law enforcement of proven principals and consistent dogmatics, and what further challenges the constant development of information society sets up for them. The focus was on the tension between the ever-changing information society and the rigid criminal legal system.

It was assumable that the reasons for anomalies are not certainly wrong legislator decisions but the new phenomenon of information society originally offers the possibility for inapplicability of criminal regulating schemes. The qualitatively new form of social cohabitation necessarily resulted in new social relations, values, interests and also new deviances. One of these new deviances, the regulation of IT crimes – due to missing former examples – is often not properly elaborated, the criminal law dogmatics with its set of concepts and principles from before the communicational revolution is not always able to handle certain crimes properly which often leads to the justification of criminal jurisdictional values.

The complete prevailing of the principals of constitutional criminal law can only be guaranteed by speeding up the criminal thinking itself and – being an interdisciplinary field of law – by trying to combine the regulation of IT-related criminal offences and the criminal law principles with the help of the applied concepts of the related fields of science.

In the first part of the dissertation, I am analysing the regulatory environment of criminal offences affected by information technology – e.g. the development and expected vision of information society from technological aspects, and all aspects of these that are important from the aspect of criminal regulation. As part of this analysis, I described the new types of deviances within the information society through examining its incentives and motives. As the discussion about criminal offences of information society is based on/happens on a multiple interdisciplinary field, after reviewing the concerned constitutional standards concerned – in order to enable further specialized analysis – I have done a certain kind of conceptual systematization – also considering the international regulations.

The second part of the dissertation is about the details of regulation of three criminal offences, specifically driven by the aim to discover the anomalies caused by the legislation and the environment that are to be regulated – with regards to a key concept of information society, the convergence that describes the concentration of telecommunications, information technology and content providing services. Based on these, the analysis of regulation of criminal offences related to contents that attack the IT infrastructure (IT feature), use the IT systems as tools (telecommunication feature) or are related to regularly transmitted contents (transmitted content feature) was justified.

FELHASZNÁLT IRODALOM:

HAZAI SZAKIRODALOM:

1. ÁDÁM Antal: Alkotmányi értékek és Alkotmánybíráskodás. Osiris Kiadó Budapest, 1998.
2. ADLER, Freda – MUELLER, Gerhard O. W. – LAUFER, William S.: Kriminológia, Osiris Kiadó Budapest, 2002.
3. BALOGH Gábor: Az információs társadalom olvasatai. In: Balogh Gábor (szerkesztő): Az információs társadalom dimenziói. Gondolat-INFONIA, Budapest 2006.
4. BALOGH Zsolt György: Az infokommunikációs jogról, Infokommunikáció és Jog 2004/2.
5. BALOGH Zsolt György: Az információs alapjogokkal kapcsolatos számítógépes bűncselekmények. in Informatika és büntetőjog (szerkesztette: Gál István László, Nagy Zoltán András), Pécs, 2006.
6. BALOGH Zsolt György: Jogi informatika. Dialog-Campus Kiadó Budapest-Pécs 1998.
7. BELOVICS Ervin - MOLNÁR Gábor - SINKU Pál: Büntetőjog Különös Rész. (ed. Szentpétery Petronella) HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2007.
8. BÉRCZES László - GYENGE Anikó - LENDVAI Zsófia: A szerzői jogi jogsértések esetén alkalmazható jogi eszközökről – Segédanyag a gyakorlat számára. ASVA Budapest. 2005. (Forrás: http://mek.niif.hu/03400/03428/03428.pdf (2010-02-28)
9. BÍRÓ Gyula: Kriminalisztika. Debreceni Egyetem ÁJK. Lícium-ART Könyvkiadó Kft. Debrecen, 2007.
10. BÓCZ Endre (ed.): Kriminalisztika. BM Duna Palota és Kiadó, Budapest, 2004.
11. BÓCZ Endre: Passzív alany, áldozat, sértett. Rendészeti Szemle. 2007/9.
12. BUDAI Balázs: E-közigazgatás axiomatikus megközelítésben, PhD doktori értekezés, 2008.
13. CASTELLS, Manuel: The Information Age: Economy, Society and Culture. Vol. III.: The End of the Millennium, Blackwell, Oxford 1998., A hálózati társadalom kialakulása – Az információ kora. I., Gondolat– Infonia, Budapest, 2005. [1996], Az információ kora: Gazdaság, társadalom és kultúra. II. kötet: Az identitás hatalma, Gondolat–Infonia, Budapest, 2006 [1997].
14. CSUKA Dénes – GASPAREZT András – TARJÁN Gábor – dr. DÓSA Imre: Információbiztonság. in: Takács Tibor (szerkesztő): Az informatikai jog nagy kézikönyve. Complex Kiadó Budapest, 2009.
15. DÖMÖLKI Bálint – KÓSA Zsuzsanna – KÖMLŐDI Ferenc – KRAUTH Péter – RÁTAI Balázs: Égen-földön informatika – Az információs társadalom technológiai távlatai. Typotex. Budapest, 2008.
16. DURKHEIM, Emile: Az öngyilkosság: szociológiai tanulmány. Osiris kiadó, Budapest. 2000.
17. ERDEI Árpád: Tény és jog a szakvéleményben. Közgazdasági és Jogi Könyvkiadó, Budapest, 1987.
18. FARAGÓNÉ HATÓ Katalin: Adatbiztonság, adatvédelem főiskolai jegyzet. Gábor Dénes Főiskola 1999/2000.

19. FARKAS János: Úton az ipari társadalomból az információalapú társadalom felé. in: Balogh Gábor (ed.): Az információs társadalom dimenziói, Gondolat/Infonia, Budapest, 2006.
20. FÖLDI András - HAMZA Gábor (Brósz Róbert és Pólay Elemér): A római jog története és institucióri. Nemzeti Tankönyvkiadó, Budapest, 1996. p. 84-91.
21. GALÁNTAI Zoltán: E-privacy olvasókönyv. Forrás: http://mek.oszk.hu/04100/04134 (2009-09-28)
22. GARAMVÖLGYI Vilmos – VISKI László (ed.): Kriminalisztika. Belügyminisztérium Tanulmányi és Módszertani Osztálya, Budapest, 1961.
23. GÁRDOS-OROSZ Fruzsina: Alapjogok korlátozása. in: Jakab András (szerkesztő): Az Alkotmány kommentárja I. Századvég Kiadó Budapest, 2009. 416-427. oldal.
24. GELÁNYI Anikó: A számítógépes bűnözés szabályozásának összehasonlítása a magyar és a svájci jogban. in Informatika és büntetőjog (ed.: Gál István László, Nagy Zoltán András) Pécs, 2006.
25. GÖNCZÖL Katalin, KEREZSI Klára, KORINEK László, LÉVAY Miklós (ed.): Kriminológia – Szakkriminológia CompLex Kiadó Budapest, 2006.
26. GYÁNYI Sándor: Informatikai WLAN-hálózatok zavarása. Védelmi infokommunikáció
27. GYENGE Anikó: Szerzői jogi korlátozások és a szerzői jog emberi jogi háttere. HVG-ORAC Budapest, 2010.
28. HÜTTL T., Jovanovics E., Szabó M. D. & Vissy B.: Alkotmánybíróságok az adatmegőrzésről – Adalékok az Alkotmánybíróság számára az adatmegőrzési irányelvet átültető magyar szabályok alkotmányossági felülvizsgálatáról szóló eljáráshoz. Infokommunikáció és Jog, 2010. április (37. szám)
29. IBOLYA Tibor: A torrentrazziák büntetőjogi megítélése. Belügyi Szemle 2011/2.
30. ILLÉSI Zsolt: Az igazságügyi informatikai szakértés modellezése. Hadmérnök IV. évfolyam 4. szám (2010. december)
31. JÁVORSZKI Tamás – RONGÁNÉ DR. SRAKTA Ibolya: A szerzői vagy szerzői joghoz kapcsolódó jogok megsértése bűncselekményének jogalkalmazási kérdései. Ügyészek Lapja 2008/5.
32. JÓRI András: Adatvédelmi kézikönyv. Osiris Kiadó, 2005.
33. JUHÁSZ, L., Az Európai Unió információs stratégiája. In: PINTÉR Róbert (ed.), *Információs társadalom.* Gondolat Kiadó, Új Mandátum, 2007.
34. KÁRMÁN Gabriella – NAGY László Tibor – SZABÓ Imre – WINDT Szandra: A szellemitulajdon-jogokat sértő bűncselekmények kutatása. Kriminológiai tanulmányok, 2011. 48. szám.
35. KERTÉSZ Imre: A szakértői bizonyítás. In: Kriminalisztika (szerkesztette: Bócz Endre) BM Duna Palota és Kiadó Budapest, 2004.
36. KINCSEI Attila: Technológia és társadalom az információ korában. In. Balogh Gábor (szerkesztő): Az információs társadalom. Gondolat-Új Mandátum, Budapest 2007.
37. KIRÁLY Tibor: Büntetőeljárási Jog. Osiris Kiadó, Budapest 2008.
38. KOLLÁNYI Bence: Térhasználat az információs társadalomban. In. Pintér Róbert (szerk). Információs társadalom, Gondolat Kiadó, Új Mandátum, 2007.

39. KOPPÁNYI Szabolcs: Hírközlési jog az európai közösségben és Magyarországon. Osiris Kiadó Budapest, 2003.

40. KORINEK Beáta: A stalking és a családon belüli erőszak. in Családi Jog 2005/1.

41. KORINEK Beáta: A stalking. in Korinek László – Kőhalmi László – Herke Csongor (ed.) Emlékkönyv Irk Albert egyetemi tanár születésének 120. évfordulójára. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs

42. KORINEK László: Nemek, szexualitás és bűnözés. forrás: http://www.pecshor.hu/periodika/2007/VIII/korinek.pdf (2008. október 31.) Például: ugyanazt a viccelődést, célozgatást másként élhetik meg a sértettek.

43. LACZI Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és nyomozás felügyeletének speciális kérdései. in Magyar Jog 12/2001.

44. LAKATOS János: A nyomozás – kriminalisztikai szempontból. in: Kriminalisztika (szerkesztette: Bócz Endre) BM Duna Palota és Kiadó Budapest, 2004.

45. LONTAI Endre – FALUDI Gábor – GYERTYÁNFY Péter – VÉKÁS Gusztáv: Magyar polgári jog – Szellemi alkotások joga. Eötvös József Könyvkiadó, Budapest 2008.

46. MAJTÉNYI László: Az információs szabadságjogok. Complex Kiadó, 2006.

47. MASUDA, Yonei: Az információs társadalom, OMIKK, Budapest, 1988.

48. MATUS Márk: Kutatás, lefoglalás, bűnjelkezelés számítástechnikai környezetben. In: Kriminalisztika (Szerkesztette: Bócz Endre) BM Duna Palota és Kiadó, Budapest 2004.

49. MÉSZÁROS Rezső: A kibertér mint új földrajzi tér. In. Kiss, A., Mezősi, G. & Sümeghy, Z. (ed.), Táj, környezet és társadalom: ünnepi tanulmányok Keveiné Bárány Ilona professzor asszony tiszteletére, Szeged: SZTE Éghajlattani és Tájföldrajzi Tanszék – SZTE Természeti Földrajzi és Geoinformatikai Tanszék, 2006.

50. MÉSZÁROS Rezső: A kibertér társadalomföldrajzi megközelítése. In: Balogh Gábor (szerkesztő): Az információs társadalom dimenziói, Gondolat-INFONIA, Budapest 2006.

51. NAGY Zoltán: A számítástechnikai rendszer és adatok elleni új bűncselekmények. Belügyi Szemle 2002/11-12.

52. NAGY Zoltán: A számítógépes környezetben elkövetett bűncselekmények kriminológiai aspektusairól. in. Informatika és büntetőjog (ed.: Gál István László, Nagy Zoltán András) Pécs, 2006.

53. NAGY Zoltán: Konferencia az információtechnikai bűnözésről. Magyar Jog. 1993/2.

54. NOSZKAY Erszébet: Informatikai és rendszerszervezési alapismeretek. Múzsák Kiadó Budapest. 1999.

55. OTT István: A büntetőjogi felelősség önálló elbírálása és a bizonyítási teher kérdésköre a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének egyes eseteiben. Ügyészek Lapja 2008/6.

56. PARTI Katalin – VIRÁG György: A szájbergyerek és a bicikli – A kelet-európai gyerekek nethasználatának specifikumai. Kriminológiai Tanulmányok 2011. 48.

57. PARTI Katalin: Az internetes bűncselekmények nyomozásának egyes kérdései. Kriminológiai tanulmányok, 41. szám. 2004.

58. PARTI Katalin: Devianciák a virtuális valóságban, avagy a virtuális közösségek személyiségformáló ereje. Infokommunikáció és jog 2007/2.

59. PARTI Katalin: Gondolatok a szerver-lefoglalásokról. in. Infokommunikációs és Jog 2004/3.

60. PARTI Katalin: Számítástechnikai devianciák. in: Látens fiatalkori devianciák – Fiatalkori devianciák egy önbevalláson alapuló felmérés tükrében – „ISRD-2". (szerkesztette Kerezsi Klára, Parti Katalin) ELTE Állam- és Jogtudományi Kar Kriminológiai Tanszék és az Országos Kriminológiai Intézet Budapest 2008.

61. PARTI Katalin-VIRÁG György: Beszámoló a Számítógépes bűnözéssel foglalkozó kormányközi munkacsoport (Intergovernmental Expert Group on Cybercrime) üléséről, (Bécs, 2011. január 17-21.) és az ennek kapcsán felmerült kérdésekről.

62. PESZLEG Tibor:A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük. Ügyészek Lapja 2010/2.

63. PINTÉR Róbert: Divatos hívószavak, nagy elméletek, fejlesztési szupernarratívák és metanarratívák – Az információs társadalom jelentésvilága. In: Pintér Róbert (szerk), Információs társadalom. Gondolat Kiadó, Új Mandátum, 2007.

64. PINTÉR Róbert: Úton az információs társadalom megismerése felé. In. Pintér Róbert (szerkesztő): Az információs társadalom – Az elmélettől a politikai gyakorlatig. Gondolat – Új Mandátum, Budapest, 2007.

65. ROMHÁNYI Tamás: A világháló foglyai. Népszabadság, 2004. szeptember 18. http://nol.hu/cikk/333242/ Beszélgetés dr. Vincze Gáborral, a gyulai Pándy Kálmán Kórház pszichiátriai osztályának osztályvezető főorvosával.

66. ROPOLYI László: Internethasználat és hálólét-konstrukció, Információs társadalom: társadalomtudományi folyóirat, 2006. (6. évf.) 4. sz.

67. SIMON Éva: Bevezetés az információs társadalom jogi szabályozásába. In. Pintér Róbert (szerk). Információs társadalom, Gondolat Kiadó, Új Mandátum, 2007.

68. SIMON Zoltán: Érdekérvényesítés a bírói hatalmi ágban: az amicus curiae levelek http://jesz.ajk.elte.hu/simon15.html [2011.07.04.]

69. SUM Szabolcs: A szellemi alkotások jogának információtechnológiai vonatkozásairól. in: Takács Tibor (szerkesztő) Az informatikai jog nagy kézikönyve. Complex Kiadó Budapest, 2009.

70. SZABÓ András: Alkotmány és büntetőjog. Jogtudományi Közlöny 1999/4.

71. SZABÓ András: Jogállami Forradalom és a büntetőjog alkotmányos legitimitása. Belügyi Szemle 1999/10.

72. SZABÓ Máté Dániel: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival. Információs Társadalom: társadalomtudományi folyóirat 2005. (5. évf.) 2. sz.

73. SZABÓ Imre: A számítástechnikai adat mint elektronikus bizonyíték – A magyar szabályozás elemzése az Európai Tanács számítástechnikai bűnözésről szóló egyezménye alapján. in. Kriminológiai tanulmányok. 2011. (48. kötet) 16.

74. SZABÓ Imre: Informatikai bűncselekmények. in: Takács Tibor (szerkesztő) Az informatikai jog nagy kézikönyve. Complex Kiadó Budapest, 2009. 607.

75. Szabó, K., Hámori, B., Információgazdaság – Digitális kapitalizmus vagy új gazdasági rendszer, Akadémiai, Budapest, 2006.

76. SZATHMÁRY Béla: Jogi Informatika. Tanulmányi segédlet a jogi informatika oktatáshoz. Debreceni Egyetem Állam-és Jogtudományi Kar. é. n.

77. SZATHMÁRY Zoltán: A szerzői vagy szerzői joghoz kapcsolódó jogok megsértése nyomozásának jogalkalmazási anomáliái, Magyar Jog, 2010/3.

78. SZATHMÁRY Zoltán: Bűnözés az információs társadalomban. Az információs társadalom devianciái. In. Infokommunikáció és jog 2008/8. (26. szám)

79. SZATHMÁRY Zoltán: Gondolatok a zaklatásról. Magyar Jog

80. SZÉPVÖLGYI Ákos: Az infomációs társadalom térszerkezet alakító hatásai. Doktori (PhD) értekezés, 2007.

81. THUN Éva: A szexuális zaklatás mint társadalmi jelenség. in Belügyi Szemle, 2000. 4-5. szám

82. TÓTH András: Az elektronikus hírközlés és média gazdasági szabályozásának alapjai és versenyjogi vonatkozásai. HVG-ORAC Budapest, 2008.

83. TÓTH Mihály: Gazdasági bűnözés és bűncselekmények. KJK-KERSZÖV, Budapest, 2002.

84. UJVÁRI Ákos: A zaklatásról. In: Ügyvédek Lapja 2009. 2.

85. Ulrich Sieber: A számítógépes bűnözés és más bűncselekmények az információtechnika területén. Magyar jog. 1993/1.

86. VIDA József: A szerzői jog büntetőjogi védelmének néhány gyakorlati kérdése, különös tekintettel a zeneművekre. Ügyészek Lapja 2005/5.

87. VILLÁNYI József: Az Európa Tanács Informatikai bűnözéssel kapcsolatos egyezményéről. Magyar Jog. 2001/8.

88. WIENER A. Imre: Alkotmány és büntetőjog. Állam és Jogtudomány. 1995. (37. évf.) 1-2 szám.

89. Z. KARVALICS László: Információs társadalom – Mi az? Egy kifejezés jelentése, története és fogalomkörnyezete. in: Pintér Róbert (szerkesztő): Információs társadalom. Gondolat Kiadó, Új Mandátum, 2007.

90. ZAKARIÁS Kinga – SZIRBIK Miklós: Az élethez és az emberi méltósághoz való jog. in: Jakab András (szerkesztő): Az Alkotmány kommentárja II. Századvég Kiadó Budapest, 2009.

KÜLFÖLDI SZAKIRODALOM:

1. ADAMS, Jo-Ann M.: Controlling Cyberspace: Apllying the Computer Fraud and Abuse Act to the Internet. In: Computer & High Technology Law Journal [Vol.12. 1996.]
2. ALTMAN, I.: The environment and the social behavior. Monterey, CA: Brooks/cole, 1975.
3. AMICHAI-HAMBURGER, Yair: Personality, individual differences and Internet use. in: The Oxford Handbook of Internet Psychology (edited by: Adam Joinson, Katelyn McKenna, Tom Postmes, Ulf-Dietrich Reips), Oxford University Press, 2007.
4. ARCABASCIO, Catherine: Sexting and Teenagers: OMG R U Going 2 Jail??? in: Richmond Journal of Law & Technology Volume XVI, Issue 3.
5. BARAK, Azy: Phantom emotions – psychological determinants of emotional experiences on the Internet. in: The Oxford Handbook of Internet Psychology (edited by: Adam Joinson, Katelyn McKenna, Tom Postmes, Ulf-Dietrich Reips), Oxford University Press, 2007.
6. BAUMLER, Karla: Sexting: Is it Teenagers Being Teenagers? Or Is It Child Porn? in: Children's Legal Rights Journal Vol. 30. No. 4. 2010.
7. BOCIJ, Paul-MCFARLANE, Leroy: Cyberstalking: the technology oh hate. The Police Journal Vol. 76. (2003.)
8. CASEY, Eoghan: Criminal Behavior on the Internet. in Criminal Profiling – an introduction to behavioral evidence analysis (edited by Brent E. Turvey). Elsenier Inc. 84. Theobald's Road, London 2008.
9. Computer Crimes - American Criminal Law Review [Vol. 45:233 2008.]
10. DIMARCO, Heather: The elektronic cloak: secret sexual deviance in cybersociety. In: Dot.cons - Crime, deviance and identity on the Internet (edited by Yvonne Jewkins) Willan Publishing 2003. Portland, Oregon USA.
11. DOYLE, Charles: Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statue and Related Federal Criminal Laws. Congressional Research Service report for Congress 2010.
12. DURHAM, M. Gigi: The Lolita Effect: The Media Sexualization of Young Girls and What We Can Do About It. (Overlook Hardcover 2008.)
13. FAFINSKI, Stefan: Computer Misuse: the Implications of the Police and Justice Act 2006. The Journal of Criminal Law (2008) 72.
14. GIBSON, W., Neuromancer. Harper Collins, London. 1984.
15. GREEN, Melanie C.: Trust and social interaction on the Internet. in The Oxford Handbook of Internet Psychology (edited by: Adam Joinson, Katelyn McKenna, Tom Postmes, Ulf-Dietrich Reips), Oxford University Press, 2007.
16. IRONS, Alastair-KONSTADOPOULOU, Anastasia: Professionalism in digital forensics. Digital Evidence and electronic signature law review. 2007.
17. JEWKINS, Yvonne – SHARP, Keith: Crime, deviance and the disembodied self: transcending the dangers of corporeality. in. Dot.cons-Crime, deviance and identity on the Internet (edited by Yvonne Jewkins) Willan Publishing 2003. Portland, Oregon USA.

18. JOINSON, Adam N. – PAINE, Carina B.: Self-disclosure, privacy and the Internet. in: The Oxford Handbook of Internet Psychology (edited by: Adam Joinson, Katelyn McKenna, Tom Postmes, Ulf-Dietrich Reips), Oxford University Press, 2007.
19. JONES, Nigel: Training and accreditation – who are the experts? Digital Investigation, 2004. Vol. 1. No. 3.
20. KIFT, Sally – CAMPBELL, Marilyn – BUTLER, Des: Cyberbullying in Social Networking Sites and Blogs: Legal Issues for Young People and Schools. in: Journal of Law, Information and Science (Vol. 20(2) 2009/2010.)
21. LIPKINS, Susan – LEVY, Jaclyn – JERABKOVA, Barbara: Sex Offenders Statistics by a Voice of Reason, Sexting Part II.: Results and Recommendations of Sexting Study 2009. Forrás: http://sexoffender-statistics.blogspot.com/2009/07/sexting-partii-results-and.html
22. LUEHR, Paul H.: Real evidence, virtual crimes – The role of computer forensic experts. Criminal Justice 2005.
23. MCDONALD, Jennifer: Sexting and Excessive Texting: Symptoms of Teen Dating Violence? in: Children's Legal Rights Journal 2010. (Vol. 30. No. 4.).
24. MCKENNA, Katelyn Y. A.: Through The Internet looking glass – Expressing and validating the true self. in: The Oxford Handbook of Internet Psychology (edited by: Adam Joinson, Katelyn McKenna, Tom Postmes, Ulf-Dietrich Reips), Oxford University Press, 2007.
25. MCLAUGHLIN, Julia Halloran: Crime and Punishent: Teen Sexting in Context. in: Penn State Law Review [Vol. 115:1 2010.]
26. MELOY, J. Reid: The Psychology of Stalking. in The Psychology of Stalking Clinical and Forensic Perspectives (edited by J. Reid Meloy), Academic Press London, 1998.
27. MORAHAN-MARTIN, Janet: Internet use and abuse and psychological problems. in: The Oxford Handbook of Internet Psychology (edited by: Adam Joinson, Katelyn McKenna, Tom Postmes, Ulf-Dietrich Reips), Oxford University Press, 2007.
28. National Institute of Justice, DOJ, Computer Crime: Criminal Justice Resorurce Manual 2. (1989.)
29. NEWVILLE, Lanny L.: Cyber Crime and the Courts - Investigating and Supervising the Information Age Offender. Federal Probation [Vol. 65. No. 2], September 2001.
30. NICOL, Bran: Stalking. Reaktion Books Ltd, 2006.
31. PETHERICK, Wayne: Stalking. in Criminal Profiling – an introduction to behavioral evidence analysis (edited by Brent E. Turvey). Elsenier Inc. 84. Theobald's Road, London 2008.
32. PODGOR, Ellen S.: Computer Crimes and the USA PATRIOT Act. Criminal Justice 2002. Summer.
33. RICHARDS, Robert – CLAVERT, Clay: When Sex and Cell Phones Collide: Inside the Prosecutin of a Teen Sexting Case. 32 Hastings Comm. & Ent. L.J. 1, 8. 2009.
34. ROGERS, M. K.: A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory Study. UMI Dissertation Services.

35. SAUNDERS, Rhonda: The Legal Perspective on Stalking. in The Psychology of Stalking Clinical and Forensic Perspectives (edited by J. Reid Meloy), Academic Press London, 1998.

36. SHARP, Keith – EARLE, Sarah: Cyberpunters and cyberwhores: prostitution on the Internet. In: Dot.cons - Crime, deviance and identity on the Internet (edited by Yvonne Jewkins) Willan Publishing 2003. Portland, Oregon USA.

37. SIEBER, Ulrich: Legal Aspects of Computer-Related Crime in the Information Society 1998. Forrás: http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf [2012-02-05]

38. SMITH, Peter, et al: Cyberbullying: Its nature and impact in secondary school pupils. in: Jurnal of Child Psychology and Psychiatry 2008.

39. WEBSTER, F., Theories of the Information Society, Routledge, London – New York, Third edition 2006.

40. WESTIN, Alan: Privacy and Freedom, New York, Atheneum, 1967.

41. WHITTY, Monica T. – JOINSON, Adam N.: Truth, Lies and Trust on the Internet. Routledge, 2009. 27 Madison Avenue, New York USA.

42. WHITTY, Monica T.: Pushing the wrong buttons: Men's and women's attitude towards online and offline infidelity. CyberPsychology and Behavior