4. A kiberbűncselekmények szabályozása

Nagy Zoltán

4.1. Kiberbűncselekmények a jelentősebb nemzetközi jogi dokumentumokban

A számítástechnika gyors fejlődése, a miniatürizálás, a gyártók számának dinamikus növekedése, ezzel a tömegtermelés lehetővé tette a számítógépek széles körű elterjedését, egyben magáncélú felhasználását az 1970-es évek második felétől. Ahogy a számítógépek a konvergencia térhódításával, valamint az 1990-es évektől az internetes alkalmazások egyre szélesebb lehetőséget nyújtottak, úgy a visszaélések fajtái is folyamatosan bővültek. Az új technika-technológia által teremtett új típusú visszaélésekre mint kihívásokra először az anyagi büntetőjogot értékelve kerestek választ. Az informatikai bűncselekmények első megjelenése az Európa Tanács által a tagállamok számára 1981-ben kibocsátott gazdasági bűncselekményekről szóló ajánlásában érhető tetten, ebben példálózva három informatikai bűncselekmény szerepelt csupán. Az OECD 1986-ban kiadott éves jelentésében négyféle e körbe tartozó bűncselekményt említ. Nagy előrelépést jelentett az Európa Tanács 1989-es ajánlása, mivel az ott felsorolt cselekmények lényegi ismérveit meghatározta. Az ajánlásban a kriminalizálni javasolt cselekmények közül nyolc az úgynevezett minimális listán, további négy cselekmény az úgynevezett fakultatív listán szerepel.[1] Ezek közül kiemelhető néhány:

- *Számítógépes csalás:* adatok, programok bevitele, megváltoztatása, törlése, elrejtése vagy más, az elektronikus adatfeldolgozási folyamat befolyásolását eredményező magatartás, amellyel az elkövető egy harmadik személynek gazdasági vagy vagyoni hátrányt okoz, illetve amelynek célja az, hogy az elkövető önmaga vagy más számára gazdasági, illetőleg vagyoni előnyhöz jusson. Az ajánlás alternatív tényállási eleme, hogy az elkövető más személyt vagyonától megfosszon.
- *Számítógépes hamisítás:* adatok, programok bevitele, megváltoztatása, törlése, mentése vagy más, az elektronikus adatfeldolgozási folyamat befolyásolását eredményező beavatkozás, amelynek révén megvalósul a hazai jogban meghatározott hagyományos hamisítás bűncselekménye.
- *A számítógépes adatokban és programokban történő károkozás:* az adatok és/vagy programok jogosulatlan törlése, rongálása, károsítása, mentése.

[1] Council of Europe (1989): *Computer-related crime, Recommendation No R (89) 9 on Computer-related Crime and final report of the European Committee on Crime Problems.* Elérhető: www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf (A letöltés dátuma: 2019. 06. 01.)

https://doi.org/10.36250/00782_04

- *Számítógépes szabotázs:* olyan adatok és/vagy programok bevitele, megváltoztatása, törlése vagy a számítógépes rendszerek más befolyásolása, amely célja, hogy annak telekommunikációs funkcióját akadályozza.
- *Jogellenes behatolás:* a számítógépes rendszerbe vagy hálózatba történő jogosulatlan bejutás a biztonsági intézkedések megsértése révén.
- *Jogellenes titokszerzés.*
- *Védett számítógépes programok jogellenes másolása.*
- *Félvezető topográfiák jogellenes másolása.*

Az ajánlás tartalmazott egy rövid fakultatív listát is, mint az adat- vagy programváltoztatás, kémkedés, számítógép jogellenes és kárt okozó használata, védett számítógépes programok jogellenes használata.

A büntetőjogot érintő kihívások nemcsak a büntető anyagi jogot, hanem a büntető eljárásjogot is szükségképpen érintette, és jelenleg is érinti. Az Európa Tanács 1995-ben adott ki egy újabb ajánlást, amely az információs technológiával kapcsolatos büntető eljárásjogi problémákat gyűjtötte egybe.[2] Az Európa Tanács ajánlása az alábbi kérdésekkel foglalkozott:

- A kutatás, lefoglalás jogszabályi feltételeinek megteremtése, ideértve a jogorvoslati lehetőséget is.
- A telekommunikációs vállalatok technikai őrizetre történő kötelezése jogi szabályainak kialakítása.
- Együttműködési kötelezettség a nyomozó hatóság és a nyomozással érintett szervek között.
- Az elektronikus bizonyítékok integritásának, eredetiségének biztosítása a nyomozás során és a nemzetközi együttműködés során. Az elektronikus bizonyítékok ugyanúgy kezelendők, mint a többi tárgyi bizonyíték.
- Titkosítás használata.
- Tudományos kutatás, képzés, statisztikák fontossága.

Hosszas előkészületek után 2001-ben írták alá a *Számítógépes bűnözés elleni nemzetközi egyezményt* Budapesten. Gyakran nevezik ezt a nemzetközi okmányt *budapesti egyezménynek* is. Az egyezményt Magyarország törvénnyel jogforrásai közé emelte.[3] Az Európa Tanács korábbi két ajánlása után – az ET 9. (89) sz. és ET 13. (95) sz. – a 2001-es *Számítástechnikai bűnözésről szóló egyezmény (Convention on Cyber-crime)* újabb mérföldkövet jelentett, mivel

- lépést tartott az elektronikus adatfeldolgozás és -átvitel technológiai fejlődésével folyamatosan megjelenő újabb visszaélések meghatározásával, így a hálózatokon megjelenő tartalomközlésekben megnyilvánuló cselekmények javasolt kriminalizálásával,

[2] Council of Europe, Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology. Elérhető: https://rm.coe.int/16804f6e76 (A letöltés dátuma: 2019. 06. 01.)

[3] 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről.

- a számítógépes bűnözéssel összefüggő anyagi, eljárásjogi és nemzetközi büntetőjogi problémákat komplexen kezeli,
- a számítógépes környezetben felmerülő (jogi és technikai) fogalmakat definiálja, azaz egységes értelmezést nyújt azokról.

Az egyezmény a bűncselekményeket – az ET 9. (89) sz. ajánlását alapul véve – immár dogmatikailag letisztultan csoportosítja:

1. *A számítástechnikai rendszer és a számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények:*
   - jogosulatlan belépés,
   - jogosulatlan kifürkészés,
   - számítástechnikai adat megsértése,
   - számítástechnikai rendszer megsértése,
   - eszközökkel való visszaélés.
2. *Számítógéppel kapcsolatos bűncselekmények:*
   - számítógéppel kapcsolatos hamisítás,
   - számítógéppel kapcsolatos csalás.
3. *Számítástechnikai adatok tartalmával kapcsolatos bűncselekmények:*
   - gyermekpornográfiával kapcsolatos bűncselekmények.
4. *Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények.*

Az 1. pontban említett cselekmények értelmezésére az Európai Tanács 2013/40-es direktíváját idézzük lentebb. A 3. pont később kiegészült egy 2002-ben született, de 2006. március 1-től hatályos jegyzőkönyvvel az informatikai környezetben elkövethető rasszista és idegengyűlölő cselekményekről.[4] Az egyezmény továbbá a büntetőeljárás során keletkezett jogi polémiák megoldására törekedett. Az egyezmény büntető eljárásjogra vonatkozó rendelkezései:

- tárolt számítástechnikai adat gyors megőrzése (tárolt számítástechnikai adat gyors megőrzése, forgalmi adat gyors megőrzése és részbeni átadása);
- közlésre kötelezés;
- tárolt számítástechnikai adat átvizsgálása és lefoglalása;
- számítástechnikai adatok valós idejű összegyűjtése (forgalmi adatok valós idejű összegyűjtése, tartalomra vonatkozó adatok kifürkészése).

Az egyezmény nemzetközi büntetőjogi tárgyú rendelkezései:

- jogsegélykérelemmel kapcsolatos eljárás hatályos nemzetközi megállapodás esetében, általános alapelvek,
- jogsegélykérelemmel kapcsolatos eljárás hatályos nemzetközi megállapodások hiányában, általános alapelvek,
- ideiglenes intézkedéssel kapcsolatos jogsegély,
- tárolt számítástechnikai adat gyors megőrzése,
- megőrzött forgalmi adat gyors átadása,

[4] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189).

- nyomozati jogkörökkel kapcsolatos jogsegély,
- tárolt számítástechnikai adathoz való hozzáférésre vonatkozó jogsegély,
- tárolt számítástechnikai adathoz való hozzáférés határokra tekintet nélkül, hozzájárulás vagy nyilvános elérhetőség esetén,
- forgalmi adat valós idejű összegyűjtésével kapcsolatos jogsegély,
- tartalomra vonatkozó adat kifürkészésére vonatkozó jogsegély,
- a 24/7 hálózat (kapcsolattartás) megteremtése.

Az Európai Parlament és a Tanács 2001/29/EK irányelve egyetlen bűncselekménytípust érint: az információs társadalomban a szerzői és szomszédos jogok egyes vonatkozásainak összehangolására tett ösztönző lépéseket. Ugyanis a modern technológiák fejlődésével a szerzői jogot érő kihívásokra a tagállamok különböző módon reagáltak. A direktíva javaslatot tesz a tagállamok szerzői jogi rendelkezéseinek közelítésére. *In concreto* egyik fontos megállapítása kiemelést érdemel, ami szerint különbséget kell tenni az analóg és a digitális másolás között, és eltérő szabályokat lenne érdemes alkotni (38. pont).

Az *Európai Tanács 2001/413/IB kerethatározata* ugyancsak egy bűncselekményi körre vonatkozó rendelkezéseket tartalmazott. A nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelem kapcsán arra hívja fel a figyelmet, hogy a készpénzhelyettesítő fizetőeszközök hamisítása számítástechnikai eszközökhöz kötött.

Az Európai Tanács 2004/97/EK határozatával[5] létrehozta az Európai Hálózat- és Információbiztonsági Ügynökséget (ENISA). A szervezet határozatban rögzített célja az, hogy az Európai Unió (EU), az EU-tagállamok és az üzleti szféra fokozottabb mértékben legyen képes a hálózat- és információbiztonsággal kapcsolatos problémák megelőzésére, kezelésére és az azokra történő reagálásra. Ennek érdekén a szervezet iránymutatásokat ad ki, tájékoztatókat, és gyakorlatokat tart. Éves jelentéseiben gyűjti össze az informatikai biztonságot érintő, az európai országokban felmerült problémákat és a megoldásukra tett javaslatot.

Az *Európai Tanács* 2009 decemberében fogadta el az úgynevezett *stockholmi programot,* amely a 2010–2014 közötti időszakra az Európai Unióban a jog, a szabadság, a biztonság szem előtt tartásával, annak érvényesülő követelményével összefüggő feladatokat határozta meg. A cselekvési program az alábbi határokat átlépő bűncselekmények, közöttük az informatikai bűncselekmények üldözésének fontosságát hangsúlyozza fő irányként:

- emberkereskedelem,
- szexuális zaklatás, gyermekek szexuális kizsákmányolása, gyermekpornográfia,
- *informatikai bűnözés,*
- gazdasági bűnözés, így a korrupció, hamisítás és kalózkodás, valamint
- a kábítószerrel összefüggő bűnözés.

A stockholmi program alapján került kibocsátásra a *2011/92/EU irányelv*, amely leszögezte, hogy a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelem egyaránt ki kell, hogy terjedjen a valós és a virtuális térre. A direktíva a tagországokat szigorú szankciók alkalmazására ösztönzi.

Ugyancsak a stockholmi program továbbvitelét jelenti a *2013/40/EU irányelv* az információs rendszerek elleni támadásokról. Az irányelv kibocsátásának célja az informa-

[5] Módosította: az 526/2013/EU rendelet.

tikai bűncselekmények tényállásaira és szankcióira vonatkozó minimumszabályokra tett javaslatok megtétele. A közös szabályrendszer ezáltal közelítse a tagállamok büntetőjogát; ezzel tegye hatékonyabbá a bűnügyi jogsegélyt, valamint a tagállamok nyomozó hatóságai, az Europol, az Eurojust[6] és az ENISA közötti együttműködés. A direktívában meghatározott minimum-bűncselekmények köre és azok tartalmi lényege a következő:

- *Információs rendszerekhez való jogellenes hozzáférés:* valamely információs rendszerhez vagy annak egy részéhez való, szándékosan és jogosulatlanul történő hozzáférés legalább a súlyosabb esetekben bűncselekménynek minősüljön akkor, ha a bűncselekményt valamely biztonsági intézkedés megsértésével követték el.
- *Rendszert érintő jogellenes beavatkozás esetében:* a számítógépes adatok szándékos és jogosulatlan bevitele, továbbítása, megrongálása, törlése, minőségi rontása, megváltoztatása vagy elrejtése, ilyen adatok szándékos és jogosulatlan hozzáférhetetlenné tétele révén történő súlyos akadályozása vagy megszakítása legalább a súlyosabb esetekben bűncselekménynek minősüljön.
- *Adatot érintő jogellenes beavatkozás esetében:* az információs rendszer számítógépes adatainak szándékos és jogosulatlan törlése, megrongálása, minőségi rontása, megváltoztatása vagy elrejtése, illetve az ilyen adatok szándékos és jogosulatlan hozzáférhetetlenné tétele legalább a súlyosabb esetekben bűncselekménynek minősüljön.
- *Jogellenes adatszerzés esetében:* az információs rendszeren belülre, kívülre vagy azon belül továbbított, nem nyilvános számítógépes adatok – többek között az információs rendszerekből érkező, ilyen adatokat hordozó elektromágneses sugárzás – technikai eszközökkel történő szándékos és jogosulatlan megszerzése legalább a súlyosabb esetekben bűncselekménynek minősüljön.
- *A bűncselekmények elkövetéséhez használt eszközök esetében:* meghatározott eszközök jogosulatlan és bármely fenti bűncselekmény elkövetéséhez való felhasználásának szándékával való előállítása, árusítása, használatra történő beszerzése, behozatala, forgalomba hozatala vagy egyéb módon történő hozzáférhetővé tétele legalább a súlyosabb esetekben bűncselekménynek minősüljön (olyan számítógépes programok, amelyek elsősorban a fentebb említett bármely bűncselekmény elkövetésére készültek vagy lettek átalakítva, olyan számítógépes jelszavak, belépési kódok vagy hasonló adatok, amelyekkel egy információs rendszerhez vagy annak egy részéhez hozzá lehet férni).
- Felbujtás, bűnsegély és kísérlet kérdésköre.
- Szankciók.

Mind a joggyakorlat, mind az oktatás-kutatás számára alapul szolgálnak – egyéb források mellett – az *Europol IOCTA-jelentései*[7] (magyarul: *Helyzetjelentés a számítógépes bűnözésről, a megismert fenyegetésekről, a várható tendenciákról*). A 2014 óta évente megjelenő kiadványok (megjelenésük alapján elnevezve *Fehér Könyvekben,* amelyek az interneten is szabadon elérhetők) összegezik az adott időszakban feltűnt fenyegetéseket, az újabb s újabb

[6] Az Eurojustot a Tanács 2002/187/IB határozata hozta létre.

[7] Internet Organised Crime Threat Assessment, avagy *az interneten zajló szervezett bűnözéssel kapcsolatos fenyegetésértékelés.*

visszaéléseket, a szakemberek, a tagállamok tapasztalatait, szakértőik és mások tudományosan megalapozott kutatásainak eredményeit.

4.2. A kiberbűncselekmények hazai szabályozása

Az első informatikai bűncselekmény 1994-ben tűnt fel a magyar Büntető Törvénykönyvben. A bűncselekmény elnevezése *számítógépes csalás* volt, de a tényállás alkalmazható volt valamennyi elektronikus adat vagy program elleni cselekményre, tehát például egy malware-támadás esetére is, így a tényállás tartalma túlnőtt a bűncselekmény elnevezésén. A tényállás 1996-ban a mobiltelefon és a közcélú mobiltelefon kártyája manipulálásának büntetendőségével bővült. A 2001-es módosítás megtartotta a bűncselekmény elnevezését. A tényállás struktúrája követte a „hagyományos" csalás szerkezetét azzal, hogy a megtévesztés az adat- vagy programmanipuláció volt, és a kár fogalmának a tényállásba épülésével a minősített esetek köre is a kár nagyságához igazodóan bővült. A 2012. évi C. törvény alapján három informatikai bűncselekmény tényállását tekintjük át.

4.2.1. Információs rendszer vagy adat megsértése

„423. § (1) Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Aki

a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy

b) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz,

bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(3) A büntetés bűntett miatt egy évtől öt évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény jelentős számú információs rendszert érint.

(4) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el.

(5) E § alkalmazásában adat: információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja."

A *bűncselekmény jogi tárgya* (a jog által védett érték) az informatikai rendszerek biztonságos működése, a *b)* pont esetében a jogi tárgy kiegészül az elektronikus adatok megbízhatóságához, hitelességéhez fűződő érdekkel.

4.2.1.1. A bűncselekmény elkövetési (tevékenységi) tárgyai

- Egyetlen számítógép vagy informatikai rendszer és
- számítógépes programok, elektronikus adatok mint elektronikus impulzusok.

Egyetlen számítógép esetében közömbös, hogy notebookról, laptopról, iPhone-ról, iPodról, iPadről, tabletről vagy okostelevízióról van-e szó. Az egyszerűség okán ezekre a továbbiakban csak a számítógép kifejezést használjuk. Az informatikai rendszer számítógépek összekapcsolódása révén létrejövő hálózat.

4.2.1.2. A bűncselekmény elkövetési (tevékenységi) magatartásai

Az (1) bekezdés *a)* pontjában szabályozott két eset:
- jogosulatlan belépés informatikai rendszerbe,
- a belépési jogosultság kereteit túllépve vagy azt megsértve a rendszerben maradás.

A jogosulatlan belépés történhet:
- egy más által jogszerűen használt számítógépbe, a jogosult használó színlelésével vagy
- számítógépen keresztül egy védett hálózatba.

A jogosulatlan belépés *akkor tényállásszerű,* ha
- a rendszer biztonsági megoldásokkal védett, és
- a védelem aktív, azaz szükséges legyen a belépéshez jelszavak, kódok, más azonosítók használata a hálózat eléréséhez. Ezek konjunktív feltételek.

Az elkövető aktív védelemmel ellátott számítógépbe vagy hálózatba *jogosulatlanul lép be,* ha
- a számítógép vagy hálózat biztonsági rendszerbeli hiányosságai kihasználásával lép be jogosulatlanul, vagy
- a jogosult felhasználó nevével (belépési kódjával), jelszavával vagy a belépést biztosító adat birtokában,
- kódfeltörő program segítségével vagy más módon teszi ezt.

Az itt olvasható (1) bekezdés esetében közömbös a kódok, jelszavak megszerzésének módja, azaz hogy megtévesztéssel, más csalárd módon, kifürkészéssel, a felhasználó hanyagsága folytán, a felhasználó ellen erőszak, fenyegetés alkalmazásával szerzi-e meg a jelszót. Az erőszakkal, fenyegetéssel történő belépési azonosító megszerzése, de fel nem használása kényszerítés bűncselekményének (Btk. 195. §) minősül. A kényszerítés útján szerzett belépési azonosítóval történő belépés esetén valódi, anyagi, heterogén halmazat jön létre. A megtévesztéssel történő belépési azonosító megszerzésének a módja az úgynevezett social engineering. A védett wifihálózatba történő jogosulatlan belépés – a kissé ijesztőnek tűnő – *war driving* elnevezéssel ismert a szakirodalomban. Büntethetőséget megszüntető ok, ha az informatikai rendszer nem védett, illetve a védelem nem aktivált. *A belépési jogosultsága kereteinek túllépésével, illetőleg annak megsértésével történő bennmaradás* esetében a belépés jogszerűen történt, az elkövető saját vagy rábízott felhasználói névvel,

jelszóval, a legális belépési ponton lép be az információs rendszerbe, ám a felhasználói jogosultságát meghaladó műveleteket kíván folytatni. Például a felhasználó jogszerűen veszi igénybe a kereskedelmi bankok telebanking szolgáltatását, de olyan műveleteket kíván végrehajtani, amelyre a bankkal kötött szerződés alapján nincs jogosultsága, például egy másik ügyfél bankszámláját, annak forgalmát kívánja megtekinteni. Továbbá, ha a rendszergazda, aki jogosult rendszerébe belépni, jogellenesen az intézmény, vállalkozás felhasználóinak adatait, forgalmát gyűjti ki, ha ez utóbbi nem valósít meg személyes adattal visszaélést (Btk. 219. §), kémkedést (Btk. 261. §), minősített adattal visszaélést (Btk. 265. §), esetleg más bűncselekményt. Megjegyezni kívánjuk, hogy a jogosulatlan belépést, „elektronikus betörést" *hackingnek* (hacker által végzett tevékenységnek) nevezik. A *hacker* és a *bűnöző* nem szinonim fogalmak. Ma már a rendőrségi nyomozáshoz, katonai műveletek folytatásához elengedhetetlenül szükség van egy szakmailag felkészült és elnevezésében „jó" hackerre, úgynevezett *white hat hackerre.* A *jó hackerek* tevékenysége nélkülözhetetlen, az ő tudásuk, ismereteik védhetik meg az állam, az intézmények, vállalkozások számítástechnikai rendszereit a *rossz hackerek* támadásaitól. Egyes országokban jó hackerekből álló önkéntes csoportokat is szerveztek. A *jó hacking* egyik legismertebb esete az űrben baleset szenvedett Apollo–13 űrhajósai életének megmentése volt 1970-ben, további példák a Hubble-teleszkóp, a Pioneer–10 működésének megmentése.

Az (1) bekezdés *b)* pontjában szabályozott esetben az elkövető az informatikai rendszer működését jogosulatlanul vagy jogosultsága kereteit túllépve *akadályozza.* Tipikus esete az úgynevezett malware-támadás indítása. A *malware* szó a *malicious software* szavak összevonásából keletkezett. Felöleli a legkülönbözőbb kártékony programokat: vírus, logikai bomba, féreg, trójai vírus, rootkit. A *spyware-ek* (kémprogamok) és *ransomware-ek* (zsarolóvírusok) ehelyütt nem vonhatók ide. A malware-ek hatása is sokféle lehet, az informatikai rendszer működését azzal akadályozhatják, hogy például lassítják, leállítják a számítógépet, felülírhatják a tárolt vagy továbbított adatainkat, módosíthatják a programokat. A malware-rel fertőzés különböző módjai sajátos bűnösségi eseteket vetnek fel: offline feltöltés esetében a malware számítógépre telepítése bármely adathordozóról történhet. A malware-program önállóan vagy más programba (például egy játékprogramba) rejtve is telepíthető.

A feltöltőnek közvetlen fizikai kontaktusba kell kerülni a célzott számítógéppel. Ez történhet:

i) a helyiségbe történő jogellenes behatolással,
ii) a számítógépet meghackelve (elektronikus betörés révén),
iii) jogszerűen hozzáférve a számítógéphez.

Az i) pont esetében a magánlaksértés (Btk. 221. §) is szóba jöhet. Hivatali helyiségbe történő jogosulatlan bemenetel esetében a bejutáshoz szükséges rongálás (Btk. 371. §) is szóba jöhet. Ezekben az esetekben a valódi, anyagi, heterogén halmazat állapítható meg. Az ii) pontban írt eset a bűncselekmény (1) bekezdés *a)* pontját is kimeríti. Az azonos jogi tárgy a halmazati értékelést kizárja. Az iii) pont esetében az (1) bekezdés *b)* pont alkalmazható, mivel az akadályozás a jogosultság kereteit túllépő tevékenység. Ezzel szemben a számítógépes hálózaton terjesztett (megosztott) malware-ek esetében, azaz online feltöltés esetében nem szükséges közvetlen fizikai hozzáférés a számítógéphez:

- a célzott szervert meghackelve történhet a malware telepítése,
- célzott számítógép hiányában is az informatikai hálózaton keresztül, például illegális warezoldalakra, *peer to peer (P2P-)* kapcsolat révén torrent- vagy más hálózatra telepítve, különböző alkalmazásokba rejtve, e-mailben, VOIP-hez csatolt fájlban.

A célzott számítógép hiányában történő feltöltés jellemzője, hogy a sértettek száma előre nem látható (attól függ, hogy hányan töltik le és telepítik azokat). Az informatikai rendszer akadályozásának másik tipikus esete a program manipulálása, megváltoztatása, valamely elemének egészben történő átírása vagy annak részleges vagy teljes törlése, továbbá ezek kombinációja. Valamint idetartozik minden olyan utasítás felvitele is, amelynek révén meg nem engedett műveletek végezhetők, amelyekkel az informatikai rendszert akadályozni lehet (szabotálni). A sértetti közrehatás sajnos ebben az esetben is valós problémát jelent, főként, ha

- a felhasználó kétes helyről (például warez-, szexoldalról, P2P-hálózatról) tölt le, telepít egy fertőzött programot,
- ellenben nem telepít számítógépére malware-t felismerő és azt törlő programokat,
- illetve nem frissíti a számítógépén dolgozó programokat.

Óvatosan ugyan, de felvethető a felhasználó felelőssége, hogy megtesz-e mindent számítógépe védelmében? A kérdés komolysága abban áll, hogy nem vagy nem megfelelően védett számítógépe nagyon súlyos bűncselekmények (terheléses támadás, spamek milliós megosztása stb.) „résztvevője" lehet. Felelőtlen magatartása kárt okoz intézményének, szervezetének, saját magának, esetleg szolgáltatójának stb.

4.2.1.3. A bűncselekmény minősített esetei

Súlyosabban büntetendő, ha a kárt okozó támadás jelentős számú információs rendszert érint – akár a felhasználók mint sértettek nagy számában, akár úgy, hogy a felhasználók tudtukon és akaratukon kívüli aktív részesei egy jogsértésnek (például DoS vagy DDoS). A számítógép erőforrásai meggyengülhetnek (például a weboldal lassabban töltődik be, az audio- és videostreamek megszakadhatnak, az e-mail-küldés akadozik stb.). Bár ennek valójában a hálózat- vagy a weboldal szolgáltatójánál keletkezett probléma is oka lehet. Az egyre nagyobb sávszélesség (az adatátvitel gyorsabbá válása) miatt egyre kevésbé érzékelhető az, ha terheléses támadás részese a felhasználó.

A terheléses támadás célpontjai jellemzően nem az egyéni felhasználók számítógépei, hanem azok az informatikai rendszerek, amelyek vagy különösen védett rendszerek (kritikus infrastruktúra, honvédelem, pénzügyi szféra stb.), vagy azok az informatikai rendszerek, amelyeknek 24 órás működése szükségszerű (például energetikai vagy online-szerencsejáték-szerverek). A terheléses támadással történő zsarolás (Btk. 367. §) mint modern „védelmipénz-behajtás" már ismert a szakirodalomban.

Még súlyosabban bünteti a törvény azt az esetet, ha a támadás közérdekű üzem ellen irányul. A közérdekű üzem fogalmát a Btk. 459. § 21. pontja tartalmazza, ami szerint:

a) a közmű,
b) a közösségi közlekedési üzem,

c) az elektronikus hírközlő hálózat,
d) az egyetemes postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központok és üzemek,
e) a hadianyagot, haditechnikai eszközt, energiát vagy üzemi felhasználásra szánt alapanyagot termelő üzem.

4.2.1.4. Büntetéskiszabási szempontok

Büntetéskiszabási szempontok között súlyosbítóként jöhet szóba az információs rendszer működéséért felelős személyek és számítástechnikai szakemberek büntetni rendelt ténykedései, hiszen ők szakmai ismeretük felhasználásával követték el a bűncselekményt.

4.2.2. Az információs rendszer védelmét biztosító technikai intézkedés kijátszása

„424. § (1) Aki a 375. vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő

a) jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez vagy forgalomba hoz, illetve

b) jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Nem büntethető az (1) bekezdés *a)* pontjában meghatározott bűncselekmény elkövetője, ha – mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő jelszó vagy számítástechnikai program készítése a büntetőügyekben eljáró hatóság tudomására jutott volna – tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.

(3) E § alkalmazásában jelszó: az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy ezek kombinációjából álló bármely azonosító."

A törvényi szabályozás szerint a 375. és a 423. szakaszokban szabályozott bűncselekmények elkövetése céljából büntetni rendeltek a technikai megoldások kijátszásához szükséges vagy azt könnyítő cselekmények.

A bűncselekmény *jogi tárgya* – a fentebb említett jogi tárgyaknak megfelelően – az elektronikus adatfeldolgozás és -átvitel integritása, biztonsága, amely magában foglalja a számítástechnikai rendszert és annak működését, valamint a feldolgozásra rendelt adatok mint elektronikus impulzusok biztonságát.

1. A bűncselekmény *elkövetési (tevékenységi) tárgya* az elektronikus adatfeldolgozó és adatátviteli rendszer védelmi-biztonsági megoldásainak kijátszására alkalmas program, belépési kód, jelszó vagy egyéb adat, amely a védett rendszerbe történő jogszerű belépést biztosítja [424. § (1) bekezdés *a)* pont].

- *Belépési kód:* a felhasználónév, amely a hozzárendelt jelszóval együtt teszi lehetővé a jogosult számára a belépést valamely hálózatba, számítógépbe.

- *Jelszó:* hálózat (internet, intra- és extranet), valamint adatállomány hozzáféréséhez szükséges azonosító kulcsszó. Általában jelszavak védik a BIOS-t, különböző operációs rendszerekben például a megosztott erőforrásokat, a szövegszerkesztő programokban a dokumentumokat.

A különböző hálózatok használatához alkalmaznak jelszavakat. Az operációs rendszereket, a levelezőprogramokat vagy más programokat, a védett könyvtárakat és fájlokat is különböző azonosítók, jelszavak védik, védhetik.[8] A bűncselekmény elkövetési (tevékenységi) magatartásai közé tartozik az (1) bekezdés *a)* pontjában írott büntetni rendelt tevékenység: valamely védett informatikai rendszerbe jogosulatlan belépést biztosító program, jelszó, belépési kód vagy adat, illetve más számítógépes program, amely az informatikai csaláshoz vagy az informatikai rendszer, az abban kezelt adatok ellen irányul.

- *Készítés:* számítógépes program írása, az adott infromatikai rendszer védelmére szolgáló jelszó generálása, a jelszó felülírása stb. A szerzői jogi törvény 58. § (2) bekezdése miniszteri indokolását alapul véve, a szoftver bármely elemének (forráskód, tárgyi program, kísérő anyag) készítése e szakasz alá vonható. De az *interface* (hardver-szoftver közti összeköttetést létrehozó utasítássorozat) készítése már kívül esik e körön.
- *Átadás:* az adott számítástechnikai rendszer vonatkozásában a program készítőjétől stb. különböző személynek a birtokba adása. Közömbös, hogy ez ingyenesen, visszterhesen, megtévesztéssel vagy más módon történt.
- *Hozzáférhetővé tétel:* a program, jelszó, adat eljuttatása egyéb módon, akár aktív, akár passzív magatartással (például többek által használt helyiségben, irodában, gépteremben a belépési kód, jelszó stb. asztalon, képernyőre ragasztott papírdarabon történő otthagyása).

Tipikus lehet például a warezoldalon történő közzététel, a P2P-hálózaton, chatszobában, fórumrovatban, elektronikus hirdetőtáblán való megosztás stb. Közömbös, hogy ingyenesen vagy ellenszolgáltatás fejében történik. Ne feledjük, hogy az ingyenes sem ingyenes, igen nagy valószínűséggel ezekben a programokban egy másik kártékony program is rejtőzik.

- *Megszerzés:* a jelszó, program birtokbavétele a program írójától, más személytől, letöltése az internetről. Közömbös, hogy ellenszolgáltatás fejében, megtévesztéssel vagy más módon. A megszerzés módja legfeljebb büntetéskiszabási szempontként értékelhető.
- *Forgalomba hozatal:* több, akár meg nem határozható számú személy számára hozzáférhetővé teszi e programot akár úgy, hogy saját maga juttatja el a felhasználóknak, akár úgy, hogy egyetlen személynek adja át, ám abban a tudatban, hogy az a személy több személynek adja tovább. Irreleváns, hogy ez ellenszolgáltatás fejében történt-e, vagy sem.

2. A (1) bekezdés *b)* pontja szerint büntetendő cselekmény, egyfajta *delictum sui generis* bűnsegédi tevékenység büntetni rendelt. A tényállás megfogalmazásában mindkét

[8] A tényállás másik fordulatának elkövetési (tevékenységi) tárgyai a fentebb részletezett malware-vírusok, lásd 424. § (1) bekezdés *b)* pont.

bűnsegélyi alakzat (fizikai és pszichikai bűnsegély) szerepel: 1. a számítástechnikai program, jelszó, belépési kód vagy valamely számítástechnikai rendszerbe való belépést lehetővé tevő adat készítésére vonatkozó gazdasági, műszaki, szervezési ismeret átadása másnak; 2. kódfeltörő program írásához, jelszógeneráláshoz, ezek megszerzéshez, forgalomba hozásához szükséges elméleti vagy gyakorlati ismereteket, programrészleteket másnak továbbad, kapcsolatrendszert megoszt. Nem tartozik ide a programok megnevezése, a program működésének, hatásmechanizmusának leírása.

A bűncselekmény elkövetője mindkét esetben bárki lehet. Közömbös a szakismeret, a tudás szintje. Büntetéskiszabási szempont lehet, és súlyosító körülményként jöhet szóba az, ha a vádlott számítástechnikai képesítéssel bír, vagy ilyen munkakörben dolgozik, számítástechnikai cég, szerviz dolgozója stb. Az elkövetési (tevékenységi) magatartások célzatosak, azaz a Btk. 375. §-a, illetőleg a Btk. 423. §-a végrehajtása céljából történik, így a bűnösség az egyenes szándékra *(dolus directus)* korlátozódik.

3. A (2) bekezdés szerint nem büntethető az, aki program-, jelszó-, adatkészítő tevékenységét a hatóság előtt felfedi, és az elkészített dolgot a hatóságnak átadja, valamint lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását. A büntethetőséget megszüntető ok akkor jöhet szóba, ha a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő számítástechnikai programot, jelszót, belépési kódot vagy valamely számítástechnikai rendszer egészébe vagy egy részébe való belépést lehetővé tevő adatot az elkövető azelőtt hozza a hatóság tudomására, vagy adja át a hatóságnak stb., mielőtt a hatóságnak erről ismerete lett volna.

Az (1) bekezdésben megfogalmazott bűncselekmény az elkövetési magatartás tanúsításával (program írása, belépési kód, jelszó generálása, ennek megszerzése, forgalomba hozatala, kereskedés, hozzáférhetővé tétel) befejezett, nem szükséges, hogy a 375. §, illetőleg a 423. § bármelyike is akár csak kísérleti szakaszba jusson. A (2) bekezdés esetében a gazdasági, műszaki, szervezési ismeretek másnak történő rendelkezésre bocsátásával a bűncselekmény befejezetté válik. Nem szükséges, hogy ez a személy ezeket programok írására, belépési kódok, jelszavak generálására felhasználja. A bűncselekmény rendbelisége a veszélyeztetett elektronikus adatfeldolgozó- és átviteli rendszerek számához igazodik. *De ege ferenda:* mivel az informatikai rendszerbe történő bejutást követően többféle bűncselekmény követhető el – a jogosulatlan adatszerzéstől a *defacingen* keresztül a tiltott tartalom feltöltésének lehetőségéig –, így nincs indoka annak, hogy a Btk. 424. §-a csupán a 375. § és a 423. § megvalósításához kapcsolódik. A harmadik tényállás *az információs rendszer felhasználásával elkövetett csalás.* A tényállás megalkotása azt a szakmai vitát zárta le, hogy a sértetti kontroll nélküli megtévesztő adatbevitel, adatmanipuláció – amely kárt okoz a sértettnek – lehet-e csalás. Ezt a vitát zárta le először a 89/9. európai tanácsi ajánlásban megfogalmazottakkal szinte azonos módon, ennek ellenére egy évtizeden át tévesen közelítette meg a kérdést a hazai törvénykezés. A mostani tényállás dogmatikailag már sokkal helyesebb.

4.2.3. Információs rendszer felhasználásával elkövetett csalás

„375. §. (1) Aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés egy évtől öt évig terjedő szabadságvesztés, ha

a) az információs rendszer felhasználásával elkövetett csalás jelentős kárt okoz, vagy

b) a nagyobb kárt okozó, információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.

(3) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha

a) az információs rendszer felhasználásával elkövetett csalás különösen nagy kárt okoz, vagy

b) a jelentős kárt okozó, információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.

(4) A büntetés öt évtől tíz évig terjedő szabadságvesztés, ha

a) az információs rendszer felhasználásával elkövetett csalás különösen jelentős kárt okoz, vagy

b) a különösen nagy kárt okozó, információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.

(5) Az (1)–(4) bekezdés szerint büntetendő, aki hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával okoz kárt.

(6) Az (5) bekezdés alkalmazásában a külföldön kibocsátott elektronikus készpénz-helyettesítő fizetési eszköz a belföldön kibocsátott készpénz-helyettesítő fizetési eszközzel azonos védelemben részesül."

A bűncselekmény eklektikusságának megfelelően több *jogi tárgyat* véd: egyfelől az informatikai rendszer integritását, biztonságos működését, másfelől – a célcselekmény irányultsága folytán – a vagyoni viszonyokat. A bűncselekmény *elkövetési (tevékenységi) tárgya* a számítógépes adat, amely mint elektronikus impulzus ehelyütt vagyoni értéket jelöl. A bűncselekmény *elkövetési (tevékenységi) magatartása* a jogtalan haszonszerzés végett a számítástechnikai rendszerbe történő elektronikus adat bevitele, az informatikai rendszerben kezelt adat megváltoztatása, teljes törlése vagy hozzáférhetetlenné tétele. A tényállás e része a haszonszerzés végett végrehajtott, azaz célzatos cselekményeket foglal magában. Megtévesztő (csalárd) adatbevitel történhet:

- a számítógép billentyűzetét használva (offline vagy online módban),
- külső adathordozóról történő feltöltés,
- áru vagy szolgáltatás rendelésekor, illetve azok kifizetésekor,
- ATM-en keresztül hamis, hamisított, valódi más nevére szóló bankkártyával történő készpénzfelvétel,
- ATM-en keresztül mobiltelefonegyenleg-feltöltés, különféle szolgáltatók (telekommunikációs, közüzemi stb.) számláinak befizetése, szerencsejátékokra történő befizetés, utasbiztosítás kötése, autópálya-matrica vásárlása és más, a továbbiakban várhatóan bővülő fizetési lehetőségek.

A tényállás *materiális,* azaz a törvényhozó az eredményt, vagyis kár bekövetkeztét határozza meg befejezett bűncselekményként. Mivel az első minősített eset a jelentős kár fogalmát jelöli meg, így az alapesetben a cselekmény akkor büntetendő, ha a kisebb és a nagyobb kár is bekövetkezik, azaz a kárérték ötvenezertől ötmillió forintig terjed. A további minősített esetek a következő értékhatárokhoz igazodnak: ötmillió-egy és ötvenmillió forint között jelentős, ötvenmillió-egy és ötszázmillió forint között különösen nagy, ötszázmillió forint felett különösen jelentős (Btk. 459. § 6. pont).

A minősített esetekben az értékhatár mellett más körülmények is relevanciával bírnak. Bűnszövetség akkor létesül, ha két vagy több személy bűncselekményeket szervezetten követ el, vagy ebben megállapodik, és legalább egy bűncselekmény elkövetését megkísérlik, de nem jön létre bűnszervezet (Btk. 459. § 2. pont). Üzletszerűen követi el a bűncselekményt, aki ugyanolyan vagy hasonló jellegű bűncselekmények elkövetése révén rendszeres haszonszerzésre törekszik (459. § 28. pont).

4.3. Joghatósági problémák az interneten

A *világháló* mint virtuális tér már elnevezésében is jelzi azt a nehézséget, hogy megállapítsuk, egy-egy bűncselekmény hol és mikor válik befejezetté, vagy lép kísérleti szakba, illetőleg, ha a Btk. az előkészületet is büntetni rendeli, mikor és hol tekinthető előkészületnek. Dogmatikailag és a törvényi szabályozásban (Btk. 2–3. §) is egyszerű a válasz: ahol a bűncselekmény tényállási elemei közül akár egyetlen is megvalósul (például a billentyűzet leütése magyar IP-címet jelző számítógépen vagy akár magyar IP-címről, de proxy-szerveren keresztül történik a tiltott tartalomközlés vagy más bűncselekmény elkövetése, vagy a tényállásban szereplő vagyoni kár, más sérelem Magyarországon következik be). De megalapozza a joghatóságot az, ha magyar állampolgár külföldön valósít meg a magyar Btk. szerint üldözendő bűncselekményt, (akár egyetlen) tényállási elemet, vagy egy nem magyar állampolgár által külföldön történő tényállási elem megvalósítása is idetartozik, ha az a cselekmény a magyar törvény szerint bűncselekmény, és az elkövetés helye szerint is büntetendő a cselekmény; de más eseteket is szabályoz a hatályos Btk. Az informatikai bűncselekmények esetében a joghatóság markáns megjelenése nem mindig egyértelműen rögzíthető, mert

- a cselekmény több országban valósul meg (a billentyű leütése az egyik országban történt, a pénzt egy másik ország pénzintézetéből szerezték, az így ellopott pénzt további más országban, országokban bújtatták, majd mindezektől is különböző országban, országokban mosták tisztára, majd egy ismeretlen országban, országokban helyezték el bankbetétként vagy költötték el),
- több ország felhasználóit érinti (például a botnet esetében),
- az elkövetők különböző országokból szerveződnek – akár egy akcióra is –, az internet sötét világában tűnnek fel és el,
- külön problémát jelent a határokon, földrészeken átívelő, a feltöltött adatokat folyamatosan áramoltató *felhőszolgáltatás.*

Az Európai Unió Tanácsának 2009/948/IB számú, a joghatóság gyakorlásával kapcsolatos, büntetőeljárások során felmerülő összeütközések megelőzéséről és rendezéséről szóló keret-

határozata (2009. november 30.) törekszik e problémát feloldani. A joghatósági viták során a tagállamok közötti konszenzusra hívja fel az EU tagállamait (3–113. pont), illetőleg ennek sikertelensége esetén az Eurojusthoz történő fordulást javasolja (14. pont). A joghatósági összeütközés vitájának megoldására, a konszenzus megteremtéséhez az Eurojust 2003-as éves jelentésében megadott szempontok együttes értékelését javasolja az EU Tanácsa. Eszerint a tagállamok vegyék figyelembe

- azt a helyet, ahol a bűncselekmény legnagyobb részét elkövették,
- azt a helyet, ahol a kár vagy veszteség jelentős része keletkezett,
- a gyanúsított vagy vádlott tartózkodási helyét, valamint
- más joghatóságok számára történő átadásának vagy kiadatásának lehetőségeit,
- a gyanúsított vagy vádlott állampolgárságát vagy lakóhelyét,
- a gyanúsított vagy vádlott jelentős érdekeit,
- a sértettek és tanúk jelentős érdekeit,
- a bizonyítékok elfogadhatóságát vagy
- az esetlegesen előforduló késedelmeket.

A felsorolt tényezők egyben sorrendet mutatnak az értékelésben. E körülmények elméletileg megalapozhatják Magyarország joghatóságát.[9] Azonban lehetőség van a büntető joghatóságról – célszerűségi okok miatt – való lemondásra. A büntetőeljárás *átadható,* ha

a) a Magyarországon tartózkodó terhelt annak az államnak az állampolgára, amelynek részére az eljárás átadása történik, vagy abban az államban van az állandó lakóhelye, illetve szokásos tartózkodási helye,
b) a terhelt az eljárás során külföldön tartózkodik, kiadatásának, illetve átadásának nincs helye, kiadatását, illetve átadását megtagadták, vagy kiadatási kérelem előterjesztésére nem kerül sor. A virtuális térben elkövetett bűncselekmények esetében gyakori, hogy a terhelt nem magyar állampolgár, akivel szemben a lefolytatandó büntetőeljárásról célszerű lemondani.

A büntetőeljárás átadására sor kerülhet – a jogerős határozat meghozataláig – az eljárás bármely szakaszában. A hazai jogi szabályozás szerint a büntetőeljárás átadásáról a vádemelésig a legfőbb ügyész, azt követően az igazságügyi és rendészeti miniszter dönt. Külföldi államban folyó büntetőeljárás e hatóság megkeresésére akkor vehető át, ha a terhelt magyar állampolgár vagy Magyarországra bevándorolt nem magyar állampolgár. A büntetőeljárás átvételéről a legfőbb ügyész dönt."[10]

4.4. A kiberbűncselekmények nyomozásának sajátosságai

A nyomozati teendők általában:

- A bűncselekmény alapjául szolgáló, inkriminált adatállomány felkutatása, megismerése, rögzítése.
- A naplózott és a regisztrációs adatok beszerzése a szolgáltatóktól.

[9] Btk. 2–3. §.
[10] 8002/2008 IRM tájékoztató.

- Az informatikai rendszerben fellelhető egyéb elektronikus nyomok, bizonyítékok kutatása, rögzítése.
- Valós térbeli nyomozati munka az ez idáig összegyűjtött bizonyítékok alapján gyanúsítható elkövetőkkel szemben.

A bizonyítékok összegyűjtése a bűncselekmény jellegétől függ. A bizonyítékoknak több lehetséges forrása is lehet.

Kézenfekvő a nyílt forrásból elérhető bizonyítékok felkutatása, rögzítése (OSINT), ezen túlmenően, ha szükséges, jogsegély alapján más nyomozati munkák eredményes elősegítéséhez is használható

- az 1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről,
- a 2000-ben aláírt uniós kölcsönös jogsegélyi egyezmény,
- az ez alapján született 2012. évi CLXXX. törvény az Európai Unió tagállamaival folytatott bűnügyi együttműködésről,
- olyan bilaterális vagy multilaterális szerződés, amelynek Magyarország részese,
- a budapesti egyezmény mint multilaterális egyezmény, amely szerint a nyomozáshoz szükséges segítségnyújtás nemzetközi szerződés hiányában (27. cikk) is történhet,
- továbbá előzetes megkeresés nélkül is segítség nyújtható egy másik államban zajló nyomozáshoz (26. cikk); a segítségnyújtásra rövid úton (e-mail, fax) is lehetőséget teremt az egyezmény (25. cikk 3. pont).

4.5. A közvetítő szolgáltatók típusai, felelőssége

A közvetítő szolgáltatók az információs társadalommal összefüggő szolgáltatást nyújtják:

- hozzáférést biztosító szolgáltatók,
- tárhelyszolgáltatók,
- keresőszolgáltatók,
- gyorsítótár-szolgáltatók,
- tartalomszolgáltatók,
- alkalmazásszolgáltatók.

Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény nem is mindegyiket nevesíti.[11]

1. *A hozzáférést biztosító szolgáltatók (accesss provider)* az internet elérését biztosítják a felhasználók számára. Ma már a legtöbb hozzáférést biztosító szolgáltató nemcsak hozzáférést biztosít, hanem további szolgáltatásokat is nyújt. E-mail fiókot működtet, tárhelyet biztosít, tartalomszolgáltatást nyújt: híreket és más tartalmakat közölnek, saját és mások szolgáltatásait hirdetik, üzletkötési, előfizetési és más lehetőségeket biztosítanak a weboldalukat felkeresőknek.

[11] 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

2. *A tárhelyszolgáltatók* számítógépük, szervereik részleges vagy teljes területét bocsátják rendelkezésére ingyenesen vagy díj fizetése fejében olyan felhasználóknak, akik adataikat, tartalmaikat feltölthetik a tárhelyszolgáltató által biztosított területre. Ismert az osztott tárhelyszolgáltatás is, amikor egy fizikai szerveren, azonos IP-címen több weboldal is elérhető.
3. A *keresőszolgáltatók* (röviden: *search engines*) fő funkciója az internetre feltöltött óriási információtömeg tematikus elérésének biztosítása. A keresőszolgáltatók általában a *surface webet* érik el, a *deep webnek* saját szolgáltatója van. A keresőszolgáltatók további jellemző alkalmazásai a tartalomszolgáltatás, az e-mail-fiók biztosítása, nem ritkán a profilkövető reklámok szolgáltatása (számukra bevételként).
4. *A gyorsítótároló (cache-tároló)* elősegíti az elérni kívánt információ gyorsabb hozzáférését, átmeneti tárolását. Tipikus a böngészőprogramok korábbi eredményeinek tárolása.
5. *Internetes tartalmat nyújtó szolgáltatók (content providers).* A tartalomszolgáltatók információkat, azaz tartalmat töltenek fel az internetre (weboldalaikra), amelyeket az internetes szolgáltatást nyújtó szolgáltató kiszolgálóin (szerverein) helyezik el. A tartalomszolgáltatók szintén többféle lehetőséget nyújtanak, tárhelyet biztosítanak, üzletkötés, előfizetés lehetősége, e-mail-fiók biztosítása is gyakori eleme ezeknek a weboldalaknak.
6. *Az alkalmazásszolgáltatók (current providers)* lehetővé teszik a felhasználók számára, hogy az ahhoz szükséges eszközök megvásárlása nélkül, bérleti vagy eseti díj ellenében vegyenek igénybe információs és feldolgozási szolgáltatásokat (Facebook, Twitter, Yahoo stb.)

Az információs társadalommal összefüggő szolgáltatás megkezdéséhez, folytatásához általában előzetes engedély vagy hatósági határozat nem szükséges. Korlátozás csak a törvényben meghatározott okokból lehetséges:

- a közrend védelme, különösen a bűncselekmények megelőzése, nyomozása, felderítése és üldözése érdekében,
- ideértve a kiskorúak védelmét és a faji, nemi, vallási vagy nemzeti alapú bármilyen gyűlöletre uszítás és az egyének emberi méltóságának megsértése elleni fellépést,
- a közegészség védelme érdekében,
- a közbiztonság érdekében – ideértve a nemzetbiztonsági és honvédelmi érdekeket is,
- a fogyasztók vagy a befektetők érdekei védelmére; és ha a hatósági intézkedés
  a) a fentiekben említett érdekeket sértő vagy súlyosan veszélyeztető szolgáltatás ellen irányul; és
  b) az érdeksérelemmel, illetve a veszélyeztetéssel arányos (az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 3–3/A. § [Ekertv.]).

A törvény külön kiemeli a gyermekek védelme érdekében teendő intézkedéseket is. Olyan információ esetén, amely súlyosan károsíthatja a kiskorúak szellemi, lelki, erkölcsi vagy fizikai fejlődését, különösen azáltal, hogy meghatározó eleme az erőszak, illetve a szexualitás közvetlen, naturális ábrázolása, az adott aloldalt az információ megjelenítése előtt egy figyelmeztető jelzéssel kell ellátni, amely arról tájékoztat, hogy ez az információ

veszélyeztetheti a kiskorúakat. Továbbá az aloldal forráskódjában szereplő olyan azonosítókkal tehető csak közzé az ilyen információ, amelyek utalnak a tartalom kategóriájára, és amelyek szűrőszoftver által felismerhetők (Ekertv. 4/A. §). A *szolgáltatók felelősségéről* az Ekertv. az alábbiak szerint rendelkezik:

1. A *hozzáférést biztosító szolgáltató,* valamint az *alkalmazásszolgáltató* akkor nem felel a továbbított információért, ha
   a) nem a szolgáltató kezdeményezi az információ továbbítását;
   b) nem a szolgáltató választja meg a továbbítás címzettjét, és
   c) a továbbított információt nem a szolgáltató választja ki, illetve azt nem változtatja meg.
2. A *gyorsítótároló szolgáltatója* akkor nem felel az információ közbenső és átmeneti jellegű automatikus tárolásával okozott kárért, ha
   a) a szolgáltató nem változtatja meg az információt;
   b) a tárolt információhoz való hozzáférés megfelel az információ hozzáférésével kapcsolatban támasztott feltételeknek;
   c) a közbenső tárolóban az információ frissítése megfelel a széleskörűen elismert és alkalmazott információfrissítési gyakorlatnak;
   d) a közbenső tárolás nem zavarja meg az információ felhasználásával kapcsolatos adatok kinyerésére szolgáló, széleskörűen elismert és alkalmazott technológia jogszerű használatát; és
   e) a szolgáltató haladéktalanul eltávolítja az általa tárolt információt vagy nem biztosítja az ahhoz való hozzáférést, amint tudomást szerzett arról, hogy az információt az adatátvitel eredeti kiindulási pontján a hálózatról eltávolították, vagy az ahhoz való hozzáférés biztosítását megszüntették, illetve, hogy a bíróság vagy más hatóság az eltávolítást vagy a hozzáférés megtiltását elrendelte.
3. A *tárhely- és az alkalmazásszolgáltató* nem felel szolgáltatásáért, ha nincs tudomása az információval kapcsolatos jogellenes magatartásról vagy arról, hogy az információ bárkinek a jogát vagy jogos érdekét sérti. Amint a fentiekről tudomást szerzett, haladéktalanul intézkednie kell az információ eltávolításáról, vagy a hozzáférést meg kell tagadnia.
4. A *keresőszolgáltató* nem felel az információ hozzáférhetővé tételével okozott kárért, ha nincs tudomása az információval kapcsolatos jogellenes magatartásról vagy arról, hogy az információ bárkinek a jogát vagy jogos érdekét sérti.

Amint a 3–4. pontban írt szolgáltató tudomást szerzett a fenti tiltott cselekményekről, haladéktalanul intézkedik az információ eltávolításáról vagy a hozzáférés megtiltásáról. Ellenben a szolgáltató nem mentesül a felelősség alól, ha az igénybe vevő a szolgáltató megbízásából vagy utasításai alapján cselekszik (Ekertv. 7–12. §). Ha a bíróság az elektronikus adat ideiglenes hozzáférhetetlenné tételét rendelte el egy tárhelyszolgáltatónál, akkor a bíróság ítéletének egy napon belül eleget kell tenni. Ennek nem teljesítése rendbírság kiszabását vonja maga után (Ekertv. 12/A. §). Az EU e-kereskedelmi irányelve bevezette a *notice and take down (értesítés és levétel)* intézményét, amelyet az Ekertv. az alábbiak szerint emelt be a belső jogba: a felhasználó az őt sértő tartalomközlésről értesíti a közvetítő szolgáltatót, amely az értesítés kézhezvételét követő tizenkettő órán belül köteles az értesítésben megjelölt információt eltávolítani és feltüntetni, hogy az eltávolítás a jogosult

jogsértést állító értesítése alapján történt. Egyben három napon belül köteles értesíteni azt az igénybe vevő felhasználót, aki a tartalmat közzétette, hogy a feltételezett jogsértés miatti eltávolítás ellen kifogással élhet, tudniillik az általa közzétett tartalom mégsem volt jogsértő. Amennyiben az eltávolított tartalom közlője 8 napon belül teljes bizonyító erejű magánokiratba vagy közokiratba foglalt indokolt kifogással él az eltávolítás ellen, abban az esetben a közvetítő szolgáltató mérlegelés nélkül köteles az érintett információt újra hozzáférhetővé tenni, és erről a jogosultat a kifogás megküldésével értesíteni (Ekertv. 13. §). A jogosult egyébként a kifogás miatt újra közzétett információ vonatkozásában az igényét – többek között – a jogsértés abbahagyására és az eltiltás iránt ideiglenes intézkedés iránti kérelmet tartalmazó kereset vagy fizetési meghagyás útján érvényesítheti, vagy büntetőfeljelentést tehet. Ez utóbbi esetben a nyomozó hatóságnak felvilágosítási kötelezettsége van, ha magánindítványra büntetendő bűncselekményről van szó. Interneten történő tartalomközlés esetén jellemzően a magánindítványos személyiségi jogokat sértő bűncselekmények jöhetnek szóba (Btk. 211–228. §), kivéve, ha a becsületsértés sértettje rendvédelmi dolgozó. Ha egy szolgáltató – ahogy a fentiekben láttuk – többféle szolgáltatást nyújt, akár ugyanazon a szerveren/weboldalon (például tartalmat közöl és tárhelyként kívülállók kommentárjának is helyt ad), akkor felelőssége is eszerint alakul, azaz a tartalomközlésért felel (hiszen általa írt, szerkesztett tartalmat jelenített meg); míg a tárhelyszolgáltatás esetében (mivel a tartalmat közlő egy kívülálló személy, aki természetesen felelősséggel tartozik megnyilvánulásaiért) a *notice and take down* szabályai szerint kell eljárnia. A tartalommal érintett természetes vagy jogi személytől vagy jogi személyiséggel nem rendelkező személytől függ annak megítélése, hogy a róla közölt tartalom sértő-e vagy sem. Nyilvánvaló bűncselekmény elkövetése esetén a tartalomszolgáltató felelhet a tárhelyén egy kívülálló felhasználó által elhelyezett tartalomért, de a bejegyzés, vélemény jogi megítélését nem lehet a tartalomszolgáltatón számon kérni, különösen, ha az csupán véleménynyilvánítás.

4.6. A felhőszolgáltatás büntetőjogi problémája

A felhőszolgáltatás *(cloud computing)* napjaink olyan új technikai megoldása, amely tehermentesíti a felhasználót attól, hogy nagytömegű adatot tároljon, illetve különböző programokat kelljen telepítenie a számítógépére. A *cloud computing* első hulláma internetes levelezőszerverek (Gmail, Yahoo), közösségimédia-alkalmazások (Facebook, Twitter) és online alkalmazások (Wikinews, blogok, Google Docs) használatával kezdődött. A szerverek számos személyes adatot is tárolhatnak (például bankkártyaszámokat, egy e-mail-kliens címeit, kártyatársaságok adatait). De a felhasználó által előállított információk is (szövegek, képek) kerülhetnek ilyen tárhelyekre (például Dropbox, Evernote). E technikai megoldás következménye, hogy a bűnözés is átterjed a felhőre (2012, *Operation High Roller:* csalás olyan malware segítségével, amely kiiktatta a PIN-es és chipes azonosításokat).

A felhőszolgáltatások típusai:

- szoftverszolgáltatás: a webböngészőn keresztül érhetők el különböző szoftverek,
- platformszolgáltatás: az alkalmazás üzemeltetéséhez szükséges környezetet biztosítja terheléselosztással, frissítéssel,
- infrastruktúraszolgáltatás: virtuális hardver szolgáltatása, tárhely, számítási stb. kapacitás szolgáltatása.

A szolgáltatás számtalan előnnyel kecsegtet. Lehetővé teszi azt, hogy a felhasználók az adataikhoz, programokhoz, egyéb feladatok végrehajtásához a világ bármely pontjáról hozzáférhetnek. A felhasználó adatai nem vesznek el. Itt a jogtiszta programok legfrissebb verziói találhatók meg, amelyek garantáltan vírusmentesek, a szolgáltatás gyors és biztonságos. A felhasználó több platformot tud egyesíteni munkája végzéséhez (például a munkahelyén, utazása során és másutt a saját számítógépén, laptopján, mobiltelefonján keletkező, előállított adatokat együtt tárolja, dolgozik azokkal). A technikai részletek kíméletes említése nélkül nem érthetjük meg a jogi problémákat. A szolgáltatók több szerveren, más eszközön tárolják az adatokat, programokat. A szerverek lehetnek ugyanazon vagy különböző országokban, távoli szigeteken. Ez utóbbi a jellemző. Közöttük az adatkapcsolat élő, hiszen az adatok folyamatos biztonsági mentése a felhőszolgáltató feladata, kötelessége. Az adatokat a felhőszolgáltató titkosítja, a felhasználókon kívül más nem ismerheti meg. Kérdés, hogy a felhőben (egy ismeretlen helyen levő szerveren, illetve a szerverek között mozgásban) levő inkriminált adatállomány (például egy tiltott tartalom) és annak előállítója, közösségi oldalon közlője, blogoldalra feltöltője stb.) hogyan válhat egy büntető- vagy más eljárás alanyává, illetve bizonyítékká. A nyomozás nehézségei általában a felhőszolgáltatás vagy egy külföldön található szerver (tárhely) esetében a következők:

- különbözők a szolgáltatók, különböző a szerverek földrajzi elhelyezkedése, különböző joghatóságok alá tartoznak,
- sem a fizikai eszköz, sem az elektronikus adat nem alapozhatja meg a joghatóságot,
- a különböző országban (földrészen) levő szervereken az inkriminált adatállomány szétszórva is lehet, amit csak a *cloud service provider* képes összegyűjteni,
- a szolgáltató a székhelye szerinti jogi szabályokat alkalmazza (például közösségi oldalakon, *social networks* vonatkozásában; szigorúbb lehet az adatvédelem, tágabb lehet a véleménynyilvánítás szabadsága stb.),
- minél nagyobb földrajzi területen szolgáltat (a felhőszolgáltató, közösségi oldalak, kereskedelmi oldalak), annál több megkeresés érkezhet a szolgáltatóhoz, amely miatt a megkeresett szolgáltató szelektál.

A felhőszolgáltatók, a közösségi oldalak üzemeltetői, a kereskedelmi szolgáltatások együttműködési hajlandóságától függ, hogy az adott ügyben a magyar hatóságok megkeresésére válaszolnak-e vagy sem. Ugyanakkor, ha a szolgáltató nem adja át a kért információkat, akkor esetleg a koronabizonyítékokat vagy az azokat előállító személyek megismerését ez rendkívül megnehezíti. Mondhatnánk, hogy az eljáró hatóság keressen más bizonyítékot a cselekmény bizonyításához, de egy tartalomközlést a tartalom egészével, az azt feltöltő személyt annak adataival lehetséges bizonyítani. Manapság a terrorizmussal, emberöléssel, kábítószerrel kapcsolatos bűncselekményekkel, pénzmosással és más nagyon súlyos bűncselekménnyel összefüggésben történő megkeresés kecsegtet sikerrel. A polgárjogi felelősség kérdése is valós, például az elvesztett adatállományért vagy szolgáltatás igénybevételének elmaradásáért való civiljogi felelősség. Kívánatos volna a nemzetközi együttműködés megteremtése, a magánkézben levő szolgáltatók (és profitérdekeik), valamint az igazságszolgáltatás érdekei közötti egyensúlyt megtalálni.