DOI: 10.38146/BSZ.2017.1.2

LAKATOS ALEXANDRA ANNA

Az informatikai bűncselekmények és a bitcoin

Tanulmányomban az informatikai bűncselekményeket és a bitcoin nevű virtuális valutát általánosságban, továbbá annak a büntetőjogra gyakorolt hatását kívánom bemutatni, kitérve a hazai és a nemzetközi gyakorlati tapasztalatokra is.

Az informatikai bűncselekmények[1]

Hogyan hatott a számítógép és az internet a büntetőjogra?

A számítógépes bűnözés egyidős a számítógépek elterjedésével. Sokoldalúsága miatt a számítógép eszközévé vált egyes, korábban már ismert bűncselekményeknek, emellett katalizátora lett újabb, a társadalomra veszélyes cselekmények megjelenésének.

Az internet alapjait az 1960-as években fejlesztették ki az Egyesült Államokban. Az ARPANET *(Advanced Research Projects Agency Network)* eredetileg katonai célokat szolgált, és megteremtette az összeköttetést Angliával, Hollandiával és a skandináv államokkal.[2] 1991-es kereskedelmi megjelenésével az internet új színtere lett a bűnelkövetésnek: a klasszikus bűncselekmények (például csalás, pornográfia, kábítószerrel visszaélés) új formát öltöttek, és új deliktumok (például szerzői jogi jogsértések, phishing, hacking, vírustámadások) is elkövethetők lettek.[3] A bűncselekmények áttörték a határokat, megnehezítve ezzel a felderítést és az elkövetők felelősségre vonását, nagy feladat elé állítva a nemzetközi jogalkotást és jogalkalmazást.

A világ és az Európai Unió reakciója a számítógépes bűnözésre

Az Egyesült Nemzetek Szervezete 1994-ben jelentette meg az informatikai bűnözéssel foglalkozó tanulmányát *UN Manual on the Prevention and Control of Computer-Related Crime* címmel, amely meghatározta a számítógéppel kapcsolatos bűncselekmények lehetséges megjelenési formáit, és hangsúlyozta az eljárási kérdések, különösen a nemzetközi együttműködés fontosságát.[4]

Az Európa Tanács 2001-ben fogadta el a számítástechnikai bűnözésről szóló egyezményt *(Conviction on Cyber-Crime)*. Mintegy harminc ország képviselője 2001. november 23-án, Budapesten írta alá a budapesti egyezmény néven is ismert megállapodást, amely több lényeges szempontból meghaladta elődeit, hiszen definíciókat adott a számítástechnikai rendszer elemeire, valamint együtt tárgyalta a nemzetközi, anyagi és eljárásjogi összefüggéseket.[5]

Az Európai Unióban – a szabadságon, biztonságon és a jog érvényesülésén alapuló térség részeként – a tagállamokkal megosztott hatáskörbe tartozik a tagállamok közötti bűnügyi együttműködés, ezért a számítástechnikai bűncselekményekre nézve is minimumszabályok írhatók elő. A tanács 2005. február 24-én fogadta el a 2005/222/IB számú kerethatározatot, amely átvette a budapesti egyezmény számítástechnikai bűncselekményeket érintő tényállásait, és uniós jogforrásként kötelezővé vált az unió valamennyi tagállamára, így igen jelentős lépésnek számít az informatikai bűncselekmények elleni nemzetközi együttműködésben.[6]

Magyar fellépés az informatikai bűncselekmények ellen

Magyarországon először az 1990-es évek elején jelentek meg a számítógépet érintő bűncselekmények. Számuk néhány éven át rendkívül csekély maradt, de a számítástechnika fejlődésének gyors ütemére, a különböző informatikai alkalmazások terjedésére tekintettel egyre növekvő tendenciát mutat.[7]

A hagyományos bűnelkövetéssel ellentétben, az informatikai bűncselekményeknél kevés a rendelkezésre álló statisztikai adat, a különleges infrastruktúra miatt magas a latencia, speciális az elkövetés helye, ideje, eszköze, az elkövetéshez – és a felderítéshez – speciális szakismeret szükséges, kevés adat van az elkövetők személyéről, speciális a jogi és az elkövetési tárgy is. Az információs társadalom[8] új deliktumai többfajta jogi tárgyat sértő, illetve veszélyeztető bűncselekmények.[9]

Informatikai bűncselekmények a büntető törvénykönyvben[10]

Hazánkban a számítógépet, az informatikát és az internetet érintő deliktumokat többféleképpen csoportosíthatjuk. Ha az internet az elkövetés tárgya, akkor a bűncselekmény számítástechnikai[11], de ha az elkövetés eszköze, internetes bűncselekménnyel állunk szemben.[12]

Az interneten, illetve annak felhasználásával megvalósuló bűncselekmények közé tartoznak a tartalomszolgáltatás terén elkövetett, a hálózat biztonságát sértő és egyéb internetfelhasználással összefüggő deliktumok.[13]

Tartalom-bűncselekmények

A tartalomszolgáltatás terén elkövetett bűncselekményekkel a jogalkotó az interneten megjelentetett tartalom, illetve annak tiltott volta miatt kriminalizálja a cselekményeket.

A szerzői jogról szóló 1999. évi LXXVI. törvény (a továbbiakban: Szjt.) oltalomban részesíti a szellemi alkotásokat, amit kiegészít a büntetőjog által nyújtott védelem. Így a szerzők műveinek jogszabálysértő módon történő felhasználása[14] szankciót von maga után.[15]

Ugyancsak a tiltott adattartalom közzététele körébe tartozik a gyermekpornográfia[16], az önkényuralmi jelkép használata[17], valamint a személyiségi jogi jogsértések[18] egyes esetei is.

Számos deliktum kapcsolódik internetes hirdetésekhez. Itt kell megemlíteni az előkészületi magatartások között szabályozott ajánlkozást, vállalkozást bűncselekmény elkövetésére[19], a közokirat-hamisítást[20], a kábítószerkereskedelmet[21], valamint a csalást[22].

A hálózat biztonságát sértő bűncselekmények[23]

Az internet és a számítógép által uralt világban az adatot, az információt és magát az információs rendszert is védeni kell. Ehhez a büntetőjog is segítséget nyújt az információs rendszer felhasználásával elkövetett csalás[24], a készpénz-helyettesítő fizetési eszköz hamisítása[25], a védelmet biztosító műszaki intézkedés kijátszása[26], a tiltott adatszerzés[27], az információs rendszer vagy adat megsértése[28], valamint az információs rendszer védelmét biztosító technikai intézkedés kijátszása[29] törvényi tényállásaival.

Internetfelhasználással elkövetett egyéb bűncselekmények

Az internet bármely bűncselekménynél kommunikációs csatornaként funkcionálhat az elkövetők között, színtere lehet a részletek megvitatásának e-mail, chat vagy bármi más formájában.

A közösségi portálok és a cyberbullying

A közösségi portálok megjelenéséhez szükség volt az úgynevezett web 2.0-s szolgáltatások kialakítására, amelyek olyan internetes közegben működő közösségre épülnek, ahol a felhasználók megosztják egymás információit, és így a tartalmat együtt hozzák létre, maga a szerver ehhez csak a keretrendszert adja.[30]

Facebook

A Facebook, a világ egyik legnagyobb és legismertebb közösségi hálózata, 2004. február 4-én kezdte meg működését. Egyik alapítója, az amerikai *Mark Zuckerberg* ma a világ egyik leggazdagabb embere. 2012. október 4-én a Facebook elérte az egymilliárd regisztrált felhasználót, számuk jelenleg 1,23 milliárd, ami a teljes internetpopuláció harmincnyolc százaléka.[31]

A közösségi oldal használójává regisztrációval válhatunk, ehhez mindenképpen meg kell adnunk a nevünket, születési dátumunkat, e-mail-címünket, a nemünket és az általunk választott jelszót. Ezeken kívül saját döntésünk, hogy megadjuk-e iskolai végzettségünket, politikai és vallási nézetünket[32], családi állapotunkat, telefonszámunkat, vagy éppen képet, videót töltünk fel, amivel óhatatlanul kiszolgáltatjuk magunkat, családunkat és barátainkat az internetes bűnelkövetőknek.[33]

Jó, ha tudjuk, hogy a felhasználók adatlapjait folyamatosan ellenőrzik a rendszergazdák, és bármilyen nem megengedett, tisztességtelen vagy akár erőszakos viselkedés következményeként a hozzászólást vagy változtatást törlik. Ha ez a tevékenység nem szűnik meg, akkor a felhasználói profilt felfüggesztik, végső soron törlik, amit maga a felhasználó is végrehajthat. Az adminok természetesen csak olyan közösségi aktivitást „szankcionálnak", ami a Facebook felhasználási feltételeivel[34] és közösségi alapelveivel[35] ütközik.[36]

Saját védelmünk érdekében felhasználóként elsősorban arra kell figyelnünk, hogy az adatvédelmi beállítások közül a számunkra legmegfelelőbbet válasszuk, és alaposan gondoljuk át, hogy mely adatokat szeretnénk másokkal megosztani. Felhasználói fiókunkat „erős" jelszóval[37] védjük, és ismerjük a közösségi alapelveket annak érdekében, hogy ha azok megsértésével találkozunk, be tudjuk azonosítani, és tisztában legyünk azzal is, hogy úgynevezett jelentésben felhívhatjuk a szolgáltató figyelmét a megfelelő lépések megtételére.[38]

Cyberbullying

A cyberbullying, más néven elektronikus zaklatás[39] elsősorban a tinédzserek között tapasztalható iskolai kiközösítés új típusa, amely az áldozathoz elektronikus úton, sok esetben közösségi portálokon eljutó durva csúfolódásokból, fenyegetésekből álló üzenetek sorozatát jelenti, amit egy vagy több felhasználó valósít meg. Az ismétlődő ellenséges magatartás hatása rendkívül káros a személyiségfejlődésre és az önbecsülésre: ami az elkövetőnek egyszerű tréfának tűnhet, az súlyos, egész életen át tartó lelki sérüléseket okozhat az áldozatnak.[40]

A fenyegetések akár ismeretlen telefonszámról történt hívásokkal, smsben vagy mms-ben, e-mailben, vagy az áldozat honlapján, a közösségi oldalakon létrehozott profilján, akár a képei alatt vagy az általa látogatott chatszobákban, illetve MSN-en érhetik el a sértettet. A zaklatók gyakran lejáratő, gyűlölködő weboldalakat hoznak létre, titokban felvételeket készítenek a kiszemelt áldozatról megalázó helyzetben (például ahogy az iskolában csúfolják, megverik), vagy lementik az áldozat közösségi oldalakon közzétett fotóit, amelyeket retusálnak, és trágár módon kommentálják.[41]

Hazánkban a 15-17 évesek 93 százaléka, és a 14 évesnél fiatalabbaknak is majdnem a fele rendszeres használója az internetnek, elsősorban a közösségi oldalaknak. Pontos adat arról azonban nincs, hogy mennyire elterjedt, illetve jelen van-e egyáltalán közöttük a cyberbullying, amely *Parti Katalin,* az Országos Kriminológiai Intézet munkatársa szerint az offline változatnál is veszélyesebb, és mindig a való életben zajló zaklatás folytatása.[42]

A bullying ellen prevenciós programok[43] indultak, amelyek leginkább a passzív szemlélőket célozzák. Az áldozatot ugyanis már azzal meg lehet védeni a káros lelki hatásoktól, ha valaki kiáll mellette, a be nem avatkozás viszont legitimálhatja is a bántalmazást.[44]

A virtuális közösségek és a virtuális bűncselekmények

Virtuális közösségek[45]

Az olyan online közösségi terek fejlődésével, mint a Facebook, a YouTube vagy a sokszereplős online szerepjátékok (MMORPG)[46], a felhasználók számára lehetővé vált, hogy a fizikai világban megszokottól teljesen eltérően viselkedjenek egymással. Ennek az az oka, hogy az internet lehetőséget teremt arra, hogy a felhasználók olyan online személyiséget hozzanak létre, amely-

nek segítségével olyan viselkedést tanúsíthatnak, amelyet lehet, hogy soha sem tennének meg a valódi világban. Az úgynevezett kiberteret az emberek eszközként használják, amelyen keresztül kommunikálhatnak másokkal a Föld bármelyik pontjáról, s közben ellátja őket hírekkel, reklámokkal és szórakozással. Vannak olyanok is, akik nemcsak eszközként használják, hanem birtokba is veszik a kiberteret. Életük egy részét átviszik az itt található virtuális valóságba, és online személyiséget alakítanak ki, amelynek irányításába teljesen belefeledkeznek, miközben sok esetben elveszítik a közvetítettség tudatát: a személy nem érzékeli többé, hogy maga is benne van a médiumban.[47]

Virtuális bűncselekmények

A *virtual crime* (virtuális bűnözés) kategóriája a számítógépes szoftverek által szimulált virtuális közösségekben történő bűnözést jelenti. Idetartoznak a virtuális világon belüli játékos (avatar) ellen irányuló személy elleni bűncselekmények (például kényszerítés, zaklatás), vagy a virtuális javakra[48] elkövetett csalás, lopás, sikkasztás, a más tulajdonában lévő virtuális tárgyak jogosulatlan elpusztítása. A *virtual crime* olyan deliktumokat ölel fel, amelyeket egyedül az különbözteti meg a fizikai világban elkövetett bűncselekményektől (például egy fizikai értelemben vett dolog ellopásától), hogy azokat egy másik, alternatív univerzumban követik el. A *virtual crime* körébe sorolható számítógépes bűnözés a visszaélések sajátos, egyedi csoportja, amely speciális tendenciákat mutat.[49]

A bitcoin

A bitcoin (általánosan használt megjelölése: BTC)[50] egy magát Nakamoto Szatosinak nevező ismeretlen személy[51] 2008 novemberében megjelentetett cikke[52] nyomán került be a köztudatba. A bitcoin egyfelől egy új típusú, peer-to-peer (P2P) hálózatra[53] épülő, decentralizált fizetési rendszer, technológiai értelemben tehát működésének egy központi szerver az alapja.[54] Másfelől egységnyi, nyílt forráskódú digitális fizetőeszköz, egy kriptovaluta[55], amelyet a bitcoinhálózat hoz létre egy matematikai algoritmussal, egy generált elektronikus adat, amely tranzakciók feldolgozása és jóváhagyása révén keletkezik egy előre meghatározott algoritmus alapján. Ezt a folyamatot nevezzük bányászásnak *(mining)*.[56]

A teljes bitcoinállomány folyamatosan bővül, becslések szerint végleges állapotát a 2140. év környékén éri el, amikor huszonegymillió bitcoin lesz

forgalomban. Az elemzések azt mutatják, hogy a teljes BTC-állomány hetvenöt százalékát tizenegyezer ember birtokolja, ami hozzájárul a rendszer viszonylagos stabilitásához.[57]

A bitcoin mint virtuális fizetőeszköz

Eltérően az általános értelemben vett elektronikus pénztől[58], a BTC-nek nincs kibocsátója, a rendszer felett semmilyen szervezetnek vagy vállalatnak nincs hatalmi befolyása, és így prudenciális felügyelete[59] sem. A bitcoin tehát közgazdasági értelemben decentralizált, egy virtuális fizetőeszköz, amely az interneten létezik és teljes mértékben bitekből áll, fizikai megtestesülésével, érmeként vagy bankjegyként sehol sem találkozhatunk vele. Nincs mögötte fedezet áruban, aranyban vagy bármilyen más nyersanyagban, csupán az a harmincegyezer sornyi forráskódból álló szoftver, amivel hozzáférhetünk a teljesen virtuális fizetőeszközhöz. A BTC a P2P csomópontjai által tárolt elosztott adatbázisra támaszkodik, amely tartalmazza a tranzakciók adatait, garantálva az elektronikus fizetőeszközökre vonatkozó alapvető követelményeket.[60]

A polgári törvénykönyvről szóló 2013. évi V. törvény (Ptk.) 5:14. § alapján a bitcoin polgári jogi értelemben nem dolog, és nem tekinthető sem pénznek, sem készpénz-helyettesítő fizetési eszköznek minősülő elektronikus pénznek, hiszen nincs kibocsátója. Ugyanezen okból a tőkepiacról szóló 2001. évi CXX. törvény (Tpt.) 5. § (1) bekezdésének 29. pontja szerint értékpapírnak sem minősül. Mivel a vagyoni jog, az árucikk és a szellemi termék fogalmába sem tartozik, a BTC jogi megítélése jelenleg kérdéses, nemzeti jogunkban egyelőre kezelhetetlen, értelmezhetetlen.[61]

A Magyar Nemzeti Bank fogyasztóvédelmi feladatkörében kiadott figyelmeztetéseiben[62] ugyanakkor már foglalkozott a BTC-vel, és azt „fizetésre használható eszközként" jelölte meg. *Szathmáry Zoltán* emiatt arra a következtetésre jutott, hogy a bitcoin jelenleg jogilag nem kategorizált virtuális jószág, virtuális vagyontárgy, amely részben dolog (pénz) módjára viselkedik.[63]

Hogyan lehet BTC-vel fizetni?

A bitcoinhálózat váza egy úgynevezett blokklánc *(block-chain),* amely egy nyilvános adatbázis: tartalmazza az összes eddig megtörtént tranzakciót, és az újabb tranzakciókkal folyamatosan bővül. A blokklánc jelentősége az, hogy nyilvános adatbázisként visszakövethető, ellenőrizhető és szabadon le-

kérdezhető, emellett az összes lezajlott tranzakció adatbázisaként minden további intézkedés nélkül hiteles adatokat szolgáltat.[64]

A rendszer használatához le kell tölteni egy ingyenes szoftvert[65] az internetről, amelyet a bitcoin hivatalos honlapján[66] találunk meg. Ez a nyílt forráskódú program funkcionál virtuális pénztárcaként a számítógépen, amely a digitálisan megjelenő BTC-t tárolja. A bitcoin tehát nem kézzelfogható, fizikailag létező fizetőeszköz, hanem egy olyan virtuális pénzösszeg, amely társítva van egy virtuális pénztárcával, ami nem más, mint egy wallet.dat nevű fájl a merevlemezen. A pénztárcát ezért akár el is lehet lopni, ha valaki illetéktelenül behatol a rendszerbe. Ennek megakadályozása érdekében érdemes biztonsági másolatokat készíteni a fájlokról, de léteznek olyan internetes szolgáltatások is, ahova regisztrálva feltölthetjük a tárcánkat, és ahhoz csak megadott jelszavunkkal férhetünk hozzá.[67]

A virtuális pénztárcaként működő program másik jellemzője, hogy azzal lehet egymásnak bitcoinokat küldeni. A tranzakciók kivitelezésére szolgálnak az úgynevezett bitcoincímek, amelyeket a virtuálispénztárca-szoftver kérésünkre automatikusan generál. Minden felhasználónak van legalább egy bitcoincíme, amely logikailag egy e-mail-címhez hasonlít. A program elvileg minden egyes tranzakcióhoz külön címet készít, növelve ezzel az anonimitást és a rendszerbiztonságot.[68] Az egyszer már létrehozott címeket nem lehet kitörölni, azok a digitális pénztárcában bármikor visszakereshetők, és az is megtekinthető, hogy adott címről mennyi pénzt kapott, illetve mennyit utalt át annak tulajdonosa.[69]

Mindegyik bitcoincím két részből áll: az egyik az úgynevezett nyilvános kulcs, a másik a privát kulcs. A nyilvános kulcsot a programba való belépéskor látni lehet, míg a címhez tartozó privát kulcs rejtve marad. Egy adott cím nyilvános kulcsának olvasható formája 33 karakterből áll, és mindig egyessel kezdődik.[70] Az ilyen nyilvános kulcsot kell megadnunk másoknak, amikor a bitcoinhálózaton keresztül BTC-t szeretnénk küldeni. A tranzakciók hitelesítéséhez a program a privát kulcsot használja, amely egyfajta elektronikus aláírásként funkcionál, növelve ezzel a biztonságot. A nyilvános kulcsokat és a hozzájuk tartozó privát kulcspárokat a wallet.dat fájlban tárolja a program. A tranzakció teljesüléséhez a privát kulcsokat nem szükséges megadni a másik félnek, ellentétben a publikus kulcsokkal. A bitcoinhálózat a rajta keresztül létrejövő tranzakciókat az egész hálózaton szétküldi, így azok teljesen nyilvánosak.[71] A BTC-vel végzett valamennyi tranzakció a hálózatot használó közösség 51 százalékának konszenzusa után végleges és visszafordíthatat-

lan. A rendszer működése tehát kizárja a többször felhasználható bitcoinok forgalomba hozatalát, vagy egy BTC többszöri felhasználását.[72]

A program semmilyen információt nem kér a személyes adatokat illetően, a bitcoincímek tulajdonosaira vonatkozó információk tehát egyáltalán nem ismertek, így részükre garantált a teljes anonimitás. Általánosságban elmondható, hogy a professzionális titkosítás és az anonimitás miatt az elővigyázatos felhasználók informatikai eszközökkel való nyomon követése nem vagy csak nagyon nehezen kivitelezhető.[73] Ez az, ami miatt sokan megkérdőjelezik a bitcoin legitimitását, hiszen nem kell ahhoz túl nagy fantázia, hogy elképzeljük: milyen lehetőségeket nyújthat a rendszer a teljes anonimitás mögé bújó internetes bűnelkövetők számára.

Az interneten elkövetett bűncselekmények nyomozati és bizonyítási nehézségei

Az internetes bűnelkövetésnél alapvetően az jelenti a nyomozás és a bizonyítás nehézségeit, hogy digitális bizonyítékokkal kell dolgozniuk a hatóságoknak. Ilyenek az adathordozókon lévő digitális dokumentumok (szövegek, képek, filmek, adatbázisok), a jellemzően winchestereken megtalálható digitális nyomok (swap file, átmeneti, töredék-, törölt állományok), valamint a szolgáltatók által nyilvántartott napló- és regisztrációs adatok. Közülük az első megtekintéséhez nem, míg a második rögzítéséhez szükséges a különleges szakértelem (igazságügyi informatikai szakértő), a harmadik kategória kapcsán pedig a szolgáltatók törvényben előírt megőrzési kötelezése[74] nyújt segítséget a felderítésben. E bizonyítékok beszerzése elsősorban a Be. 71. §-a szerinti megkereséssel, a Be. 151. §-ában szabályozott lefoglalással, vagy a Be. 158/A § (1) bekezdésében írt számítástechnikai rendszer[75] útján rögzített adatok megőrzésére kötelezés keretében történik.[76]

Bűnüldözés: cyber-attacks

A *cyber-attacks* a személyek vagy komplett szervezetek elleni támadások olyan formája, amely informatikai rendszereket, számítógépes hálózatokat és/vagy személyi számítógépeket céloz, azokat rendszerint anonim eszközökkel támadja a rendszer túlterhelése, az oda való betörés, vagy adatlopás érdekében.[77]

Magyarország

2015. december 22-én kutatási célú interjút készítettem *Pál Tamás* rendőr őrnaggyal, a Készenléti Rendőrség Nemzeti Nyomozó Iroda[78] csúcstechnológiai bűnözés elleni osztályának osztályvezető-helyettesével. Pál Tamás elmondta, hogy az osztály a hatáskörébe tartozó kiberbűncselekmények *(cyber-attacks)*[79] miatt induló büntetőügyekben nyomozati tevékenységet végez, és bár a Nemzeti Nyomozó Iroda szakirányítási feladatot nem lát el, segítséget nyújtanak a kiberbűnözés kapcsán eljáró más szerveknek is. Nyomozóik emellett elsősorban az online gyermekpornográfiával (gyermekek szexuális kizsákmányolása) kapcsolatos büntetőügyekben járnak el.[80] Az osztályon dolgozó technikusok továbbá monitorozó tevékenységet folytatnak nyílt forráskódú adatok elemzése körében[81], valamint külső segítőként tevékenykednek hiteles adatmentések során (forenzikus munka).

A konkrét büntetőügyeket illetően Pál Tamás azt mondta, hogy leginkább rendszer elleni támadások miatt indult eddig nyomozás az osztályon, bitcoint érintő bűncselekmény miatt Magyarországon még nem tettek feljelentést. A közelmúltban elsősorban az Anonymous nevű hackercsoport[82] 2012. márciusi Alkotmánybíróság elleni[83], valamint a 2015. december végén Magyarország kormánya, miniszterelnöke és a nagyobbik kormánypárt elleni[84] támadásai miatt induló nyomozásokról értesülhettünk.

Nemzetközi bűnügyi együttműködés

Tanulmányom témájára koncentrálva fontos kiemelni, hogy a kiberbűncselekményeket általában határokon átnyúló elkövetés jellemzi, ezért az ilyen ügyekben zajló nyomozások során gyakran bűnügyi együttműködésre, illetve jogsegélykérelmekre van szükség.

A nemzetközi bűnügyi együttműködés formáit a nemzetközi bűnügyi jogsegélyről szóló 1996. évi XXXVIII. törvény, a bűnüldöző szervek nemzetközi együttműködéséről szóló 2002. évi LIV. törvény, valamint az Európai Unió tagállamaival folytatott bűnügyi együttműködésről szóló 2012. évi CLXXX. törvény szabályozza. Ezek közé tartozik például a közös nyomozó csoport létrehozása, valamint a fedett nyomozó alkalmazása, amelyben a magyar bűnüldöző szervek az Országos Rendőr-főkapitányság Nemzetközi Bűnügyi Együttműködési Központjának (Nebek) közreműködésével vesznek részt.

Pál Tamás elmondása szerint a Nemzeti Nyomozó Iroda munkatársai 2014. november 6-án nemzetközi bűnügyi együttműködés keretében vettek

részt az Amerikai Egyesült Államokkal együttműködve, az Europol koordinálásával világszerte zajlott úgynevezett Onymous akcióban, amelynek két magyar szála is volt. Az akció keretében összesen 17 online piacteret üzemeltető személyt fogtak el, 410 rejtett hálózatot kapcsoltak le, valamint nagy értékű BTC-t, eurót és egyéb vagyontárgyakat foglaltak le.[85]

Az egyre fenyegetőbbé váló kiberbűnözés elleni küzdelem jegyében 2013 januárjában hozták létre az Europol EC3 (European Cybercrime Center) nevű európai rendőrségi szervezetet, amely fő prioritásaként jelölte meg – a gyermekek szexuális kizsákmányolása és az online csalások mellett – az Európai Unió kritikus infrastruktúrái és informatikai rendszerei elleni kibertámadások *(cyber-attacks)* megakadályozását, aminek következtében szoros együttműködés alakult ki a részt vevő országok hatóságai és a civil szféra számos szakértője[86] között. Az Europol EC3 munkatársai nemzetközi szinten koordináló, elemző és felderítő munkát végeznek, segítségükkel felgyorsult az információáramlás, valamint a nyilvántartásokba történő adatfeltöltés és -letöltés is, ami jelentősen megkönnyíti a bűnüldöző szervek munkáját.[87]

A bitcoint érintő visszaélések a gyakorlatban

Az Europol EC3 és a Nemzeti Nyomozó Iroda gyakorlata szerint a BTC-vel elkövetett deliktumok három csoportba oszthatók: *1.* a tisztán kiberbűncselekmények (például a világ legnagyobb virtuális pénzügyi kereskedési központjának számító japán tőzsde, az MtGox BTC tőzsde összeomlása az ott található bitcoinok eltulajdonítása miatt[88]); *2.* a kiberbűncselekményekkel összefüggésbe hozható cselekmények (például az úgynevezett *ransomware*-ek, a különböző zsarolóprogramok használata, majd a sértettől BTC követelése[89]); valamint *3.* az olyan bűncselekmények, ahol az anonimitás érdekében BTC-vel lehet fizetni (például a Silk Road nevű illegális weboldal esete).

A Silk Road

Ahogy a tanulmány elején említettem, az internet őse katonai alapokon jött létre, ez után kezdték alkalmazni először az egyetemek zárt közösségeiben, majd 1991-ben a kereskedelmi használata is lehetővé vált.

A kereskedelmi megjelenés után kialakult az internetnek egy olyan része, amely az átlagos felhasználók által érzékelt, kb. tíz-tizenöt százaléknyi adattartalmat magában foglaló nyílt interneten túli láthatatlan részt jelenti. Ezt nevezzük angolul *deep web*nek, e terület legfőbb jellemzője, hogy az ott futó

szolgáltatásokat nem lehet azonosítani, illetve ahhoz szükség van egy speciális programra, mint amilyen például a TOR *(the onion router)*. A TOR eredetileg az amerikai haditengerészet projektje volt, napjainkban azonban nyílt forráskódú programként bárki letöltheti, így vált az internet sötét oldalának *(dark web)* motorjává, a kábítószer és a gyermekpornográfia fellegvárává.[90]

A *dark web* egyik méltán hírhedt site-ja volt a Silk Road, egy a TOR titkosító hálózaton elérhető – tehát a klasszikus keresőszerverek számára láthatatlan – online piactér, ahol különböző illegális tevékenység folyt: lehetett például hamis személyi okmányokat és drogot is rendelni, tiltott pornográf tartalmak voltak elérhetők, sőt emberek megölésére is lehetett megbízást adni úgy, hogy – az anonimitás érdekében – a számlát nem valódi pénzzel, hanem bitcoinnal egyenlítették ki, ami a BTC már említett jellemzői miatt – a banki átutalással ellentétben – nem nagyon volt visszakövethető.[91] Az Amerikai Egyesült Államok Szövetségi Nyomozó Irodája (FBI) 2013 őszén hajtott végre rendőrségi akciót az ügyben, ennek keretében zárolták a Silk Road weboldalát, ahol több mint 1,2 billió amerikai dollár értékben bonyolítottak le illegális üzleteket, amiből 9,5 millió BTC (1,2 milliárd dollár) haszon származott, ebből csak a tulajdonoshoz hatszázezer BTC (80 millió dollár) bevétel folyt be.[92]

Az FBI cyber-crime-specialistája, *Christopher Tarbell* beszámolója szerint[93] a Silk Road alapítója, a Dread Pirate Roberts (DPR) nicknevű személy úgy került rendőrkézre, hogy a website létrejötte után, 2011. január 27-én „Altoid" felhasználónév alatt egy kábítószerekkel kapcsolatos fórumbejegyzésben megemlítette a Silk Roadot, és javasolta annak kipróbálását. Két nappal később egy Bitcoin Talk nevű fórumon „Altoid" közzétette az oldal linkjét, és arról érdeklődött, hogy azt látta-e már valaki. Nyolc hónappal később a Bitcoin Talkon „Altoid" IT-szakembereket keresett egy BTC-vállalkozáshoz, és elérhetőségként a rossulbricht@gmail.com e-mail címet adta meg. Az e-mail cím alapján *Ross William Ulbricht* nyilvános Google profilján látható volt, hogy kedvelője az osztrák Ludwig von Mises Intézetnek, amit DPR a Silk Road filozófiájának forrásaként említ. Dread Pirate Roberts egy olyan hálózatról használta az internetet, amely fals IP-címet hozott létre (virtual private network: VPN), azonban a VPN-szerver bejegyzései alapján megállapították, hogy egy San Franciscó-i internetkávézóból csatlakozott a rendszerre, amely éppen Ulbricht tartózkodási helyének közelében volt. 2011 júliusában egy Kanadából érkezett csomagot foglaltak le, amelyben kilenc különböző névre kiállított, de minden esetben Ulbricht fényképével ellátott hamis személyazonosító okmányokat találtak. A nyomozás során korábban

megállapították, hogy DPR a Silk Roadon hamis okmányokat kívánt szerezni azért, hogy további szervereket béreljen a weboldal számára. Kiderült az is, hogy nem ez volt az egyetlen eset, amikor DPR illegális szolgáltatást próbált vásárolni az oldalon: 2011 márciusában ugyanis egy a Silk Road-felhasználók ezrei személyes adatainak kiszivárogtatásával fenyegető személy megölését rendelte meg százötvenezer dollárnyi BTC-ért cserébe. A harminc-éves Ross William Ulbrichtot 2015 februárjában mind a hét vádpontban[94] bűnösnek találta a manhattani bíróság, e miatt 2015 májusában életfogytig tartó szabadságvesztés-büntetésre ítélték.[95]

Zsarolóprogramok

Az úgynevezett *ransomware*-ek hatékonyan vegyítik a digitális és a hagyományos bűnözés elemeit, hiszen olyan rosszindulatú programok, amelyek a számítógépre települve zsarolóüzenetekkel árasztják el a felhasználót. A többnyire rendőrségi logókkal ellátott figyelmeztetésekben[96] általában az áll, hogy a hatóságok a gépen tiltott pornográf tartalmat találtak, emiatt a felhasználó fizessen be egy meghatározott pénzösszeget (maximum néhány száz eurós büntetést), és ezzel a dolog el van intézve.[97] Egy román férfi, miután hasonló üzenetet kapott, elkeseredésében felakasztotta négyéves kisfiát, majd magával is végzett. Búcsúlevele szerint nem tudta elviselni a gondolatot, hogy évekre börtönbe menjen.[98]

A zsarolóprogramoknak alapvetően két fajtájuk létezik: *1.* az úgynevezett *locker*ek, amelyek csak kizárják a felhasználót; valamint *2.* a *cryptoware*-ek, amelyek titkosítják is a merevlemez tartalmát, így már nem egyszerű visszaszerezni az irányítást a számítógép felett.[99]

Az első zsarolóprogram a Gpcode volt, amelyet 2004-ben fejlesztettek ki Oroszországban. Ezt követte a fájlokat archiváló Cyrip, majd jött a Krotten, amely a regisztrációs adatbázist is átírta. 2008-ban érkezett a Gpcode továbbfejlesztett változata, amely nagyon jó titkosítást használva rejtette el a fájlokat. A fejlődés következő lépései az MBR *ransomware*-ek voltak, amelyek már az úgynevezett *master boot record*ot írták át, a merevlemeznek azt a részét, amely az operációs rendszer betöltéséért felel. Ezért lényegében el sem indult addig a gép, amíg a sértettek nem fizettek.[100]

Az online zsarolás csúcsát a CTB-locker nevű cryptolocker testesíti meg, mert nemcsak titkosítja a fájlokat, hanem az elkövetők az anonimitást biztosító TOR hálózat mögül kommunikálnak a sértettekkel, ami miatt mind őket, mind az általuk használt szervereket nagyon nehéz felderíteniük a hatóságok-

nak. A program testre szabott üzeneteket küld a sértetteknek anyanyelvükön, akik emiatt könnyebben tesznek eleget az elkövetők követelésének: fontos adataik visszaszerzése érdekében bitcoinban fizetnek. Így a tranzakciókat sem egyszerű lekövetni.[101]

A BTC-tranzakciók nyomon követése és a bitcoin biztosítása

A block-chain analízis

A BTC megtalálásának leghatékonyabb módja, ha valamilyen módon sikerül megismerni az elkövetőknél lévő privát kulcsokat. Az elkövetők megtalálása azonban ehhez képest még bonyolultabb feladat. Annak érdekében, hogy a bitcoinhálózaton zajló titkosított és anonim tranzakciókat, illetve azok adatait meg lehessen ismerni, szükség van egy olyan módszerre, amely a nyilvános adatbázisként működő blokkláncot elemzi és értelmezi. Ezt nevezzük block-chain analízisnek, e módszer azon alapul, hogy valamely, a láncolatban részt vevő személy nyilvános kulcsának birtokosa ismertté válik, ezáltal a hozzá kapcsolódó további személyek kiléte is megállapítható. Ez az új tudományterület, amelyet már az igazságszolgáltatásban is alkalmaznak, segít mindezt megvilágítani.[102]

Pál Tamás elmondása szerint a BTC-t érintő ügyekben a bűnüldözés számára elsősorban a régi és az új iskola ötvözése, tehát a hagyományos felderítő tevékenység modern informatikai eszközökkel történő megtámogatása vezethet eredményre kitartó elemző munkával, adatgyűjtéssel és fedett nyomozók alkalmazásával, amit a hivatkozott Silk Road esete is igazolt az Egyesült Államokban. A hatóságok számíthatnak emellett cégek és magánszemélyek segítő támogatására, akik block-chain elemző szoftvereket fejlesztenek. Ilyen program indult például az osztrák–német egyetemi és kormányzati együttműködés keretében Bitcrime projekt[103] elnevezéssel.

A bitcoin biztosítása

A BTC biztosítása elsősorban lefoglalással történik, hiszen a bitcoin – információs rendszerben tárolt adat lévén – elvileg lefoglalható a Be. 151. § (2) bekezdése alapján.

A probléma azonban abban rejlik, hogy a lefoglalás elsődleges tárgya csak dolog lehet, míg maga a lefoglalás a dolog birtoklásának ideiglenes elvonását jelenti. A lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének,

nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról szóló 11/2003. (V. 8.) IM–BM–PM együttes rendelet 67. § (1) bekezdésére tekintettel az elektronikus adat megőrzésének biztosítása másolással, illetve lementéssel lehetséges. Szathmáry Zoltán szerint a fizikai dolgok lefoglalásának megfelelő eljárás valójában az adat áthelyezése lenne, azaz törlése az eredeti tárhelyről és rögzítése egy új tárhelyen. A tulajdonos BTC feletti rendelkezési jogát elméletileg fel lehet függeszteni, de nem a privát kulcs biztosításával, illetve a wallet.dat fájl áthelyezésével, hanem csak tranzakció révén[104]. Az ilyen módon történő lefoglalás eredményessége azonban nagyban függ a bitcointulajdonos együttműködésétől. Ezért Szathmáry szerint indokolt lenne tisztázni a bitcoin helyzetét a magyar jogrendszerben, és ennek tükrében felülvizsgálni a büntetőeljárásban alkalmazható kényszerintézkedéseket, figyelemmel a biztosított adatok integritása megőrzésének követelményére és a bizonyítás eredményességének igényére.[105]

A gyakorlatban a bűnüldöző szervek helyi és nemzetközi szinten is számos módszert és protokollt dolgoztak ki a bitcoinnal kapcsolatos kényszerintézkedések metodikájára. Ezek bemutatásától azonban a jelenleg zajló és a jövőben folytatandó nyomozások sikerességének érdekében el kell tekintenem.[106]

Zárszó

A munkám során érintett kérdések kapcsán tanulságként az szűrhető le, hogy a bitcoin létező jelenség, amely hatással van a XXI. század emberének életére – nemcsak a széles körű informatikai tudás birtokában lévő nyugati társadalmakban, hanem már Magyarországon is. Az eddigi tendenciák alapján azt lehet mondani, hogy a bitcoin világszerte egyre ismertebb, és mint ilyen, hosszú távon fokozatosan a mindennapjaink részévé válhat.

Jelenleg azonban véleményem szerint elsődlegesen arra kell felhívni a figyelmet össztársadalmi szinten, hogy a BTC milyen veszélyeket rejt magában, hogyan hozható összefüggésbe a bűnelkövetéssel és így az áldozattá válással. Ebben a megközelítésben Magyarország szerencsére nem tekinthető célországnak. Ugyanakkor fontos, hogy az állampolgárok tisztában legyenek azzal, hogy mivel kerülhetnek szembe, ha az internetet óvatlanul használják, és a szakemberek készüljenek fel arra, hogy hamarosan Magyarországon is indulhat olyan büntetőügy, amelyben bitcoin a visszaélés tárgya.

IRODALOM

A Nemzeti Nyomozó Iroda nyomoz a Fideszt megfenyegető Anonymous-videó miatt. *Index.hu,* 2015. december 29. http://index.hu/belfold/2015/12/29/a_nemzeti_nyomozo_iroda_nyomoz_a_fideszt_megfenyegeto_anonymus-video_miatt/?token=b00c43ef2daca087daf02e3d04e98b8f

Az FBI lecsapott a web sötét oldalára. *Index.hu,* 2013. október 3. http://index.hu/tech/2013/10/03/az_fbi_lecsapott_a_web_sotet_oldalara/

Bakó Tamás: Bitcoin hálózatok elemzése. Szakdolgozat, Budapest, 2015 https://www.cs.elte.hu/blobs/diplomamunkak/msc_actfinmat/2015/bako_tamas.pdf

Berkes György (szerk.): Magyar Büntetőjog. Kommentár a gyakorlat számára. 2. kiadás. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2008

Cseh Gergely: A közösségi portálok árnyoldalai. *Infokommunikáció és Jog,* 2013/2.

Dzindzisz Magdalena: Lerohanták a bitcoin feltételezett alapítójának házát. *Index.hu,* 2015. december 9. http://index.hu/tech/2015/12/09/lerohantak_a_bitcoin_feltetelezett_alapitojanak_hazat/

Életfogytiglanit kapott a Silk Road alapítója. *Index.hu,* 2015. május 30. http://index.hu/tech/2015/05/30/eletfogytiglanit_kapott_a_silk_road_alapitoja/

Elfogták a magyar Anonymous 16 éves vezetőjét. *HVG.hu,* 2012. szeptember 8. http://hvg.hu/tudomany/20120908_Elfogtak_a_magyar_Anonymous_16_eves_vezet

Elítélték a Silk Road alapítóját. *Origo.hu,* 2015. február 5. http://www.origo.hu/techbazis/20150205-eliteltek-a-silk-road-alapitojat.html

Eszteri Dániel: A World of Warcraft-tól a Bitcoin-ig: Az egyén, a gazdaság és a pénz helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben. Doktori értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2015 http://ajk.pte.hu/files/file/doktori-iskola/eszteri-daniel/eszteri-daniel-muhelyvita-ertekezes.pdf

Ezért nem érdemes bitcoinnal kereskedni. *Privátbankár.hu,* 2014. április 22. http://m.privatbankar.hu/cikk/ezert-nem-erdemes-bitcoinnal-kereskedni-268109

Fehér Katalin: A virtuális valóság elmélete és gyakorlata. *Médiakutató,* 2003. nyár. http://www.mediakutato.hu/cikk/2003_02_nyar/06_virtualis_valosag/02.html

Hegyeshalmi Richárd: Magyarul is terjed a híres zsaroló vírus. *Index.hu,* 2014. március 20. http://index.hu/tech/2014/03/20/magyarul_is_terjed_a_hires_zsarolovirus/

Ibolya Tibor: A „torrentrazziák" büntetőjogi megítélése. http://ibolyatibor.atw.hu/Sajat/7.pdf

Laczi Beáta: A számítógép és a büntetőjog. *Magyar Jog,* 2001/3.

Lakatos Alexandra Anna: Az interneten elkövetett rágalmazás és becsületsértés egyes kérdései. http://www.mabie.hu/cikkek-tanulmanyok

Laza Bálint: Bejártuk a web sötét oldalát. *Index.hu,* 2013. január 29. http://index.hu/tech/2013/01/29/bejartuk_a_web_sotet_oldalat/

Laza Bálint: Megalakult a Nemzeti Kibervédelmi Intézet. *Index.hu,* 2015. október 1. http://index.hu/tech/2015/10/01/itt_a_nemzeti_kibervedelmi_intezet/

Laza Bálint: Gyerekpornót nézett? Fizessen! *Index.hu,* 2015. december 18. http://index.hu/tech/2015/12/18/gyerekpornot_nezett_fizessen/

Nagy Zoltán: A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról de lege lata, de lege ferenda. *Belügyi Szemle,* 1999/11.

Nagy Zoltán András: Bűnözés Magyarországon. Informatikai bűncselekmények. *Magyar Tudomány,* 2001/8. http://www.matud.iif.hu/01aug/nagyz.html

Onymous akció. *Hirpress.hu,* 2014. november 12. http://hirpress.hu/index.php?pg=cikk&id=9772

P., J: Virtual Currency. Bits and bob. *The Economist,* June 13, 2011. http://www.economist.com/blogs/babbage/2011/06/virtual-currency

Parti Katalin: Az iskolai online bántalmazás felmérése és komplex kezelése a TABBY in Internet nemzetközi keretében. *Infokommunikáció és Jog,* 2012/5–6.

Satoshi, Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. http://bitcoin.org/bitcoin.pdf

Szathmáry Zoltán: A számítástechnikai bűncselekmények és rendszertani elhelyezésük. *Jogtudományi Közlöny,* 2012. április

Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. *Magyar Jog,* 2015/11.

Szathmáry Zoltán: Bűnözés az információs társadalomban. Az információs társadalom devianciái. *Infokommunikáció és Jog,* 2008/26.

Takács Tibor (szerk.): Az informatikai jog nagy kézikönyve. CompLex Kiadó, Budapest, 2009

Vámosi Gergő: Bűntény is lehet a netes gúnyolódásból. *[origo],* 2010. március 25. http://www.origo.hu/techbazis/internet/20100325-cyberbullying-artalmatlannak-latszo-eroszak-a-kiberterben.html

Vírust kapott a számítógépe, megölte a gyerekét. *Index.hu,* 2014. március 14. http://index.hu/tech/2014/03/14/virust_kapott_a_szamitogepe_megolte_a_gyereket/

LÁBJEGYZETEK

1 Lakatos Alexandra Anna: Az interneten elkövetett rágalmazás és becsületsértés egyes kérdései. http://www.mabie.hu/cikkek-tanulmanyok

2 Nagy Zoltán előadása a PTE infokommunikációs szakjogászi képzés 2013–2014-es tanév első félévében, Budapesten.

3 Az első számítógépes bűncselekmény 1959-re nyúlik vissza, amikor az egyesült államokbeli Walston and Co. alelnöke 250 ezer amerikai dollárt sikkasztott hamis lyukkártyák segítségével. In: Nagy Zoltán: A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról de lege lata, de lege ferenda. Belügyi Szemle, 1999/11. Idézi Laczi Beáta: A számítógép és a büntetőjog. Magyar Jog, 2001/3., 138. o.

4 Laczi Beáta: i. m. 138. o.

5 Szathmáry Zoltán: A számítástechnikai bűncselekmények és rendszertani elhelyezésük. Jogtudományi Közlöny, 2012. április, 170. o.

6 Uo.

7 Laczi Beáta: i. m. 139. o.

8 Ennek a társadalomtípusnak a sajátossága az információ és az információtechnológia központi szerepe. https://hu.wikipedia.org/wiki/Információs_társadalom_(fogalom)

9 Szathmáry Zoltán: Bűnözés az információs társadalomban. Az információs társadalom devianciái. Infokommunikáció és Jog, 2008/26., 154–157. o.
10 A büntető törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.).
11 Azokat a deliktumokat értjük ezen, amelyek egy számítástechnikai rendszerrel vagy számítástechnikai adattal hozhatók kapcsolatba oly módon, hogy az elkövetés eszközeként jelennek meg, vagy a bűncselekmény elkövetési tárgyai. In: Takács Tibor (szerk.): Az informatikai jog nagy kézikönyve. CompLex Kiadó, Budapest, 2009, 547. o.
12 Uo.
13 Peszleg Tibor előadása a PTE infokommunikációs szakjogászi képzés 2013–2014-es tanév első félévében, Budapesten.
14 Ennek kapcsán manapság leginkább a fájlcserélő programokról (torrent, BitTorrent) hallhatunk. In: Ibolya Tibor: A „torrentrazziák" büntetőjogi megítélése. http://ibolyatibor.atw.hu/Sajat/7.pdf
15 Például szerzői vagy szerzői joghoz kapcsolódó jogok megsértése (Btk. 385. §), védelmet biztosító műszaki intézkedés kijátszása (Btk. 386. §).
16 Btk. 204. §
17 Btk. 335. §
18 Például személyes adattal visszaélés (Btk. 219. §), zaklatás (Btk. 222. §), rágalmazás (Btk. 226. §), a becsület csorbítására alkalmas hamis hang- vagy képfelvétel nyilvánosságra hozatala (Btk. 226/B §), becsületsértés (Btk. 227. §), kegyeletsértés (Btk. 228. §)
19 Btk. 11. §
20 Btk. 342. §
21 Btk. 176–177. §
22 Btk. 373. §
23 A számítógép elterjedése óta vannak, akik olyan adatállományokhoz kívánnak hozzáférni, amelyekhez hiányzik vagy nem elégséges a belépési jogosultságuk (hacking). A leghírhedtebb hacker Kevin Mitnick (alvilági nevén Condor), akit többször ítéltek el különböző elektronikai bűncselekményekért. In: Nagy Zoltán András: Bűnözés Magyarországon. Informatikai bűncselekmények. Magyar Tudomány, 2001/8. http://www.matud.iif.hu/01aug/nagyz.html
24 Btk. 375. §
25 Btk. 392. §
26 Btk. 386. §
27 Btk. 422. §
28 Btk. 423. §
29 Btk. 424. §
30 Cseh Gergely: A közösségi portálok árnyoldalai. Infokommunikáció és Jog, 2013/2., 91. o.
31 A felhasználók Facebook-interakciója 2014-ben: 201 milliárd ismeretségi kapcsolat, hatmilliárd lájk naponta, négyszázmilliárd megosztott fotó, 7,8 billió elküldött üzenet. https://hu.wikipedia.org/wiki/Facebook
32 Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3. § 3. pontja alapján különleges személyes adat.
33 Cseh Gergely: i. m. 92. o.
34 https://www.facebook.com/policies
35 https://www.facebook.com/communitystandards
36 Idetartozik például az erőszak és fenyegetés, a durva erőszak, a megfélemlítés és zaklatás, a gyűlöletbeszéd, a meztelenség és pornográfia, a személyazonosság, az adatvédelem és a szellemi tulajdon megsértése, az adathalászat és a kéretlen tartalmak elküldése.
37 Ezen a minél megfejthetetlenebb jelszót értjük, amelyben számok, szimbólumok, illetve kis- és nagybetűk szerepelnek.
38 Cseh Gergely: i. m. 93. o.

39 A zaklatás közvádas bűncselekmény, amelynek magánindítványra büntethető elkövetője rendszeres kapcsolat kialakítására törekszik a sértettel annak akarata ellenére, a háborgatás rendszeres vagy tartós, akár személyesen, akár valamely telekommunikációs eszköz igénybevétele útján (Btk. 222. §).

40 http://hu.wikipedia.org/wiki/Cyberbullying

41 Vámosi Gergő: Büntény is lehet a netes gúnyolódásból. [origo], 2010. március 25. http://www.origo.hu/techbazis/internet/20100325-cyberbullying-artalmatlannak-latszo-eroszak-a-kiberterben.html

42 Uo.

43 2011-ben indult a TABBY (Threat Assessment of Bullying Behavior) in Internet nevű nemzetközi projekt öt ország (Olaszország, Görögország, Ciprus, Bulgária és Magyarország) részvételével. Témája a gyermekek közti internetes bántalmazás (cyberbullying) volumenének felmérése és komplex kezelése. In: Parti Katalin: Az iskolai online bántalmazás felmérése és komplex kezelése a TABBY in Internet nemzetközi keretében. Infokommunikáció és Jog, 2012/5–6., 224–226. o.

44 Uo.

45 Eszteri Dániel: A World of Warcraft-tól a Bitcoin-ig: Az egyén, a gazdaság és a pénz helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben. Doktori értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2015, 15–17. o. http://ajk.pte.hu/files/file/doktori-iskola/eszteri-daniel/eszteri-daniel-muhelyvita-ertekezes.pdf

46 Olyan szoftverek tartoznak ide, mint a népszerű World of Warcraft, a Second Life, a Lineage II, az Eve Online, vagy akár az ingyenes Farmville is.

47 Fehér Katalin: A virtuális valóság elmélete és gyakorlata. Médiakutató, 2003. nyár. http://www.mediakutato.hu/cikk/2003_02_nyar/06_virtualis_valosag/02.html. Idézi Eszteri Dániel: i. m.

48 Ilyen például a szerepjáték során küldetések teljesítésével szerzett aranytallér vagy más jutalom.

49 Eszteri Dániel: i. m. 93–94. o.

50 Az elnevezés vonatkozik a fizetőeszközt kezelő nyílt forráskódú szoftverre és az azzal létrehozott elosztott hálózatra is. https://hu.wikipedia.org/wiki/Bitcoin

51 A Wired és a Gizmodo nemrég publikált írásai után jelenleg azt feltételezik, hogy Nakamoto Szatosi azonos egy Craig Wright nevű ausztrál férfival, aki 2014-ben jelentette be, hogy szeretné megalapítani a világ első bitcoinbankját. Dzindzisz Magdalena: Lerohanták a bitcoin feltételezett alapítójának házát. Index.hu, 2015. december 9. http://index.hu/tech/2015/12/09/lerohantak_a_bitcoin_feltetelezett_alapitojanak_hazat/

52 Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. http://bitcoin.org/bitcoin.pdf

53 Az informatikai hálózat végpontjai közvetlenül egymással kommunikálnak, központi kitüntetett csomópont (szerver) nélkül. https://hu.wikipedia.org/wiki/Peer-to-peer

54 Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. Magyar Jog, 2015/11., 6. o.

55 A kriptográfia elsősorban egy informatikai tudományág, amely a rejtjelezéssel, titkosírásokkal, kódolásokkal, azok előállításával és megfejtésével foglalkozik. Ennek segítségével jött létre az a bonyolult algoritmus, amely az első decentralizált kriptovaluta, a bitcoin megszületését eredményezte 2009. január 3-án. http://onecoinhungary.webnode.hu/a-cryptovaluta-tortenete/

56 Szathmáry Zoltán (2015): i. m. 6. o.

57 https://hu.wikipedia.org/wiki/Bitcoin

58 A jogi fogalmat az Európai Unió területére kiterjedő hatállyal a 2009/110/EK irányelv, Magyarországon a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény (Hpt.) 6. § (1) bekezdésének 16. pontja határozza meg.

59 A hitelintézetek állami felügyelete, amelynek célja a prudenciális (a pénzügyi kockázatot minimalizáló) szempontok érvényesítése a bankok gazdálkodásában, valamint a pénzügyi válságok kialakulásának megakadályozása. http://www.mimi.hu/gazdasag/prudencialis_felugyelet.html

60 Eszteri Dániel: i. m. 123–124. o.
61 Szathmáry Zoltán (2015): i. m. 8–9. o.
62 http://www.mnb.hu/archivum/Felugyelet/root/fooldal/topmenu/sajto/sajtokozlemenyek/bitcoin_kozl
63 Szathmáry Zoltán (2015): i. m. 9. o.
64 Uo. 7. o.
65 Ezt szintén bitcoinnak hívjuk.
66 https://bitcoin.org/en/
67 Eszteri Dániel: i. m. 126–129. o.
68 A biztonságot digitális aláírások és az úgynevezett proof-of-work rendszer adja, amely hasonlatos a fájlok megosztására használható BitTorrent technológiához (https://hu.wikipedia.org/wiki/Bitcoin). A proof-of-work egy olyan számítástechnikai validáló rendszer, amelyben bármilyen művelet végrehajtásának feltétele valamilyen számításigényes feladat elvégezése. Ez akkor működik hatékonyan, ha egy bizonyos aszimmetriát követ. Idézi Bakó Tamás: Bitcoin hálózatok elemzése. Szakdolgozat, Budapest, 2015. 9. o.
https://www.cs.elte.hu/blobs/diplomamunkak/msc_actfinmat/2015/bako_tamas.pdf
69 Eszteri Dániel: i. m. 126–129. o.
70 Például 1HCA3fcadYRQk5Sm3WGD2CPxsZqhdRXTY9. Uo.
71 J. P.: Virtual Currency. Bits and bob. The Economist, June 13, 2011.
http://www.economist.com/blogs/babbage/2011/06/virtual-currency Idézi Eszteri Dániel: i. m. 126–129. o.
72 Szathmáry Zoltán (2015): i. m. 7. o.
73 J. P.: i. m. Idézi Eszteri Dániel: i. m. 126–129. o.
74 Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.) hatálya alá tartozó szolgáltatók, továbbá a távközlési szolgáltatók az előfizetésre és a kommunikációra vonatkozó adatokat kötelesek megőrizni az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban: Eht.) 159/A § (1) bekezdés a)–c) és d)–k) pontjai alapján. Az első körbe tartozó szolgáltatók az általuk kezelt adatokat csak addig őrizhetik meg, amíg a szerződés meg nem szűnt, illetve a számlázás meg nem történt. Utóbbiaknál az adatmegőrzési kötelezettség egy évre, sikertelen hívások esetén fél évre terjed ki.
75 Számítástechnikai rendszer minden olyan berendezés, amely közvetlen emberi beavatkozás nélkül (automatikusan) végez adatfeldolgozást. Idetartoznak a számítástechnikai adatfeldolgozásra épülő memóriával bíró olyan egységek is, amelyek hagyományosan nem jelentenek számítógépet (például közcélú távbeszélő szolgáltatás, mobiltelefon-szolgáltatás igénybevételére szolgáló elektronikus kártyák, számítástechnikai berendezések felhasználásával működő hírközlési és telekommunikációs rendszerek). Berkes György (szerk.): Magyar Büntetőjog. Kommentár a gyakorlat számára. 2. kiadás. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2008, 944. o.
76 Peszleg Tibor előadása a PTE infokommunikációs szakjogászi képzés 2013–2014-es tanév első félévében, Budapesten.
77 https://en.wikipedia.org/wiki/Cyber-attack
78 A Készenléti Rendőrség szervezete 2012. szeptember 1-jén bővült ki a Nemzeti Nyomozó Irodával, amely a Készenléti Rendőrség parancsnokának közvetlen irányítása alá tartozó országos illetékességű, igazgatóság jogállású, bűnügyi feladatokat ellátó szervezeti egység. http://www.police.hu/a-rendorsegrol/testulet/teruleti-szervek/keszenleti-rendorseg
79 Idetartoznak a BTC-vel elkövetett bűncselekmények is.
80 E két területtel a Budapesti Rendőr-főkapitányságon belül a számítógépes bűnözés elleni alosztály, valamint a gyermek- és ifjúságvédelmi osztály foglalkozik (Pál Tamással folytatott interjú). A magyarországi kiberbiztonsági szervezetrendszert a 2015. október 1-jén megalakult Nemzeti

Kibervédelmi Intézet koordinálja. Laza Bálint: Megalakult a Nemzeti Kibervédelmi Intézet. Index.hu. 2015. október 1. http://index.hu/tech/2015/10/01/itt_a_nemzeti_kibervedelmi_intezet/

81 OSINT: Open Source Intelligence. http://kereses.blog.hu/2015/10/21/ismet_open_source_intelligence_osint_konferencia

82 https://hu.wikipedia.org/wiki/Anonymous_(csoport)

83 Elfogták a magyar Anonymous 16 éves vezetőjét. HVG.hu, 2012. szeptember 8. http://hvg.hu/tudomany/20120908_Elfogtak_a_magyar_Anonymous_16_eves_vezet

84 A Nemzeti Nyomozó Iroda nyomoz a Fideszt megfenyegető Anonymous-videó miatt. Index.hu, 2015. december 29. http://index.hu/belfold/2015/12/29/a_nemzeti_nyomozo_iroda_nyomoz_a_fideszt_megfenyegeto_anonymus-video_miatt/?token=b00c43ef2daca087daf02e3d04e98b8f

85 Onymous akció. Hirpress.hu, 2014. november 12. http://hirpress.hu/index.php?pg=cikk&id=9772

86 Ilyen például a Kaspersky Lab, amely a világ legnagyobb, magánkézben lévő informatikai biztonsági vállalataként bűnüldöző szervekkel is együttműködik a kiberbűnözők elleni harcban. http://www.kaspersky.hu/

87 https://www.europol.europa.eu/ec3

88 Ezért nem érdemes bitcoinnal kereskedni. Privátbankár.hu, 2014. április 22. http://m.privatbankar.hu/cikk/ezert-nem-erdemes-bitcoinnal-kereskedni-268109

89 Laza Bálint: Gyerekpornót nézett? Fizessen! Index.hu, 2015. december 18. http://index.hu/tech/2015/12/18/gyerekpornot_nezett_fizessen/

90 Laza Bálint: Bejártuk a web sötét oldalát. Index.hu, 2013. január 29. http://index.hu/tech/2013/01/29/bejartuk_a_web_sotet_oldalat/

91 Az FBI lecsapott a web sötét oldalára. Index.hu, 2013. október 3. http://index.hu/tech/2013/10/03/az_fbi_lecsapott_a_web_sotet_oldalara/

92 A Pál Tamással folytatott interjú alapján.

93 http://edition.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/

94 Az ügyészség drogkereskedelemmel, pénzmosással és számítógépek feltörésével vádolta. http://www.portfolio.hu/gazdasag/lecsapott_az_fbi_a_silk_roadra.190032.html

95 Elítélték a Silk Road alapítóját. Origo.hu, 2015. február 5. http://www.origo.hu/techbazis/20150205-eliteltek-a-silk-road-alapitojat.html ; Életfogytiglanit kapott a Silk Road alapítója. Index.hu, 2015. május 30. http://index.hu/tech/2015/05/30/eletfogytiglanit_kapott_a_silk_road_alapitoja/

96 Az úgynevezett police ransomware Angliában, illetve Hollandiában indult el, azóta hullámokban jelenik meg. A Pál Tamással folytatott interjú alapján.

97 Hegyeshalmi Richárd: Magyarul is terjed a híres zsaroló vírus. Index.hu, 2014. március 20. http://index.hu/tech/2014/03/20/magyarul_is_terjed_a_hires_zsarolovirus/

98 Vírust kapott a számítógépe, megölte a gyerekét. Index.hu, 2014. március 14. http://index.hu/tech/2014/03/14/virust_kapott_a_szamitogepe_megolte_a_gyereket/

99 Laza Bálint: Gyerekpornót nézett? Fizessen! Index.hu, 2015. december 18. http://index.hu/tech/2015/12/18/gyerekpornot_nezett_fizessen/

100 Uo.

101 Uo.

102 http://www.coindesk.com/what-block-chain-analysis-tells-bitcoin/

103 https://www.bitcrime.de/

104 Az átutalás rendőrségi pénztárcába történik, ahonnan a bitcoint értékesítik. Ekkor azonban kockázatot jelent a BTC árfolyam-ingadozása, amit – szabályozó hatalom híján – önmagában a kereslet és a kínálat határoz meg. A Pál Tamással folytatott interjú alapján.

105 Szathmáry Zoltán (2015): i. m. 9–11. o.

106 A Pál Tamással folytatott interjú alapján.