dr. Gyaraki Réka r. fhdgy (PTE-ÁJK Doktori Iskola III. évfolyam)
BRFK

A számítógépes bűnözés elleni harc az új büntetőtörvénykönyvvel

Az információs rendszerek fejlődését az elmúlt években alkalmazzák az élet majd minden területén. A kereskedelemben, a kommunikációban, politikában, oktatásban és még sorolhatnánk, hová is gyűrűzött be az internet alkalmazás. A világháló népszerűsödésével együtt megjelent a számítógépes bűnözés illetve a számítógépes bűnözői csoportok.
Az Európai Unió több kerethatározatában, irányelvében felhívta a tagállamok figyelmét az internet veszélyeire, valamint egy közös cselekvési program kidolgozására. Felismerték továbbá azt is, hogy nem elég, ha tagállami szinten kerül sor a világháló biztonságának illetve az azt támadó szervezetek elleni biztonságpolitika kialakítására.

A Brüsszelben kiadott 2007.05.27-i bizottsági közlemény[1] rámutatott arra, hogy *a számítógépes bűncselekmények száma folyamatosan növekszik és bűnözés egyre kifinomultabbá és nemzetközibbé válik, a számítógépes bűnözésben egyre inkább részt vesznek a szervezett bűnözői csoportok az első két pont ellenére a bűnüldözési együttműködés alapján folytatott európai büntetőeljárások száma nem növekszik.*

Az internetes bűncselekmények terjedése miatt sürgős intézkedéseket kell hozni a nemcsak a tagállamoknak, hanem valamennyi államnak, annak érdekében, hogy hatékonyabban és gyorsabban fel tudjanak lépni a bűnözőkkel szemben.

A gyorsaság miatt, mivel ez az egyik jellemzője a számítógépes bűncselekményeknek, hatékonyan csak azonnali reagálással lehet küzdeni. Mivel állandó problémát okoz, hogy nem vagy nem megfelelően implementálták a jogszabályokat az aláíró országok, így előfordulhat, hogy egy-egy bűncselekmény nem, vagy nem megfelelően lesz szankcionálva.
A gyorsaság mellett a nemzetközi jelleg és a határok nélküliség is kedvez a bűnözőknek. Ha az országok között joghatósági vita alakul ki, annak tisztázása alatt bizonyítékok semmisülhetnek meg, elkövetők tűnhetnek el, ami az eljárás eredménytelen befejezését jelentheti.

Magyarországon még az 1978. évi IV. törvény a Büntető Törvénykönyv van hatályba, amiben kevés utalás van arra, hogy 2001. november 23-án mi is aláírtuk a Cybercrime, vagyis a Számítógépes bűnözésről szóló Egyezményt.

A 2013. július 01-jén fog hatályba lépni és már tartalmaz az új Büntető Törvénykönyv, melyet a cikkemben sok helyen Tervezetként említek, az információs rendszer ellen,- illetve felhasználásával elkövetett bűncselekményeket.

Az elektronikus adat végleges hozzáférhetetlenné tétele[2]

A Tervezet új intézkedésként vezeti be az elektronikus adat véglegese hozzáférhetetlenné tételét, mivel az illegális adatok esetében nincs lehetőség arra, hogy blokkolják és ezáltal mások számára hozzáférhetetlenné tegyék a jogellenes tartalmakat.

[1] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak és a Régiók Bizottságának: A számítógépes bűnözés elleni küzdelemre vonatkozó általános politika felé
[2] új Btk. 77. §-a

A 2005/222/IB kerethatározata, az Európai Parlament és a Tanács 2011/92/EU irányelvének 25. cikke szerint a gyermekpornográfiát tartalmazó vagy azt terjesztő weboldalakon a tartalmat hozzáférhetetlenné kell tenni, azaz blokkolni kell.

Jelenleg egy ilyen tartalommal kapcsolatban nincs túl sok lehetősége a hatóságnak, hiszen egy illegális tartalom esetében csak kötelezni lehet az adott weboldal üzemeltetőjét, hogy a tiltott tartalmat távolítsa el az oldalról, illetve a Be. 158/A.§[3]-t, mint kényszerintézkedést alkalmazzon az adatok birtokosával, feldolgozójával vagy kezelőjével szemben. Az eljárási törvényünk lehetőséget ad arra, hogy a számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés következtében a megőrzésre kötelezett adatot a hatóság átvizsgálja és bizonyítékként használja fel. A kötelezett pedig köteles az adatot változatlan formában megőrizni. Ehhez az adathoz a kényszerintézkedés tartalma alatt csak az azt elrendelő hatóság vagy annak engedélyével az adat birtokosa vagy kezelője férhet hozzá.

A hozzáférhetetlenné tétel előnye lenne, hogy azoknál a tartalmaknál is lehessen alkalmazni, amiket külföldi szervereken tárolnak. Bár a jogszabályszöveg erről nem tesz említést, így akkor a korlátozás miatt csak Magyarországon nem lehetne az adatokhoz hozzáférni?! A hozzáférhetetlenné tételt követően pedig értesíteni kellene az adott államot, ahol feltehetőleg a szerver van.

Az indokolás a már általam is említett 2011/92/EU irányelv 25. cikkére hivatkozik,- ennek következtében szűken kell értelmezni-, csak a hazánkban üzemeltetett weboldal esetében lehetne megtenni a hozzáférhetetlenné tételt. Mivel az internetes bűncselekmények egyik jellemzője (amint már említettem), hogy határokon átnyúló, internacionális, és ennek következtében az elkövetők nem feltétlenül ugyanabban az országban tartózkodnak, ahol a feljelentést megteszik a hatóságoknál, így technikai, valamint jogi probléma is felmerülhet a blokkolással kapcsolatban.

Még egy kitételt tesz a törvény szövege: a végleges hozzáférhetetlenné tételt akkor is el kell rendelni, ha az elkövető gyermekkor, kóros elmeállapot vagy a törvényben meghatározott büntethetőséget megszüntető ok miatt nem büntethető[4], illetve megrovásban részesítették. A bekezdés szövege érthető, csak nem értelmezhető. Vagyis, megfordítva a gondolatmenetet, ha az illegális adatot- mondjuk pedofil képeket- olyan személy, aki nem áll a büntethetőség hatálya alatt, készítette, akkor az kevésbé okozott kárt annak a személynek, aki szerepel a képen, mintha olyan személy készítette volna, aki büntethető?!

Gyermekpornográfia

A jelenleg hatályos, és a 18. életévet be nem töltött személyekről készült pornográf felvétel készítése a *Btk. 204.§-a szerint a tiltott pornográf felvétellel való visszaélés* bűncselekménye. A tényállásban az elkövetési magatartások:

1. megszerzés
2. tartás
3. hozzáférhetővé tétel
4. forgalomba hozatal és
5. a nagy nyilvánosság számára hozzáférhetővé tesz

[3] 1998. évi XIX. törvény a büntetőeljárásról szóló törvény 158/A.§ - számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés

[4] 2012. évi C. tv. 77.§ (2) bekezdése

A még hatályban lévő deliktumot a Büntető Törvénykönyv Tervezete már a Gyermekpornográfia címre módosította, mivel a miniszteri indoklás szerint a hatályos törvényben a „visszaélés” kifejezés nem tükrözi a ténylegesen védett jogi tárgyat. Valamennyi nemzetközi egyezmény illetve uniós irányelv, vagy kerethatározat szintén a gyermekpornográfia kifejezést használja. Az alapvető elkövetések maradnak, vagyis: megszerez, tart, készít, kínál, átad, forgalomba hoz, kereskedik, nagy nyilvánosság számára hozzáférhetővé tesz.

A sértettek korhatára továbbra is a 18. életév. Egyetlen esetben tesz kivételt a jogalkotó, amikor 14 életévet be nem töltött személyekről pornográf felvétel készítéséhez, forgalomba hozatalához a kereskedelemhez szükséges vagy azt könnyítő feltételeket szolgáltat, azt biztosítja, úgy vétséget követ el. Igaz, amennyiben 18. életévet be nem töltött személyekkel kapcsolatban teszi meg ugyanezt a cselekményt, úgy már magasabb büntetési tételt állapít meg.

Véleményem szerint, amennyivel előbbre mutató a jelenleg hatályos, gyermekek sérelmére elkövetett visszaélés, úgy a Tervezet szabályozásában akkora változások nincsenek. Ha már tett a jogalkotó kísérletet arra vonatkozóan, hogy egy esetben az életkor nem a 18. életév, akkor épp a gyermekek szexuális felvilágosításával összefüggésben a 12. életévet be nem töltött személyek ellen elkövetett cselekményt súlyosabban kellene értékelni. Figyelemmel, hogy még az értelmük, a testi fejletlenségükről is sokkal inkább bizonyítható, hogy az elkövető szándéka kifejezetten a kiskorúról készült pornográf tartalmú képek készítése, megszerzése, tartása. Ne felejtsük el, hogy a pedofilok a képeket nem csak elkészítik, terjesztik, hanem azzal kereskednek is egymás között. Azaz, minél inkább látható, hogy a felvételen vagy műsorban szereplő személy gyermek, úgy annál többet kérhetnek érte.

A miniszteri indoklás tesz egy összehasonlítást a nemzetközi dokumentumokban szereplő követelmények (ezt angol és magyar nyelven sorolja fel) valamint a törvényben megjelenő fogalmak között. A táblázatban látható, hogy a törvény szövege szegényesebben lett megfogalmazva, mint a dokumentumokban illetve a fordításában. Ilyen például az „információs és kommunikációs technológia segítségével történő tudatos hozzáférés” (knowingly obtaining acess by means of information and communication technology), ami a törvényben egyszerűen a „tart” szóval helyettesítik. Ezt a kifejezést azért emelem ki, mert talán érthetőbbé tennék azok számára is a törvényt, akik nincsenek otthon a számítástechnika világában.

Tervezetben már értelmezik a pornográf jellegű műsort, valamint a pornográf jellegű felvételt.

A pornográf jellegű felvétel: videó-, film-, vagy fényképfelvételt, illetve más módon előállított képfelvételt ért, amely a nemiséget súlyosan szeméremsértő nyíltsággal, célzatosan a nemi vágy felkeltésére irányuló módon ábrázolja. A pornográf jellegű műsor: nemiséget súlyosan szeméremsértő nyíltsággal megjelenítő, célzatosan a nemi vágy felkeltésére irányuló cselekvésként vagy előadásként azonosítható[5].

Mindenképpen szerencsésnek tartom, hogy az új törvényszöveg megalkotásakor már figyelemmel voltak a vállalt kötelezettségekre, valamint a technológia fejlődésére.

[5] 2004. évi C. törvény 204.§ Gyermekpornográfia tényállásának miniszteri indokolása

A számítógépes csalás

A Cybercrime Egyezmény 2. cikke szerint bűncselekménynek kell minősíteni az aláíró tagállamoknak a jogosulatlan belépést, vagyis a számítástechnikai rendszerbe vagy annak bármely részébe történő jogosulatlan és szándékos belépést.
Ezen Egyezmény alapján, valamint az Uniós kerethatározat alapján, Magyarországon a Btk. 300/C.§-a a számítástechnikai rendszer és adatok elleni bűncselekmény tényállásának elkövetési magatartása a rendszerbe történő jogosulatlan belépés vagy a jogosultság kereteit túllépés, vagy azt megsértve a „bent maradás". A Btk. 300/C.§ (3) bekezdése a számítógépes csalást fogalmazza meg, hiszen a bekezdés a „jogtalan haszonszerzés" célzatával követi el a számítástechnikai rendszerbe történő adat bevitelt, az abban tárolt, feldolgozott, kezelt vagy továbbított adatot megváltoztatását, törlését, hozzáférhetetlenné tételét, vagy a rendszer működésének akadályozását.

Ugyanakkor a hagyományosnak nevezhető csalást a Btk. 318.§-a szabályozza. Mivel a csalás és a „számítógépes csalás" nincsenek alaki halmazatban, így egy-egy nyomozásnál szükséges az elhatárolása.

A két szakasz között Dr. Szathmáry Zoltán szerint a különbség, hogy a számítástechnikai rendszer az elkövetés, vagy a leleplezés eszköze-e. Valamint az, hogy az elkövető felhasználta-e a számítógépben rejlő lehetőséget és a úgy követte el a csalást, vagy a bűncselekmény elkövetése érdekében manipulálta az adatokat[6].
A Btk. Tervezete az Információs rendszer felhasználásával elkövetett csalás tényállását nevesíti meg. A miniszteri indokolás szerint lényegét tekintve megtartja a hatályos Btk. 300/C.§ (3)-(4) bekezdéseit. Tehát a számítógépes csalást az követi el, 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…*[7]

Azonban annyiban túlmutat már a Btk. 300/C.§ (3)- (4) bekezdésein, hogy a hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználást vagy az azzal történő fizetést is csalásnak minősíti az 5, bekezdésébe, amennyiben azzal kárt okoznak.
Itt épp ezért szükséges megemlíteni, hogy a jelenlegi büntető törvénykönyvünkben ez a cselekmény a Btk. 313/C. § (1) bekezdéshez hasonlít, így szükségessé vált, hogy a tényállást megváltoztassák. Ennek a módosítását a következő pontban fogom ismertetni.
A jogalkotók szerint azért volt erre a változtatásra szükség, mert az információs rendszer felhasználásával elkövetett, kárt okozó magatartások elsősorban vagyoni érdekeket sértenek.
A hatályos Btk.-nál már mondhatni korszerűbb a Tervezetben az információs rendszer felhasználásával elkövetett csalás tényállása.

Érdemes még megemlíteni azokat a csalásokat, amelyeket számítógépes környezetben követnek el[8].
Ilyen csalások:

1.) *az ún. előrefizetéses csalások (csak néhány példát említek: nigériai levelek, áruvásárlás-, szolgáltatás megrendelése hamis weboldalon, nyereményt ígérő kérdőív küldése, igénybe nem vett, nem létező Internet szolgáltatások kiszámlázása…stb).*

[6] Dr. Szathmáry Zoltán: Az alkotmányos büntetőjog és az információs társadalom doktori értekezés (2011.)
[7] 2012. évi C. törvény 375.§ (1) bekezdés az információs rendszer felhasználásával elkövetett csalás
[8] Dr. Nagy Zoltán András: Bűncselekmények számítógépes környezetben (Ad Librum kiadó, Budapest, 2009.) 143-152. oldal

2.) csalárd adománygyűjtések
3.) kattintásos csalás
4.) on-line aukciós csalás
5.) „betárcsázós csalás”

Azért említem meg ezeket a fent nevezett csalás típusokat, mert ezekben az esetekben a nyomozás „hagyományos” csalás elkövetésének tényállásában indul. A hatályos Btk nem, de az új Btk-ban a Csalás[9] tényállásának minősített eseteként említi például már akár a szabálysértési értékhatárra is elkövetett csalást, ha azt jótékony adománycélra követik is el.

Sajnos az adathalászatot, vagy a kéretlen levelek (Spam) küldését, amik ehhez a bűncselekményhez is hozzájárulnak, nem említi a törvény.

Készpénz- helyettesítő fizetési eszköz hamisítása és az azzal való visszaélés

A törvényalkotóknak figyelembe kellett venni, hogy egyre többen és gyakrabban használják a készpénzkímélő eszközt, a bankkártyát. Ennek egyre szélesebb körben történő felhasználása miatt a hatályos szabályozás nem biztosítja a plasztikkártyába vetett bizalmat. A pénzintézetek, valamint a természetes és jogi személyek sérelmére elkövetett a fent megnevezett bűncselekmények száma megnőtt. Az elkövetéshez használt technikai eszközök valamint az elkövetési módok skálája egyre tágabb.
A Tervezet a bűncselekményt elkövetők körét szélesítette, annyiban, hogy megtartotta a Btk. 313/B. § (1) bekezdését, de büntetni rendeli még azokat a személyeket is, akik a bankkártyán tárolt adatokat vagy az ahhoz kapcsolódó biztonsági elemeket rögzítik.
A cselekmény büntetendővé nyilvánításához nem szükséges a károkozás. Amennyiben megtörténik a vagyoni hátrány okozása, úgy az előbbiekben leírt, számítógépes csalás, vagyis az információs rendszer felhasználásával elkövetett csalás tényállása valósul meg.

A bankkártyával való visszaélésnek különböző módozatai vannak, amelyeket a törvényben leírt elkövetési magatartásokkal hasonlítok össze, így remélem, hogy egy megfelelő értelmezést kapunk a Tervezet szövegének megértéséhez:

- Az eredeti bankkártyákkal történő visszaélés. Az elkövető hamis adatokkal igényel bankkártyát, vagy lopott illetve talált bankkártyával követi el a cselekményt.
- A bankkártya adatainak - vagyis a plasztikkártyán lévő információk (név, szám, érvényességi idő)- manuális módon történő lemásolása.
- A másolás, melynek 3 típusa ismert: a kézben lévő ún. skimmerrel történő másolás, a POS terminálon és az ATM-es terminálon keresztül történő adatszerzés
- az adathalászat vagy Phising
- internetes vásárlások

A fenti elkövetési módok büntetendővé nyilvánítását a Tervezetben mind a 392.§, mind a 393.§ szakaszokban találjuk.
A hamisítást a törvény csak akkor nyilvánítja büntetendővé, ha a készpénz-helyettesítő fizetési eszköz készítése illetve az adatainak rögzítése felhasználás céljából történik.

A Tervezet Záró rendelkezésében a készpénz-helyettesítő fizetési eszköz valamint az elektronikus készpénz-helyettesítő fizetési eszköz fogalmát megadja. Utalva a hitelintézetekről szóló törvényben meghatározott fogalomra, valamint ezek mellett a kincstári

[9] új Btk. 373.§ csalás tényállása

kártya, elektronikus utalvány, utazási csekk, a váltó (bizonyos feltételek esetén). De csak abban az esetben használja a törvény a fogalmat, amennyiben annak másolása, meghamisítása illetve jogosulatlan felhasználása védett.

A visszaélés tényállása - bár itt a jogalkotó a tiltott pornográf felvétellel való visszaélés esetében kivette a visszaélés szót - már a hatályos Btk. 313/C.§-sal ellentétben az elkövetési magatartás olyan készpénz-helyettesítő fizetési eszköz mástól történő megszerzése, amelynek használatára nem vagy nem kizárólag jogosult, valamint a hamis vagy meghamisított, vagy jogtalanul megszerzett, vagy az azokon tárolt adatokat vagy az ahhoz kapcsolódó biztonsági elemek átadása, vagy az országba behozatala, kivitele.

Mivel ez a deliktum is számítógépes/ internetes bűncselekmények körébe tartozik, így az adatok országba történő behozatala, kivitele történhet virtuális módon is. Azaz nem véglegesen „megy" ki az adat az országból.

Készpénz-helyettesítő fizetési eszköz hamisításának elősegítése

A készpénz-helyettesítő fizetési eszköz hamisítása leginkább számítástechnikai berendezések útján történik. Az előző pontban felsorolt, a hitelintézetekről szóló törvényben meghatározott készpénz-helyettesítő fizetési eszközközöknek nemcsak a hamisítását, hanem azokon lévő adatok rögzítéséhez szükséges anyagot, eszközt, berendezést, program készítését, megszerzését, tartását, átadását…stb. bünteti.

A hatályos Btk. még csak a berendezés vagy számítógépes program készítését bünteti, míg a Tervezet már az adatok rögzítéséhez szükséges eszközök bármilyen formában történő megszerzését.

Ez a módosított tényállás már sokkal inkább figyelemmel van például a bankkártya hamisítás módszereire. Valamint a hatályos törvényi tényállásban a kereskedik szó helyett már az országba behozatalt nyilvánítja büntetendővé.

A készpénz-helyettesítő fizetési eszköznek nemcsak az minősül tehát, amikor hamis bankkártyát készítenek[10], hanem ezen túlmutatva már a különböző adatok megszerzéséhez szükséges számítógépes programok- így azok letöltése, továbbítása, terjesztése (a törvény szövegében a tartás szó utalhat erre) vagy különböző számítástechnikai rendszereken történő forgalmazása jelenti a cselekmény elősegítését.

Mivel sok esetben az elkövetők külföldi állampolgárok és a megszerzett adatokat, nem hazánkban, hanem más országban használják fel, adják el, illetve ezeket számítástechnikai rendszeren keresztül továbbítják.

A még hatályban lévő büntető törvénykönyvhöz képest már szigorítást is megfigyelhető, mégpedig akkor, ha bűnszövetségben vagy üzletszerűen követik el a cselekményt. Véleményem szerint általában nem egyedül követik el és nem egyszeri alkalommal történik, végzik el a cselekményt.

Sokkal inkább jellemző az elkövetőkre a bűnszövetség - hiszen alá-fölé rendeltség, illetve munkamegosztás tapasztalható az elkövetők között, valamint a rendszeres haszonszerzés a cél.

Információs rendszer vagy adat megsértése és az azt biztosító technikai intézkedés kijátszása

A Tervezet 423.§-a tartalmazza az információs rendszer vagy adat megsértése tényállását, mely lényegét tekintve megegyezik a hatályos Btk. 300/C. §-sal. A Tervezet megtartja a

[10] nem maga a kártya külső tulajdonságait másolják- így annak színe, a kibocsátó bank logója, jellegzetessége - hanem a kártya száma, lejárata, és a kártyabirtokos neve a fontos

jelenlegi elkövetési magatartásokat, viszont tekintettel van a technika gyors ütemű fejlődésére[11], valamint a 2005/222/IB tanácsi kerethatározatra, azaz súlyosbító körülményként értékeli, ha *jelentős számú rendszert érint"* valamint *közérdekű üzem ellen* követik el.

Az elkövetési magatartások tehát: az információs rendszerbe belépés és bent maradás, a működésének akadályozása, a meglévő adatok megváltoztatása, törlése, illetve hozzáférhetetlenné tétele. Ezek az elkövetések akkor jogellenesek, amennyiben az elkövetőnek nincs jogosultsága, vagy a jogosultsága kereteit túllépte, megsértette. Vagyis a hatályos szabályozáshoz képest ezen nem változtat.

Az információs rendszer védelmét biztosító technikai intézkedés kijátszása alatt a jelszó megszerzését, vagy az ahhoz szükséges technikai eszköz készítését, átadását, hozzáférhetővé tételét..stb. szankcionálja a törvény.

A Cybercrime Egyezmény Számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények Fejezetének 6. cikke- az Eszközökkel való visszaélés- alapján büntetendővé kell nyilvánítani a jelszó[12] egyszeri átadását is, de a Tervezet az ehhez szükséges eszköz birtoklását valamilyen ismeretlen okból nem bünteti.

Végszó

Az elkövetési magatartások: készítés, átadás, hozzáférhetővé tétel, megszerzés, forgalomba hozatal.
A számítástechnikai, vagy ahogy a törvény említi az információs rendszeren keresztül elkövetett bűncselekmények törvényi tényállásai szinte kivétel nélkül ugyanazok, pedig a magyar nyelv nemcsak szép szavakat, kifejezéseket alkotott, de sok angol szót is átvett, amivel az elkövetési magatartásokat pontosabban lehetett volna definiálni.

Összességében szerencsésnek tartom, hogy a jogalkotók újra gondolták a büntető törvénykönyvünk általános és különös részét. Bízom benne, hogy ennek segítségével mi bűnüldözők hatékonyabban tudjuk majd a munkánkat végezni.

Felhasznált irodalom

- Dr. Nagy Zoltán András: Bűncselekmények számítógépes környezetben (Ad Librum kiadó, Budapest, 2009.)
- 1978. évi IV. törvény a Büntető Törvénykönyv
- 2012. évi C. törvény az új Btk.
- Dr. Szathmáry Zoltán: Az alkotmányos büntetőjog és az információs társadalom doktori értekezés (2011.)
- 1998. évi XIX. törvény a büntetőeljárásról szóló törvény
- 2004. évi LXXIX törvény a Számítógépes Bűnözésről szóló Egyezmény

[11] 2012. évi C. törvény 423. § miniszteri indoklása
[12] jelszó: az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy azok kombinációjából álló bármely azonosító (2012. évi C. tv. 424.§ (3) bekezdése

Cím: 1042 Budapest, Árpád út 48-50 II. emelet 11. ajtó