MEZEI KITTI

A jogosulatlan belépés, avagy a hacking szabályozása a büntetőjogban

Általános bevezető

Az első büntetendő magatartás, amivel részletesen foglalkozom, a jogosulatlan belépés, más néven *„hacking”,* mely utóbbi elnevezés gyakran előfordul a nemzetközi és a hazai szakirodalomban egyaránt. A *hacker* kifejezést általában azokra az informatikai szakemberekre használják, akik kiemelkedően magas fokú szaktudással és gyakorlattal rendelkeznek. Az egyik legnépszerűbb nézet szerint a hackerek között különbséget lehet tenni aszerint, hogy milyen szándékkal törik fel a rendszert. Ez alapján beszélhetünk az úgynevezett *„white hat”* vagy fehér kalapos hackerekről, akik jóhiszeműen tesztelik az adott rendszer biztonságát és sebezhetőségét. Emellett vannak az úgynevezett *„black hat”* vagy fekete kalapos hackerek, illetve *„crackerek”,* akik többek között azért hatolnak be a rendszerbe, hogy kárt okozzanak, vagy hozzájussanak az értékes információkhoz. Végül az utolsó csoportot képezik az úgynevezett *„grey hat”* vagy szürke kalapos hackerek, akik nehezen behatárolható módon valahol az előző két csoport között helyezkednek el.

A bemutatott terminológiák használata azonban vitatható. Általában egyetértés van a tekintetben, hogy az etikus hackerek[1] tevékenysége a fehér kalapos csoportba tartozik, azonban nehezíti a helyzetet, hogy hiányzik ennek a megfelelő szabályozása, valamint nincs kialakítva egy széles körben elfogadott gyakorlata. Ennek ellenére a piacon már megjelentek különböző információbiztonsági cégek, amelyek kifejezetten ilyen képzést kínálnak.

[1] Steven Furnell: Hackers, viruses and malicious software. In: Jewkes–Yar (szerk.): Hackers, viruses and malicious software. Willan Publishing. 2010. 43–45. o.

Ezt a problémakört közelebbről megvizsgálva felmerül a kérdés, hogy a jogosultság hiánya esetén beszélhetünk-e egyáltalán etikus hackelésről. Steven Furnell rámutat, hogy a *„biztonság fejlesztése”* érdekében végzett hacking megítélése esetén a fő kérdés az, mi történik a megszerzett információval. Amennyiben ezt a hacker diszkréten bejelenti a cégnek, akkor az etikus hozzáállásnak tekinthető. Azonban ha a nagy nyilvánosság előtt tárja fel a biztonsági rést, akkor ez a részéről nehezen tekinthető etikusnak, különösen azért, mert ezzel felhívja figyelmet a rendszerben található hibára, de facto arra, hogy mások is használják ki a rendszer sebezhetőségét. Furnell szerint további megválaszolandó kérdésként merül fel, hogy egy diszkrét bejelentés esetén is etikusnak tekinthető-e, ha a rendszerbe valaki engedély nélkül belép, és mindezt úgy teszi, hogy más informatikai műveletet nem végez. Álláspontja szerint a hacker ebben az esetben is hátrányt okozhat a jogosulatlan hozzáféréssel anélkül, hogy a rendszerben bármit megváltoztatna vagy megzavarná annak a működését, ellenben például könnyedén láthat olyan szenzitív információt (például személyes adatot vagy üzleti titkot), amivel később visszaélhet.[2] Erre tekintettel a jogosulatlan belépés azon esetei, amelyek károkozási szándék nélkül történnek, jó példaként szolgálnak a szürke kalapos hackelésre. A fehér kalapos típus pedig kizárólag azokra az esetekre korlátozódik, amikor a hacker erre kifejezetten speciális vagy általános felhatalmazást kap. Ezért azok a személyek, akik csak saját elhatározásukból, jogosultság hiányában keresnek programhibákat vagy biztonsági réseket, nem tekinthetők etikus hackernek, hanem csak azok, akik valamilyen formában rendelkeznek jogosultsággal (például az információs rendszer tulajdonosa kifejezetten megbízza őket a rendszer tesztelésével és támadásával).

A jogosulatlan belépés megvalósulhat egyszerűen vagy összetettebb módon is, például ha az elkövetők egy számítástechnikai hálózatot használnak fel arra, hogy távoli hozzáférést szerezzenek, és ez gyakran különböző joghatóságok alá tartozó számítógépek közbeiktatásával történik. A hozzáférés megszerzése történhet alap felhasználói szintű műveletekkel, vagy úgynevezett *„root level access”,* illetve *„god level access”* szintűvel,

[2] Alisdair Gillespie: Cybercrime – Key Issues and Debates. Routledge. 2016. 44–45. o.

amikor ugyanazokkal a jogosultságokkal rendelkeznek, mint a rendszergazda, és ezáltal a rendszerben tárolt valamennyi adat elérhetővé válik számukra, sőt módosításokat hajthatnak végre, vagy akár (rosszindulatú) programokat futtathatnak.

A szoftverek gyors ütemű fejlesztése elkerülhetetlenül magában hordozza a programhibákat is, amiket az elkövetők gyakran kihasználnak, mielőtt még a szoftverfejlesztők észrevennék és kijavítanák ezeket. Ezek az úgynevezett nulladik napi (zero-day) támadások, amelyek a programkészítők és a felhasználók által még nem ismert olyan sebezhetőséget használnak ki, amelynek eredményeképpen könnyedén hozzáférhetnek az információs rendszerekhez.

Emellett gyakran olvashatunk a felhasználói fiókok (például e-mail, közösségi oldalak) feltöréséről szóló híreket, azonban érdemes felhívni a figyelmet arra, hogy a jogosulatlan belépések többségének célpontjai elsősorban a nagyobb cégek, gazdasági szereplők vagy állami szervek, és nem a magánszemélyek.

A jogosulatlan hozzáféréssel az elkövető célja továbbá az is lehet, hogy több számítógépet felhasználva a közbeiktatásuk révén elrejtse személyazonosságát, a bűncselekmény elkövetésének helyét, vagy éppen bűncselekmények elkövetésére használja, így gyermekpornográf tartalmakhoz való hozzáférésre, vagy spam küldésére, amire különösen alkalmasak a nyilvános wifihozzáférési pontok (hotspot).[3]

Megállapítandó, hogy az egyes hacking jellegű cselekmények mögött leggyakrabban a következő motivációk húzódnak: hozzáférés az információhoz, az adat megváltoztatása, illetve törlése, valamint az információs rendszer használata.[4] A jogosulatlan belépés további büntetendő magatartásokat segíthet elő, például az „ellopott" szenzitív adatokkal a sértetteket zsarolhatják. Más esetekben az adatokat további csalás jellegű magatartásokhoz használják fel, többek között adathalászathoz, vagy arra, hogy a

[3]Jonathan Clough: Principles of cybercrime. Cambridge University Press. 2014. 37. o.
[4] Clough: i. m. 33. o.

versenytársak bizalmas információkhoz férjenek hozzá. Az esetek többségében személyes, pénzügyi és egyészségügyi adatokat szereznek meg (például név és születési idő, telefonszámok, e-mail címek, felhasználói adatok,[5] jelszavak és bankkártya adatok). Az elkövetők ezeket gyakran nem a saját részükre szerzik meg, hanem azért, hogy később a Darknet-fórumokon értékesítsék[6].

A jogosulatlan belépés nemzetközi és uniós szintű szabályozása

A Budapesti egyezmény[7] értelmében a jogosulatlan belépés bűncselekményét követi el, aki a számítástechnikai rendszerbe vagy annak bármely részébe (legyen többek között az tárolt vagy forgalmi adat, mappák, egyéb komponensek, adathordozók) jogosulatlanul és szándékosan belép. Azonban nem minősül jogosulatlan belépésnek például egy e-mail küldés vagy fájltovábbítás, ellenben bűncselekményt valósít meg, aki olyan számítógépbe lép be, amely a nyilvános telekommunikációs hálózatra csatlakozik, vagy ugyanazon hálózaton belül található, mint például egy szervezeten belül elérhető helyi hálózat (LAN) vagy intranet. E tekintetben a kommunikáció módja közömbös (például lehet vezetékes vagy vezeték nélküli). A szerződő felek kiköthetik, hogy a bűncselekményt a biztonsági intézkedések megsértésével vagy számítástechnikai adatok megszerzésére irányuló, illetve más tisztességtelen céllal kövessék el.[8]

A büntetendő cselekményt jogosulatlanul kell elkövetni, ami azt jelenti, hogy ez a rendszer vagy a rendszer egy része jogosultjának vagy egyéb

[5] Forrás: http://www.europarl.europa.eu/news/hu/headlines/society/20180418STO02004/facebook-cambridge-analytica-botrany-zuckerberg-valaszoljon-az-europaiaknak Letöltés ideje: 2018.07.21.

[6] Lásd ehhez bővebben Mezei Kitti: A szervezett bűnözés az interneten. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. PTE ÁJK – MTA Társadalomtudományi Kutatóközpont. Budapest–Pécs, 2019. 125–147. o.

[7] Az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye, amelyet a 2004. évi LXXIX. törvénnyel hirdettek ki Magyarországon.

[8] Council of Europe: Explanatory Report to the Convention on Cybercrime. European Treaty Series – No. 185. 2001. 9–10. o.

jogosultjának az engedélye nélkül történik (például a már említett engedélyezett tesztelés nem minősül ennek). Nem büntetendő azonban, ha a számítástechnikai rendszerhez ingyenes és nyilvános hozzáférés áll rendelkezésre.

Az Európai Parlament és Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról [9] (a továbbiakban: 2013-as irányelv) is hasonlóan határozza meg a jogosulatlan belépés fogalmát, mert jogosulatlannak minősül minden olyan magatartás – ideértve a belépést, beavatkozást vagy adatszerzést is –, amelyet a rendszernek vagy a rendszer részének tulajdonosa vagy egyéb jogosultja nem engedélyezett, vagy amelyet a nemzeti jog nem tesz lehetővé.

A rendszert érintő jogellenes beavatkozással (3. cikk) kapcsolatban kimondja, hogy a tagállamoknak meg kell hozniuk a szükséges intézkedéseket annak érdekében, hogy a 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.

A tagállamok kötelesek az informatikai bűncselekményeket (3–7. cikk) szabadságvesztéssel büntetni, amelynek a felső határa – legalább a súlyosabb esetekben – két év, valamint biztosítaniuk kell, hogy az ezekre való felbujtás vagy az elkövetésükhöz nyújtott bűnsegély is bűncselekménynek minősüljön.

Azonban a 2013-as irányelv nem állapít meg büntetőjogi felelősséget abban az esetben, ha a bűncselekmény objektív kritériumai teljesülnek, de a cselekményt nem jogsértő szándékkal követték el, például az érintett személy nem tud arról, hogy az adott hozzáférés jogosulatlannak minősül, vagy az információs rendszerek tesztelésével/védelmével bízták meg (például egy cég kijelöl valakit a biztonsági rendszere tesztelésére). Ezenkívül az információs rendszerekhez való hozzáférést felhasználói szabályzat vagy szolgáltatási feltételek révén korlátozó szerződéses kötelezettségek

[9] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. HL L 218/8. 2013.8.14.

vagy megállapodások, valamint a munkáltató információs rendszereihez való magáncélú hozzáféréssel és azok magáncélú használatával kapcsolatos munkaügyi jogviták nem vonhatnak maguk után büntetőjogi felelősséget, amennyiben a hozzáférés az említett körülmények között minősülne jogosulatlannak, és ezáltal a büntetőeljárás kizárólagos alapját képezné. Nem érinti az információhoz való hozzáférésnek a nemzeti és az uniós jogszabályokban meghatározott jogát, ugyanakkor ez a jog nem szolgálhat az információhoz való jogellenes vagy önkényes hozzáférés igazolásául.

A jogosulatlan belépés hazai szabályozása

Az 1980-as évek második felében a hazai büntetőkódexbe először a számítógépes csalás tényállását iktatták be, amelynek megfogalmazásakor rendszerint a hagyományos csalás tényállásának szerkezetét követték, beépítve a magatartások megtévesztő jellegét és a jogtalan haszonszerzési célzatot. Kezdetben a Legfelsőbb Bíróság döntése például befejezett csalásként értékelte azt a büntetendő magatartást, amikor a számítógép-kezelő terhelt az őt terhelő hátralék összegét valótlan adat betáplálásával egyenlítette ki.[10] Rövid időn belül azonban egy új és önálló tényállás megalkotása vált szükségessé, ezért a számítógépes csalás az 1978. évi IV. törvény a Büntető Törvénykönyvről (a továbbiakban: 1978. évi Btk.) 300/C. §-ába lett beiktatva. Emellett a bankkártyával elkövetett tényállásokat is beemelték, amelyek ugyancsak a számítástechnikai eszközökkel elkövetett, illetve azok ellen irányuló bűncselekmények büntethetőségét teremtették meg. Már ebben az időszakban is felmerült a számítógépes adatok kikémlelésének szankcionálása, illetve az *„elektronikus betörés”* önálló bűncselekménnyé nyilvánítása. Azonban még hiányoztak a törvényből a számítógépes elkövetéssel kapcsolatos speciális definíciók is, mint például a számítógépnek, a számítógépes adatnak és az adatfeldolgozásnak a fogalma. Jelentős változásokat még az 1999. évi CXX. törvény hozott, mert a nagy nyilvánosság általános részi fogalmát kiterjesztette az elektronikusan rögzített információ távközlő hálózaton való közzétételére is.

[10] BH 1989/184.

Végül a Budapesti egyezményben foglalt büntetőjogi rendelkezésekkel összhangban léptette életbe a 2001. évi CXXI. törvény a számítástechnikai rendszer és adatok elleni bűncselekmény (1978. évi Btk. 300/C. §), valamint a számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása elnevezésű bűncselekmények (1978. évi Btk. 300/D. §) tényállásait, ami koncepcionálisan új szabályozást teremtett. Ezeket a bűncselekményeket azonban ekkor még a gazdasági bűncselekmények című XVII. fejezetben helyezték el, de ezt a megoldást kritikaként érte, hogy nem juttatta megfelelően kifejezésre a védendő értékek sokféleségét.

A számítógépes csalás helyébe iktatott új tényállás már büntetni rendelte a számítástechnikai rendszerbe történő jogosulatlan belépést, valamint a számítástechnikai rendszer és az abban tárolt, feldolgozott, kezelt vagy továbbított adatok sértetlensége elleni cselekményeket is. Ezt kiegészítette a számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása, amely már az alapcselekmények elkövetését lehetővé tévő feltételek biztosítását is *„sui generis”* bűncselekményként rendelte büntetni.[11]

Az egyes országok az informatikai bűncselekményeket külön törvényben szabályozzák (például Egyesült Államok), míg mások azt a szabályozási megoldást alkalmazzák, hogy a nemzeti büntető törvénykönyvükben vagy egy önálló fejezetben (például Franciaország), vagy a különös részben szétszórtan helyezik el a tényállásokat (például Németország).

Az információs társadalom jellemző indikátora az infokommunikációs eszközök általános elterjedtsége és használata, amely változásokat eredményezett a társadalmi viszonyok szinte valamennyi területén. Az informatikai környezet egyrészt megteremtette a már létező társadalmi értékek új szféráját, másrész egészen új, a büntetőjog által védett értékeket hozott létre.[12]

---

[11] Molnár Gábor: XLIII. fejezet – Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Kónya Sándor (szerk.): Magyar Büntetőjog – Kommentár a gyakorlat számára (Harmadik kiadás). HVG-ORAC Kiadó. Budapest, 2016. 971–972. o.

[12] Szathmáry Zoltán: Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban. Doktori Értekezés (PTE ÁJK). Budapest, 2012. 16. o.

2009-ben Nagy Zoltán már azt az álláspontot képviselte, hogy az informatikai bűncselekmények a tárgyi oldalon mutatkozó hasonlóságok, szoros összefüggések miatt önálló fejezetet fognak alkotni.[13] A 2012. évi C. törvény a Büntető Törvénykönyvről (a továbbiakban: Btk.) a 2013-as irányelvnek megfelelően – eleget téve a jogharmonizációs kötelezettségnek – átalakította a kiberbűncselekményekre vonatkozó szabályozást mind elnevezésben, mind tartalmilag, mert már a gazdasági bűncselekményektől külön, a XLIII. fejezetbe került, *„A tiltott adatszerzés és információs rendszerek elleni bűncselekmények”* címmel. A korábbi *„számítástechnikai rendszer”* terminológia helyébe az *„információs rendszer”* lépett.

A bűncselekmény jogi tárgya az információs rendszerek megfelelő működéséhez és a bennük tárolt, feldolgozott, továbbított adatok megbízhatóságához, hitelességéhez, valamint titokban maradásához fűződő társadalmi-gazdasági érdek.[14] Nagy álláspontja szerint e tényállás különböző bekezdései eltérő jogi tárgyat hivatottak védeni, így az (1) bekezdés az információs rendszerek integritását és biztonságát. A (2) bekezdés (a) pontja e rendszer biztonságos működését, míg a (b) pont az elektronikus adatok megbízhatóságához, hitelességéhez fűződő érdeket, valamint a tartalmuktól függően az azok által megtestesített értéket, és utóbbiak minősülnek a súlyosabb jogtárgysértésnek.[15]

Lényeges azonban kiemelni, hogy ez a tényállás továbbra is csak a számítástechnikai jellegű, szoftveres úton elkövetett támadások ellen biztosít büntetőjogi védelmet. A számítógép mechanikus védelmét ma is a rongálás törvényi tényállása látja el.[16] A büntetőkódex három külön fordulattal ha-

[13] Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Ad librum. Budapest, 2009. 61. o.
[14] Karsai Krisztina: XLIII. fejezet – Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Karsai Krisztina (szerk.): Kommentár a Büntető törvénykönyvhöz. Complex Kiadó. Budapest, 2013. 898. o.
[15] Nagy Zoltán András: XLIII. fejezet – Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Tóth Mihály – Nagy Zoltán András (szerk.): Magyar büntetőjog: Különös rész. Osiris. Budapest, 2014. 594–595. o.
[16] Molnár (2016): i. m. 946. o.

tározza meg a bűncselekmény elkövetési magatartásait, és valamennyi fordulat elkövetési tárgya az információs rendszer[17], amelynek betöltött funkciója a meghatározó.[18] Manapság már az okostelefonok is rendelkeznek olyan processzorral, mint egy hagyományos asztali számítógép, valamint egyre több más „okos" eszköz is erős kapacitással bír. Éppen ezért az elkövetők már a különböző IoT (Internet of Things) eszközöket[19], például routereket, biztonsági kamerákat vagy akár az okostelevíziókat és egészségügyi berendezéseket veszik célba egy-egy kibertámadás során, sőt az önvezető járművek is könnyedén válhatnak majd a hackertámadások célpontjaivá.[20]

A Btk. 423.§-ában a tisztán informatikai bűncselekménynek minősülő információs rendszer vagy adat megsértésének tényállását találjuk, amelynek (1) bekezdése értelmében büntetendő, 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.

Az (1) bekezdésben meghatározott enyhébb súlyú alapeset az információs rendszerbe történő jogosulatlan belépést nyilvánítja büntetendő cselekménnyé, amelynek két esete különböztethető meg. A jogosulatlan belépés irányulhat az elkövető által felhasznált számítógépre vagy a rajta keresztül elérhető védett számítógépes hálózatra (például intézményi belső

[17] Btk. 459.§ 15. pontja értelmében *„információs rendszer minden olyan berendezés – vagy egymással kapcsolatban lévő ilyen berendezések összessége –, amely automatikusan végez adatfeldolgozást, azaz adatok bevitelét, kezelését, tárolását, továbbítását látja el"*.

[18] Tóth Mihály: Alkothatók-e az informatikai bűnözés változatos formáit lefedni képes büntetőjogi tényállások? In: Gál István László – Nagy Zoltán András (szerk.): Informatika és büntetőjog. PTE ÁJK. Pécs, 2006. 184. o.

[19] Lásd bővebben Sara Sun Beale – Peter Berris: Hacking the Internet of Things: Vulnerabilities, dangers, legal responses. Duke Law & Technology Review, Vol. 16, No. 1. 162–204. o.

[20] Ambrus István: Az autonóm járművek és a büntetőjogi felelősségre vonás akadályai. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. PTE ÁJK–MTA Társadalomtudományi Kutatóközpont. Budapest–Pécs, 2019. 10–11. o.

hálózat, úgynevezett intranet, vagy az internet részét képező hálózat, például egy banki rendszer).

A bűncselekmény megállapításához szükséges, hogy az információs rendszer technikai intézkedéssel biztosított védelemmel legyen ellátva, és ez a védelem aktív legyen, azaz rendelkezzen például felhasználói azonosítóval és jelszóval vagy egyéb védelemmel. Tehát nem tekinthető jogosulatlannak a belépés abban az esetben, ha az információs rendszer nem védett, illetve a védelem nincs aktiválva, mert ezek konjunktív feltételek a bűncselekmény megállapíthatóságához.[21] Továbbá az elkövetési mód meghatározása szerint a bűncselekmény megvalósul, ha a belépés a védelmi intézkedés megsértésével vagy kijátszásával történik, például a biztonsági rendszer hiányosságait kihasználva lépnek be jogosulatlanul vagy a jogosult jelszavával, belépési kódjával, amelynek megszerzési módja azonban közömbös (például történhet megtévesztéssel, kifürkészéssel, kódtörő programmal, *„social engineering”,* vagyis pszichológiai manipulációval, vagy elképzelhető, hogy a felhasználó hanyagsága folytán jut hozzá az elkövető). Például a német büntető törvénykönyv (StGb) 202a. §-a is hasonlóan megköveteli a hacking megállapításához, hogy a jogosulatlan belépést a rendszer technikai védelmének kijátszásával valósítsák meg.[22]

A kiberbiztonságban a leggyengébb láncszem az ember. Az esetek döntő többségében ugyanis minden sikeres támadás mögött a sértetti közrehatás áll, és éppen ezért az elkövetők gyakran előnyben részesítik a social engineering támadásokat – mint például az adathalászatot (phishing) – a technikai jellegű megoldások alkalmazása helyett. Kevin Mitnick szerint a pszichológiai manipuláció könnyedén megkerüli a technológiai akadályokat (például tűzfalat vagy egyéb védelmet) a befolyásolás és megtévesztés segítségével.[23]

---

[21] Nagy (2014): i. m. 594–595. o.

[22] Alexander Niethammer – Steffen Morawiets: Germany: Cybersecurity 2019 Forrás: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany

[23] Kevin D. Mitnick: A megtévesztés művészete. *„A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer*

A bűncselekmény nem célzatos, ezért az elkövetésnek nem feltétele az sem, hogy haszonszerzési, károkozási vagy egyéb hasonló célzattal történjen. Az sem követelmény továbbá, hogy az információs rendszerben tárolt adaton az elkövető később bármilyen műveletet végezzen, vagy akár a rendszer működését akadályozza. Önmagában tehát a jogosulatlan belépés is büntetendő (mere hacking). Amennyiben ezt további jogosulatlan műveletek követik – például adatok törlése, hozzáférhetetlenné tétele –, akkor már a következő bekezdések egyik fordulata valósul meg és beleolvad, a súlyosabb jogtárgysértésre figyelemmel (Btk. 423. § (2) bek. a) és b) pont).[24]

A jogosulatlan belépés tipikus eseteként említhető az úgynevezett *„wardriving”* vagy *„wireless hacking”,* a vezeték nélküli hálózatok jogosulatlan használata. A wifikapcsolatok kialakításának több formája van: a nyilvános hálózatokhoz bárki szabadon csatlakozhat, mindenféle korlátozás nélkül. Nyilvános, de zárt hálózatok is rendelkezésre állhatnak, amelyek esetében egy speciális szoftver gondoskodik arról, hogy a hálózatot egy kód ismeretében lehet használni korlátozott ideig. A privát hálózatok esetében a hozzáférést titkosítják, általában tűzfal és jelszó használatával korlátozzák. Ezek a hálózatok saját használatra lettek kialakítva, jelszóvédelemmel, ezért kizárólag a jelszó ismeretében lehet csatlakozni hozzájuk. Azonban előfordul, hogy a tulajdonos akaratlanul védelem nélkül, „nyitva” hagyja a hálózatot. Ha a felhasználó az adatforgalom után fizet a szolgáltatója felé, akkor jelentős kárt okozhat nála a jogosulatlanul rácsatlakozó személy. A wifihálózatok további veszélyforrást jelentenek, mert rajtuk keresztül jogosulatlanul be tudnak lépni az információs rendszerekbe, illetve lehetőség van a hálózaton keresztül továbbított kommunikáció kifürkészé-

– technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.”

[24] Szathmáry Zoltán: A számítástechnikai bűncselekmények és rendszertani elhelyezésük. Jogtudományi Közlöny 2012/4. 173–174. o.

sére is. Azonban csak akkor valósítja meg a hálózatot jogosulatlanul használó személy a 423. § (1) bekezdését a „wifilopással”,[25] ha a hálózat aktív védelemmel van ellátva és ezt sérti meg, különben nem.[26]

Érdekességként megemlítendő az első nagy médiavisszhangot keltő hazai hackerügy, az Elender-per. 1999 decemberében az elkövetők beléptek a szolgáltató rendszerébe, feltelepítettek egy lehallgatóprogramot, és így később megszerezték az Elender mintegy 35 ezer ügyfelének azonosítóját. A jelszavak birtokában a cég honlapját kicserélték egy maguk által szerkesztettre, amin közzétették a birtokukba jutott felhasználói jelszavakat. A cég emiatt kénytelen volt leállítani a szervert, így a sok ezer ügyfél által igénybe vett szolgáltatások szüneteltek. Miután az elkövetők birtokába jutott a cég egyik informatikai igazgatójának jelszava, nyilvánosságra tudtak hozni rendszergazda-jogosultságot biztosító jelszavakat is, akkor emiatt már három napra leállt a teljes rendszer. A hatályos szabályozás szerint bűncselekményt valósítottak meg, azonban a cselekmény elkövetésének időpontjában az 1978. évi Btk. még nem szabályozta az informatikai bűncselekményeket, ezért az ügyészség közérdekű üzem működésének megzavarása és magántitok jogosulatlan megismerése miatt emelt vádat, de ez alól a bíróság másodfokon felmentette őket.[27]

A jogosulatlan belépéssel kapcsolatban fontos a már korábban vizsgált etikus hacking kérdését is áttekinteni a hazai szabályozás fényében: ez különösen aktuálissá vált, mert az elmúlt években több magyarországi esetre is fény derült, amelyek éles vita tárgyát képezték.

Az első eset során egy fiatal hacker 50 forintért vett bérlettel mutatott rá a BKK és T-Systems által üzemeltetett e-jegyrendszer hiányosságára, ami végül feljelentéssel zárult a jegyértékesítési rendszert ért informatikai tá-

[25] Lásd Blutmann László – Karsai Krisztina – Katona Tibor: Miért nem lehet a vezeték nélküli internet a lopás elkövetési tárgya? Bűnügyi Szemle 2008/1. 42–49. o.

[26] Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Ad librum Kft. Budapest, 2009. 272–273. o.

[27] Varga Árpád: Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben. In Medias Res 2019/1 szám. 163–164. o.

madás miatt. A vádemelésre végül nem került sor, mert az ügyészség megállapította, hogy a hacker célja valóban a biztonsági rés feltárása és ennek közlése volt a BKK felé. A rendszerhibáról való kétséget kizáró meggyőződéshez szükség volt a vásárlás befejezésére. Mindezekre tekintettel az ügyészség szerint a cselekmény nem volt veszélyes a társadalomra, ami a bűncselekmény megállapításának a feltétele. Emellett a hacker bejelentése közérdekű bejelentésnek minősül, ez pedig a büntethetőséget kizáró ok.[28]

A másik esetben egy programozónak tanuló hallgató a Magyar Telekom oldalán található nyilvános dokumentumban talált információk alapján jutott hozzá egy rendszergazdai jelszóhoz, amellyel hozzá tudott férni a Telekom teljes belső hálózatához, és erről a biztonsági résről később tájékoztatta a céget. Ezt követően azonban további, újabb sebezhetőséget talált, és ezt kihasználva lépett be újból a rendszerbe, a vállalat kifejezett kérése ellenére, aminek eredményeképpen a Telekom ismeretlen tettes ellen tett feljelentést. Az ügyészség vádat emelt az információs rendszer megsértéséért, méghozzá annak minősített esetéért, mert a meghackelt szerver a hírközlő hálózat része volt, ezért a Btk. 459. § (1) bekezdés 21. pontja alapján közérdekű üzemnek minősül.[29] Végül a Szolnoki Járásbíróság információs rendszer vagy adat folytatólagosan elkövetett megsértése bűntettében mondta ki bűnösnek a hackert, és 600 ezer forint pénzbüntetésre ítélte jogerős ítéletében.

Mindezekre tekintettel a bírónak a konkrét esetben a tényállás kimerítése mellett van-e olyan társadalmilag fontos és méltányolható érdek, ami miatt a cselekmény jogellenessége hiányzik, és ezért nem veszélyes a társadalomra? Karsai Krisztina szerint büntetőjogi értelemben azt kell vizsgálni, hogy mihez fűződik nagyobb társadalmi érdek: a személyes adatok biztonságához, vagy a biztonsági rések fenntartásához? A bíró tehát vizs-

[28] Forrás: https://jogaszvilag.hu/napi/bkk-botrany-fellelegezhet-az-etikus-hacker/
Letöltés ideje: 2019.11.05.

[29] Forrás: http://ugyeszseg.hu/valasz-a-tarsasag-a-szabadsagjogokert-tasz-etikus-hacker-ugyeben-tett-allitasaira/
Letöltés ideje: 2019.11.05.

gálja ezt a kérdést, és a bizonyítékok alapján kialakult meggyőződése szerint megállapíthatja a társadalomra veszélyesség hiányát, s így felmentheti az illetőt. Azonban az e tevékenység mögött húzódó szándékot is mindig figyelembe kell venni.[30]

Ambrus István véleménye szerint a bíróság a vizsgálat tárgyává teheti például azt is, hogy a terhelt eljárása tekinthető-e közérdekű bejelentésnek, vagy sem.[31] A közérdekű bejelentés olyan körülményre hívja fel a figyelmet, amelynek orvoslása vagy megszüntetése a közösség vagy az egész társadalom érdekét szolgálja, vagyis a bejelentő jelen esetben a közérdek védelme érdekében realizálja magát az elkövetési magatartást. A közérdekű bejelentés javaslatot is tartalmazhat.[32]

A bűncselekmény alanya az első fordulatban a belépésre jogosultsággal nem rendelkező személy lehet, míg a második fordulat esetén az adott személy rendelkezik erre vonatkozó engedéllyel.

Áttérve a jogosulatlan belépés második fordulatára, ami akkor valósul meg, ha az elkövető az engedélyezett belépést követően a jogosultsága terjedelmi vagy időbeli kereteit meghaladja, illetve a jogosultságot más módon, szándékosan megsérti az információs rendszerben való bennmaradással. E fordulat alaki bűncselekményt határoz meg.[33]

A Kúria kimondta, hogy a büntetőjog alapelveivel összhangban a jogosultság keretein való túllépés is akkor minősül bűncselekménynek, ha az egyben a rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával történik (például más jelszavának a felhasználásával). Ugyanis ha valakinek van jogosultsága az információs rendszerbe történő

[30] Forrás: https://qubit.hu/2019/02/04/torvenyt-sertett-az-etikus-hacker-de-ha-nem-jelent-veszelyt-a-tarsadalomra-a-birosagnak-fel-kell-mentenie
Letöltés ideje: 2019.11.05.

[31] Forrás: https://qubit.hu/2019/02/04/torvenyt-sertett-az-etikus-hacker-de-ha-nem-jelent-veszelyt-a-tarsadalomra-a-birosagnak-fel-kell-mentenie
Letöltés ideje: 2019.11.05.

[32] 2013. évi CLXV. törvény a panaszokról és a közérdekű bejelentésekről 1.§ (3) bekezdése

[33] Molnár Gábor Miklós: XL. fejezet – A pénzmosás. In: Belovics Ervin – Molnár Gábor Miklós – Sinku Pál (szerk.): Büntetőjog II. – Különös rész. HVG-ORAC Kiadó. Budapest, 2018. 947. o.

belépéshez, akkor pusztán e jogosultság kereteinek túllépése nem éri el azt a veszélyességi szintet, mint amit az első fordulat megkíván. Tehát önmagában a jogosultság kereteinek túllépésével való belépés vagy bennmaradás nem büntetendő, amennyiben nem valamely biztonsági intézkedés megsértésével valósul meg, vagy nem kapcsolódik össze további tisztességtelen célzattal – például jelentős érdeksérelemmel, jogtalan károkozási, haszonszerzési célú adatszerzéssel vagy -manipulálással, vagy a rendszer megzavarásának szándékával, illetve eredményével –, mert ennek hiányában a magatartás társadalomra veszélyessége csekély.

Az említett eset során a védelem utalt a jelenlegi rendőrségi gyakorlatra is, amely szerint bárkit megbízhatnak felettesei a tevékenységi körétől eltérő, bármilyen kiegészítő vagy akár érdemi feladat elvégzésével is szóbeli parancs, utasítás útján, írásbeli nyom nélkül, így álláspontja szerint kizárólag szubjektív elhatározás kérdése, hogy az ilyen, nem az adott munkakörhöz tartozó feladatok elvégzése során az informatikai rendszerbe való belépés miatt mikor és kit vonnak felelősségre.[34]

A jogosulatlan hozzáférés szabályozása az Egyesült Államokban

Az Egyesült Államokban szövetségi rendszer működik, ezért a kiberbűnözés elleni fellépés is kétszintű. A szövetségi szintű szabályozás egységes, területi hatálya az Egyesült Államok egészére kiterjed, míg az egyes állami szintek egymástól eltérhetnek, és csak az adott államok területén érvényesek. Jelen írásom kizárólag az előbbit érinti, méghozzá a – kifejezetten az informatikai bűncselekmények szabályozását célzó – Computer Fraud and Abuse Act vonatkozó rendelkezéseit (CFAA).[35]

[34] BH 2017.12.392. Ezzel kapcsolatban Parti Katalin vizsgálta, hogy a hacking szabálysértésként való felfogása mennyiben lenne hatékonyabb és nagyobb visszatartó erejű szankció. Lásd Parti Katalin: Gondolatok a számítástechnikai adatok és rendszerek elleni bűncselekmények tényállásairól. Büntetőjogi Kodifikáció 2005/2. 38. o.

[35] Eoghan Casey: Digital Evidence and Computer Crime. Amsterdam, Elsevier, 2012. 85. o.; valamint lásd ehhez még: Sorbán Kinga: Az informatikai bűncselekmények elleni fel-

A CFAA-ban szabályozott bűncselekmények egy része a *„jogosulatlan hozzáférést”* követeli meg (1030. § (a)(3), (a)(5)(B), (a)(5)(C)), míg más rendelkezések a *„jogosulatlan hozzáférést”* vagy a *„jogosultságának kereteit túllépve”* történő elkövetést (1030. § (a)(1), (a)(2), (a)(4)) is. A törvény azonban a *„jogosulatlan hozzáférés”* (unauthorised access) fogalmának meghatározásával adós maradt. Azonban a széles körben elfogadott álláspont szerint a hozzáférés nemcsak a szűken vett „belépést” foglalja magában, hanem többek között a számítógép használatát is.

A CFAA a *„jogosulatlan hozzáférés”* keretében általában azokat az eseteket szabályozza, amelyek során az elkövetők „kívülálló” személyekként (outsiders) követik el a bűncselekményeket, mint például a külső támadást indító hackerek, míg a *„jogosultság kereteinek túllépése”* esetén olyan engedéllyel rendelkező, „bennfentes” személyekről *(insiders)* van szó, mint például az alkalmazottak. A megkülönböztetés alapja a rendszerhez való hozzáférési jogosultság. Azok a személyek, akik hozzáférési jogosultsággal rendelkeznek a számítógéphez, általában kizárólag akkor vonhatók büntetőjogi felelősségre, ha szándékosan okoznak kárt. Ezzel szemben a kívülállók a szándékos károkozáson kívül a gondatlanságból bekövetkezett eredményért is büntethetők.[36]

Fontos, hogy a bűncselekményeket megalapozó hozzáférésnek jogosulatlannak kell lennie, amelynek alapját a Budapesti egyezménynél tárgyalt fogalom képezi, vagyis annak minősül, ha az adott magatartást a tulajdonos vagy egyéb jogosult nem engedélyezi.

A hozzáférés korlátozása vagy megtagadása két módon történhet: a technikai védelem alkalmazásával (code-based restriction) vagy szerződés (contract-based restriction) alapján.[37] A „kód” szerinti szabályozás esetén

lépés az Egyesült Államokban. Themis 2016/1. 150–170. o. és Dornfeld László: A kiberbűncselekmények szabályozásának története az Egyesült Államokban és Európában. Miskolci Doktoranduszok Jogtudományi Tanulmányai 16. 67–86. o.

[36] U.S. Department of Justice: Computer Crime and Intellectual Property Section Criminal Division: Prosecuting Computer Crimes. 2015. 5–6. o.

[37] Orin Kerr szerint a jogosulatlan belépés esetén kizárólag a kódalapú védelem jöhet szóba, mert a szerződésalapút nehezebb meghatározni ez esetben. Azonban a jogosultság kereteinek túllépése esetén elismeri a szerződésalapú korlátozás létjogosultságát. Orin

a tulajdonos valamilyen technikai intézkedést tesz a hozzáférés korlátozása érdekében, például felhasználónevet és jelszót ad meg a fiókhozzáféréshez. Aki ezt kijátssza akár csak jelszótalálgatással vagy technikai eszköz használatával, az jogosulatlanul fér hozzá.

A szerződéssel történő szabályozás gyengébb alapokon nyugszik: a tulajdonos határozza meg a hozzáférés feltételeit, ez történhet formálisan vagy informálisan, valamint kifejezetten vagy hallgatólagosan. Például ilyen lehet a munkaszerződés vagy a használati feltételeket tartalmazó szabályzat. A szerződéssel történő korlátozás nagymértékben függ attól, hogy a szerződési feltételek mennyiben vannak pontosan és részletesen meghatározva.

Orin Kerr hasonlata szerint a kettő közötti különbség úgy ragadható meg, hogy a kódalapú korlátozás esetén becsukjuk és egyben bezárjuk az ajtót, hogy idegenek ne tudjanak bejönni, míg a szerződésalapú korlátozás ahhoz hasonlítható, amikor az ajtót nyitva hagyjuk és kiteszünk egy táblát, hogy *„Idegeneknek belépni tilos”*.[38]

Kerr felhívja a figyelmet arra, hogy ez esetben különösen jelentős szerepe van a *„mens rea”*[39] vizsgálatának. Általánosságban a CFAA a szándékos vagy tudatos elkövetést követeli meg a felelősségre vonáshoz. Ez azt jelenti, hogy az illető tudatának át kell fognia, hogy az általa tanúsított magatartás nem engedélyezett számára. További kérdéseket vet fel például, ha egy alkalmazottat elbocsátanak – egyúttal a jogosultságát is megvonják –, és ezt követően fér hozzá a volt munkáltatója rendszeréhez. Ehhez példaként említendő a United States vs. Shahulhameed-ügy, amikor a Toyota

Kerr: Cybercrime’s Scope: Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes. 78 N.Y.U. L. Rev. 1596 (2003). 1662–1663. o.

[38] Kerr (2003): i. m. 1662–1663. o.

[39] Az angolszász jog szerint akkor állapítható meg a bűncselekmény elkövetése, ha megtörtént a bűnös cselekmény (*„actus reus”*, a bűnös tett), és arra az elkövető tudatállapota kiterjedt, azaz a cselekményt ő követte el, annak megtörténtét kívánta (*„mens rea”*, a bűnös tudat). Mindkét fogalmi elemnek meg kell valósulnia ahhoz, hogy a bűncselekmény megállapítható legyen.

Motors elbocsátotta informatikus alkalmazottját, azonban a vállalati hozzáférését még nem vonták vissza technikai értelemben, így ezt kihasználva, a rendszerbe belépve adatokat módosított és akadályozta a szerverek működését. A bíróság ezt úgy értékelte, hogy jogosulatlanul fért hozzá a rendszerhez, és felelősségre vonta ezért.[40] Ezenkívül említi a Steele-ügyet, amikor az elbocsátott alkalmazottól elvették a céges laptopját, belépőkártyáját, és aláírattak vele egy nyilatkozatot, hogy a jövőben már nem férhet hozzá a volt munkáltatója számítógépes rendszeréhez. Ezután mégis több alkalommal használta azt, és ezért felelősségre vonták. Ez azzal magyarázható, hogy már visszavonták a hozzáférési jogosultságát, és a körülményekből tudott erre következtetni, azonban vannak olyan esetek, amikor ez nem ennyire nyilvánvaló.[41]

A másik érdekes kérdés, miként minősíthető az úgynevezett *„port scanning”,* amely tesztelést általában a kiberbiztonsági szakértők és crackerek is el szokták végezni, hogy feltérképezzék a hálózat nyitott és sebezhető portjait, azonban a bíróság szerint ez nem minősül az 1030.§ szerinti jogosulatlan hozzáférésnek.[42]

A CFAA a *„jogosultsága keretének túllépését”* az 1030. § (e)(6) pontjában definiálja, melynek értelmében azt jelenti, hogy az adott személy *„jogosultsággal rendelkezik a számítógéphez történő hozzáféréshez, és e jogosultság felhasználásával információt szerez meg vagy módosít a számítógépen, azonban jogosultsága a megszerzésre vagy a módosításra nem terjed ki”*. Ennek megfelelően a vádhatóság részéről azt kell bizonyítani, hogy az adott személy hozzáférési jogosultsága hogyan lett korlátozva, valamint e korlátozást hogyan lépte túl annak érdekében, hogy megszerezze vagy módosítsa az információt a számítógépen. Előbbi bizonyítása egyszerű, ha a terhelt jogosultságának kereteit írásba foglalták (például számítógéphasználati szabályzat, munkaszerződés vagy titoktartási szerződés).

[40] Orin Kerr: Computer Crime Law. Fourth Edition. West Academic Publishing. 2018. 48–51. o.

[41] Orin Kerr: Norms of computer trespass. Columbia Law Review Vol. 116. 2016. 1182. o.

[42] Kerr (2018): i. m. 37. o.

A legvitatottabb kérdésként merül fel a jogirodalomban és a joggyakorlatban egyaránt, hogy vajon az adott személy túllépi-e a jogosultságai keretét, ha nem a meghatározott célból fér hozzá a számítógéphez. Ez különösen három esetben gyakori:

- ha az engedélyező fél kifejezetten megtiltotta a terheltnek, hogy meghatározott célból férjen hozzá a számítógéphez;
- ha az engedélyező fél kifejezetten megtiltotta a terheltnek, hogy az adataihoz meghatározott célból férjen hozzá, azonban a számítógéphez való hozzáférést ennek megfelelően nem tiltotta meg;
- ha az engedélyező fél nem tiltotta meg kifejezetten, hogy a terhelt az adatait „nem megfelelő" célra használja, de a terhelt az engedélyező fél érdekével ellenkező magatartást tanúsított.
- Az első eset a legkevésbé ellentmondásos, mert egyértelmű a célalapú korlátozás a terhelt hozzáférési jogosultságával kapcsolatban. A második eset már kérdéses, hiszen a sértett aláírathat az érintett személlyel egy titoktartási szerződést, amelyben hozzájárul, hogy nem használja fel a sértett információját személyes haszonszerzésre, de probléma merülhet fel, ha a megállapodás nem tartalmazza kifejezetten, hogy az illető nem férhet hozzá a sértett számítógépes rendszeréhez. Bár korlátozva lett az információ személyes felhasználása, de az nem, hogy az illető jogosultsága nem terjed ki a számítógépen található adatok megszerzésére vagy módosítására.[43]
- A hatályos CFAA-ban szabályozott kiberbűncselekmények, amelyek a jogosulatlan hozzáféréshez kapcsolódnak, a következők:
- nemzetbiztonsági információval való visszaélés (1030. § (a)(1)),
- számítógéphez való jogosulatlan hozzáférés és információval való visszaélés (1030. § (a)(2)),
- kormányzati számítógéphez való jogosulatlan hozzáférés (1030. § (a)(3)).

[43] U.S. Department of Justice: i. m. 8–11. o.

Zárógondolatok

Magyarországon az elmúlt években az informatikai bűncselekmények szabályozása a nemzetközi és uniós elvárásoknak megfelelően alakult. A Btk. hatályba lépésével már annak önálló fejezetébe lettek illesztve, ami mindenképpen üdvözítő megoldás és haladás az új védendő társadalmi értékek elismerése felé. A joggyakorlat egyes kérdéseket is megválaszolt, ugyanis a hacking rendelkezés második fordulatánál (Btk. 323.§ (1) bekezdés) a Kúria elvi éllel mondta ki, hogy a jogosultság keretein való túllépés is akkor minősül bűncselekménynek – az első fordulat szerinti jogosulatlan belépéshez hasonlóan –, ha az egyben a rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával történik.

A másik felmerült problémakör az etikus hackinghez kapcsolódik, amely sokszor éles vita tárgyát képezi, és visszavezethető arra, hogy hiányzik a megfelelő szabályozása és gyakorlata. A szakirodalmi álláspont szerint az információs rendszer tulajdonosa vagy egyéb jogosultja által más számára engedélyezett biztonsági tesztelés, illetve támadás tartozik ebbe a tevékenységi körbe. Erre utal rendelkezéseiben a Budapesti Egyezmény és a 2013-as irányelv is, amelyek szerint a büntetendő cselekményt jogosulatlanul kell elkövetni, ami azt jelenti, hogy ez a rendszer jogosultjának az engedélye nélkül történik. Ez különösen akkor vitatott, ha a hacker valamilyen sebezhetőségre hívja fel a figyelmet, különösen, ha a nagy nyilvánosság felé is közvetíti. A konkrét ügy során ezért a bíróságnak vizsgálnia kell az eset összes körülményére tekintettel a következőket: a hacker cselekménye mennyiben veszélyes a társadalomra, milyen szándék húzódott e magatartása mögött, valamint közérdekű bejelentésnek tekinthető-e az eljárása a megtámadott fél felé.

A hazai és amerikai szabályozást összevetve megállapítható, hogy utóbbi részletesebben szabályozza az egyes informatikai bűncselekményeket. Példaként említhető, hogy a jogosulatlan hozzáféréssel kapcsolatban több tényállást alkottak. Jelentős különbségek is tetten érhetők, azonban ez betudható annak, hogy a CFAA alapját az angolszász jogrendszer képezi. Az amerikai jog a védett számítógéphez való hozzáférés korlátozásának két

típusát határozza meg: a technikai védelem (code-based) és a szerződés (contract-based) alapján. A magyar szabályozás azonban megköveteli a technikai intézkedés megsértését vagy kijátszását a tényállásszerűséghez. A 2013-as irányelv is rögzíti, hogy például felhasználói szabályzat vagy szolgáltatási feltételek révén korlátozó szerződéses kötelezettségek vagy megállapodások nem vonhatnak maguk után büntetőjogi felelősséget. Hasonló elkövetői kör büntethető mindkét törvény alkalmazásában, így aki a hozzáférési jogosultsággal nem rendelkező (kívülálló) személy vagy jogosultsággal rendelkező, de ennek kereteit túllépő (bennfentes) személy. A CFAA legnagyobb hiányossága abban ragadható meg, hogy az egyes alapvető fogalmakat nem tisztázza, mint például *„a jogosulatlan hozzáférést”*, ezért ez a jogalkalmazókra hárul.