

Számítástechnikai rendszer és adatok elleni bűncselekmény

300/C. § (1) Aki számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve, illetőleg azt megsértve bent marad, vétséget követ el, és egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(2) Aki

a) számítástechnikai rendszerben tárolt, feldolgozott, kezelt vagy továbbított adatot jogosulatlanul megváltoztat, töröl vagy hozzáférhetetlenné tesz,

b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését jogosulatlanul akadályozza, vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(3) Aki jogtalan haszonszerzés végett

a) a számítástechnikai rendszerbe adatot bevisz, az abban tárolt, feldolgozott, kezelt vagy továbbított adatot megváltoztat, töröl vagy hozzáférhetetlenné tesz, vagy

b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését akadályozza,

és ezzel kárt okoz, büntettet követ el, és három évig terjedő szabadságvesztéssel büntetendő.

(4) A (3) bekezdésben meghatározott bűncselekmény büntetése

a) egy évtől öt évig terjedő szabadságvesztés, ha a bűncselekmény jelentős kárt okoz,

b) két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekmény különösen nagy kárt okoz,

c) öt évtől tíz évig terjedő szabadságvesztés, ha a bűncselekmény különösen jelentős kárt okoz.

Az Európa Tanács informatikai bűnözésről szóló egyezményében foglalt büntetőjogi rendelkezésekkel összhangban léptette életbe a számítástechnikai rendszer és adatok elleni bűncselekmény tényállását a 2001. évi CXXI. tv. 57. §-a.

1. Az új bűncselekmény jogi tárgya egyfelől a számítástechnikai rendszerek megfelelő működéséhez és a bennük tárolt, feldolgozott, továbbított adatok megbízhatóságához, hitelességéhez, valamint titokban maradásához fűződő érdek.

A törvényi tényállás konstrukciójának sajátossága, hogy a törvény az adott bűncselekmény három alapesetét szabályozza, amelyek az elkövetési magatartások függvényében egymáshoz képest súlyosabban büntetendő cselekmények.

A számítástechnikai bűnözésről szóló, Strasbourgban 2001. január 8-án meghozott Egyezmény 1. Cikkének meghatározása szerint számítástechnikai rendszer minden olyan önálló eszköz, illetőleg egymással kapcsolatban lévő vagy összekötött eszközök összessége, melyek - illetőleg melyeknek egy vagy több eleme - program végrehajtásával adatok automatikus feldolgozását biztosítják.

2. Az (1) bekezdésében írt alaptényállás büntetendő cselekménnyé nyilvánítja a számítástechnikai rendszerbe történő jogosulatlan behatolást, illetve a belépés jogosultságának kereteit túllépő bennmaradást. A számítástechnikai rendszerbe történő belépés azonban csak akkor tényállásszerű magatartás, amennyiben a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával történik.

Abban az esetben, ha a számítástechnikai rendszerbe jogosultán lép be az elkövető, azonban annak kereteit túllépve, illetve azzal ellentétesen marad benn a számítástechnikai rendszerben, ugyancsak elköveti a bűncselekményt.

Az elkövetési magatartás azonban csak abban az esetben tényállásszerű, ha az elkövető a megváltoztatást, törlést vagy hozzáférhetetlenné tételt jogosultság hiányában követi el. A bűncselekmény az adat bármilyen módon történő módosításával, törlésével vagy hozzáférhetetlenné tételével befejezetté válik, ugyanis nem szükséges, hogy a cselekmény következtében a számítástechnikai rendszer bármilyen károsodása bekövetkezzen.

A (2) bekezdés b) pontjában meghatározott cselekmény védett jogi tárgya a számítástechnikai rendszer működése. Míg a (2) bekezdés a) pontja esetében a tárolt, feldolgozott, kezelt vagy továbbított adatokat védi a törvény, úgy ez esetben magát a számítástechnikai rendszer hibátlan működését részesíti büntetőjogi oltalomban. A (2) bekezdés b) pontja szerint, aki a számítástechnikai rendszer működését jogosulatlanul akadályozza, vétséget követ el és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

A (3) bekezdés gyakorlatilag a korábbi számítógépes csalásnak megfelelő, attól kissé eltérő tényállást fogalmazott meg. Ezek szerint, aki a (2) bekezdés a)-b) pontjában írt magatartásokat jogtalan haszonszerzés végett követi el, büntettet követ el és három évig terjedő szabadságvesztéssel büntetendő.

A (3) bekezdésben írt minősített eset eredménybűncselekményt fogalmaz meg, ugyanis mindkét fordulat esetében a károkozás, illetve a kár bekövetkezése tényállási elemként szerepel. Ugyanakkor a (3) bekezdés a) és b) pontjában írt magatartások a jogtalan haszonszerzéssel és a károkozással együttesen is alapeseti cselekményként kerültek megfogalmazásra.

A (4) bekezdés meghatározása szerint a bűncselekmény súlyosabban minősül attól függően, hogy jelentős, különösen nagy vagy különösen jelentős kárt okoz. Ebből következően a törvényi utalás szerint is kizárólag a (3) bekezdés a) és b) pontjában írt alapeseti bűncselekménynek lehet minősített esete, ugyanis kizárólag az ott írtak szerint tényállási elem a károkozás.

A kár meghatározásánál rendkívül lényeges, hogy a károkozás nem az elkövetés módjára, hanem a cselekmény eredményére vonatkozik, vagyis a kárnak nem a számítástechnikai rendszerben kell bekövetkezni, hanem a számítástechnikai rendszer manipulációjával összefüggésben, a tevékenység eredményeként.

300/E. § (1) Aki a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából, az ehhez szükséges vagy ezt könnyítő számítástechnikai programot, jelszót, belépési kódot, vagy számítástechnikai rendszerbe való belépést lehetővé tevő adatot

a) készít,

b) megszerez,

c) forgalomba hoz, azzal kereskedik, vagy más módon hozzáférhetővé tesz,

vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő, aki a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő, számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszerbe való belépést lehetővé tevő adat készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit másnak a rendelkezésére bocsátja.

(3) Nem büntethető az (1) bekezdés a) pontja esetén, aki - mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszer egészébe vagy egy részébe való belépést lehetővé tevő adat készítése a hatóság tudomására jutott volna - tevékenységét a hatóság előtt felfedi, és az elkészített dolgot a hatóságnak átadja, valamint lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.

A Btk. 300/E. §-ának címét és szövegét a 2001. évi CXVI. tv. 58. §-a állapította meg és iktatta be a Btk. XVII. fejezetébe.

A bűncselekmény megfogalmazását a számítástechnikai bűnözésről szóló, Strasbourgban 2001. január 8-án meghozott Egyezmény 6. Cikkében megfogalmazott elvek tették szükségessé.

1. A bűncselekmény elkövetési tárgya az (1) bekezdés vonatkozásában a bűncselekmény elkövetését lehetővé tevő vagy ahhoz szükséges, illetőleg azt megkönnyítő számítástechnikai program, jelszó, belépési kód, vagy a számítástechnikai rendszerbe való belépést lehetővé tevő adat.

2. Az elkövetési magatartás a program, jelszó, kód stb. készítése, megszerzése, forgalomba hozatala, hozzáférhetővé tétele, illetve a kereskedés.

3. A bűncselekmény az illető programok, jelszó, belépési kódok stb. elkészítésével, megszerzésével, forgalomba hozatalával vagy kereskedésével, illetve hozzáférhetővé tétellel befejezett, függetlenül attól, hogy a Btk. 300/C. §-ában meghatározott bűncselekményt akár az elkövető, akár más személy, aki részére a programot átadta, hozzáférhetővé tette, elkövette-e vagy sem.

4. A bűncselekmény alanya bárki lehet, aki természetesen rendelkezik azokkal a műszaki és technikai ismeretekkel, amelyek ilyen programok, belépési kódok vagy adatok készítéséhez feltétlenül szükségesek.

E bűncselekmény tipikus elkövetői a hackerek, a crackerek és a phrackerek.

5. A (3) bekezdés speciális büntethetőséget kizáró okot fogalmaz meg az (1) bekezdés a) pontja szerinti készítő részére, ha a tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja és lehetővé teszi, hogy a készítésben résztvevő más személyek kilétét a hatóság megállapítsa.

E három feltételnek egyidejűleg kell fennállnia ahhoz, hogy az elkövető büntetlen maradjon.