

## Jogos vagy jogtalan?

Idén április 1-jétől hatályos a büntető törvénykönyv 1978. IV. cikkelyének a Számítástechnikai rendszer és adatok elleni bűncselekményről szóló passzusa. Elsőként idézzük fel magát a törvényt:

### Számítástechnikai rendszer és adatok elleni bűncselekmény

300/C. §

- (1) Aki számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy 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 hozzáférhetlenné 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 megváltoztatja, töröl vagy hozzáférhetlenné tesz, vagy
  - b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését akadályozza és ezzel kárt okoz, büntetést 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.

Ennyi a törvényszöveg, amely informatikus körökben oly nagy vihart kavart, és rácsodálkoztunk: hogy is van ez? Létrejött egy büntetőtörvényi alakzat, mely korábban nem ismert, vagy ismert, de a büntető törvénykönyvben korábban nem szerepelt cselekményeket a büntetőjog hatálya alá vont, és azokat bűncselekményeknek, enyhébb esetben vétségnek, súlyosabb esetben büntettnék minősít és hozzá büntetési tételeket rendel.

A kérdés az, kinek milyen cselekménye milyen tényállást valósít meg, és kit miért ítélnék el a független bíróság? Hogyan kerülhető el, hogy szakmai döntéseinket mások bűncselekményként értékeljék és akár alaptalanul is, de büntetőeljárást kezdeményezzenek ellenünk?

Írássorozatomban ezekre a kérdésekre keresek részben gyakorló informatikusként, részben joghallgatóként – jogi tanulmányaim alapján – választ.

Előre kell bocsátanom, írásom inkább elgondolkodásra serkentő céllal íródott. Kapcsolódó jogi fejtegetéseim tartalmát eddig végzett tanulmányaim keretei adják, így azok felhasználhatósága gondolatébresztésen kívül másra nem terjedhet ki, és egy új, eddig ismeretlen határrületen bolyongunk majd: a jog és az informatika határán. A törvényszöveget elsősre elolvasva – valljuk be – rémület lesz úrrá rajtunk. Ha csak a jelzett jogszabályhelyet nézzük, látszólag szándék kérdésévé válik, milyen szakmai eljárás minősíthető jogellenesnek.

Nézzük meg először; mivel vagyunk fenyegetve a büntetőjog oldaláról! Amit e törvényhely szerint elkövetünk, az bűncselekmény – tehát az a cselekmény, amely szándékosan, vagy ha a törvény a gondatlan elkövetést is bünteti, gondatlanságból kerül elkövetésre, és amely veszélyes a társadalomra, és amelyre a törvény büntetés kiszabását rendeli.

Egyidejűleg kell fennállnia

- társadalomra való veszélyességének,
- az elkövetői szándékosságának vagy a büntetni rendelt gondatlanságnak,
- a cselekmény büntetni rendeltségének – tényállás megvalósulásának
- és a bűnösségnek.

A cselekmény a törvény értelmezésében megvalósulhat tevészel, tehát valamilyen aktív cselekedettel, de valamitől való tartózkodással, azaz nem tevészel is.

Ezek az alapfogalmak jelen vizsgálódásunkban.

Az informatikai munka során cselekményeink (feladataink) vannak: az adatbiztonság megteremtése a működés fenntartása érdekében, de cselekmény egy folyamat figyelemmel kísérése is, jöllehet mi magunk tevélegesen nem avatkozunk be. Ezen cselekmények a büntetőjogban akként kerülnek megvizsgálásra, hogy cselekményünk megfeleltethető-e valamely törvényi tényállásnak, eleget teszünk-e a vonatkozó szakmai előírásoknak, illetve mi személy szerint megtettük-e mindazt, ami az adott helyzetben elvárható.

Ezen cselekmények megítélése a jelen törvénymódosítás hatályba lépésétől többé már nem szakmai, hanem adott esetben büntetőjogi kérdés lett.

Az adott helyzetben elvárható és a szakmai szabályoknak megfelelő cselekmények adják az informatikai szakma felelősségének alapjait.

E felelősség a jog több oldaláról is behatárolt:

- büntetőjogi – e törvény cikkelyein alapulva;
- polgári jogi;
- munkajogi;
- szabálysértési, amennyiben ezt rendelet vagy önkormányzati rendelet szabálysértéssé nyilvánítja.

A büntető törvénykönyv tárgyalat értelmezési és alkalmazási gondoljaim szerintem innen (is) kezdődnek.

Büntetőjogi oldalról szemlélve informatikai munkánk



során a számítástechnikai rendszer és adatok elleni bűncselekményt – jelen törvényi szabályozás szerint – szándékosan lehet elkövetni. Szándékosan követi el a bűncselekményt, aki magatartásának következményeit kívánja vagy e következményekbe belenyugszik. Ez viszonylagosan jól érthető és alkalmazható mindennapi élethelyezeteinkre: ha valakik szándékosan tönkretesznek például egy adatállományt, amellyel a munkáltatónak, megbízónak kárt okoznak, azért e törvényhely szerint felelniük kell. A lényeges részlet tehát a célirányos szándékos károkozás.

A szándékosság megvalósulhat például egy merevlemez szándékos megromlásával, törlésével, de megvalósulhat a beavatkozástól való tartózkodással, ha az károkozás előidézésére irányul. Így van, ha például egy egyre többször eszközhibát jelző meghajtót azért nem mentenek (cserélnék) le, mert tudják, hogy e folyamat végén tönkremegy, és ezzel akarnak kárt okozni; tehát a hiba keletkezése és a kár bekövetkezése között a „nem tevő” magatartás oksági kapcsolatot teremt – bizony, ez is szándékos magatartásnak minősül. A kárt a szándékos célirányos magatartás okozta, még ha ez tartózkodásban valósult is meg.

E törvény 300/C § (4) alkalmazásában jogtalan haszon-szerzés végett meghatározott esetekben az érték, a kár, a vagyoni hátrány, a mérték összege, illetőleg az adó-, a járulék, a magánnyugdíj-pénztári tagdíj bevételcsökkenésének összege

- *kisebb* a kár, ha tízezer forintot meghalad, de kétszáz ezer forintot nem halad meg,
- *nagyobb*, ha kétszáz ezer forintot meghalad, de kétfélmillió forintot nem halad meg;
- *jelentős*, ha kétfélmillió forintot meghalad, de ötvenmillió forintot nem halad meg;
- *különösen nagy*, ha ötvenmillió forintot meghalad, de ötszázmillió forintot nem halad meg;
- *különösen jelentős*, ha ötszázmillió forintot meghalad.

A kármérték összege az informatikában összetett fogalom: egyrészt tartalmaznia kell az eredeti állapothoz képest bekövetkező értékcsökkenést (mely sokszor az eredeti állapot helyreállítási költségeiből állapítható meg), az elmaradt hasznot, és a felmerült vagyoni és nem vagyoni értékcsökkenést, hátrányt.

Gondoljunk bele, egy üzemelő gyár számítógépes gyártásirányítási rendszerének vagy egy bank központi számítógépének tudatos tönkretételével milliárdos károkat lehet okozni! Elég, ha a kiesett forgalomra, az adatállományok helyreállításának költségére (ha egyáltalán lehetséges), vagy egy bank esetében az ügyfelek bizalomvesztésére gondolunk. Hatalmas az informatikai szakma felelőssége. Ezek szerint bűnöző lenne az a rendszergazda, akinek rendszere tönkremenetele során kára keletkezik?

Ez így nem lenne igazságos. A törvényalkotó figyelmes volt a jogszabály megalkotásánál. A szándékosan elkövetett cselekményeket emelte be a büntetőjogba. Jelen szabályozás alapján a gondatlanságból (tudatos gondat-

lanságból és hanyagságból) elkövetett cselekmény nem minősül bűncselekménynek, legyen az eredményben akár a szándékos bűncselekménnyel azonos eredményű. Ennek megértéséhez ki kell fejteni a *tudatosság* és a *szándékosság* közti különbséget. Tudatos minden olyan körülmény, amelyről tudunk, ismeretünk van róla, értelmünk átfogja. A szándékosság ennél több, mivel egyrészt tudatos (mert az általunk ismert körülményeken nyugszik), másrészt ennél is több, mert szándékosság

Btk. 300/C:

(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.

esetén az elkövető tudata átfogja a cselekmény által elérni kívánt célt-eredményt is.

Ez nem jelenti azt, hogy aki gondatlanságból követi el a károkozó cselekményét, az mentesülne a felelősségre vonhatóság alól. Nem, csak rá a felelősség más, például polgári jogi, munkajogi eseteit kell alkalmazni – kártérítési felelőssége ugyanúgy fennáll.

Gondatlanságból követi el a (bűn)cselekményt az, aki előre látja magatartásának lehetséges következményeit, de könnyelműen bízik azok elmaradásában; úgyszintén az is, aki e következmények lehetőségét azért nem látja előre, mert a tőle elvárható figyelmet vagy körültekintést elmulasztja.

A gondatlan magatartás akkor válik bűncselekménnyé, ha a Btk. Különös Része az adott tényállás gondatlan alakzatát is büntetni rendeli. Jelen esetünkben az informatikai cikkelyek nem tartalmaznak gondatlan tényállást, a gondatlan elkövetés itt tehát nem bűncselekmény (azonban a kártérítési felelősség polgári jogi vagy munkajogi úton ekkor is megállapítható).

Következésképpen az informatikai károkozásnál a felelősség megállapításánál általánosságban és nem büntetőjogi értelemben kell objektíve (szakmai írott és íratlan szabályok) és szubjektíve az adott helyzetben elvárható magatartás tanúsításának kötelezettségére alapozott felelősségről beszélnünk.

A gondatlanságnak két alakzata van: az egyik a tudatos gondatlanság, a másik a hanyagság. Tudatos gondatlanság esetén az elkövető előre látja magatartásának következményeit, de könnyelműen bízik azok elmaradásában. Ez különösen akkor állapítható meg, ha e bizalmát valamire alapozni tudta, például bízik a saját ügyességében, vagy valamilyen külső okban, ami



megakadályozhatta volna a következményeket. Hanyagság esetén az elkövetői oldalon a cselekmény előrelátása mint tudati elem és értelemszerűen a cselekményhez kapcsolódó érzelmi (lelki) elem is hiányzik. Nem törődik a várható következményekkel és nem is érdekli azok lehetséges kimenetele.

Nagyon fontos minőségi elhatárolást húzni a szándékos mulasztásban megnyilvánuló bűncselekmény (e törvény szerint büntetendő) és a jelen szempontból bűncselekménynek nem minősülő tudatos gondatlanság között. Tudatos gondatlanság esetén felmerül a várható káros kimenetel lehetősége, de bízom benne, hogy az vagy nem következik be, vagy bízom az ügyességemben, hogy képes leszek elhárítani.

Szándékos mulasztásban megnyilvánuló bűncselekmény esetén a várható káros kimenetel elérésére törekszem azáltal, hogy nem teszek semmit. Hagyom, hogy a folyamat úgy okozzon kárt, hogy nekem ne kelljen tevőlegesen közreműködnöm. A következő példával szeretném a különbséget megvilágítani.

A számítógépes rendszerben egy ismert számítógépes vírus jelenik meg, és nem irtják ki haladéktalanul, hanem megvizsgálják, milyen tüneteket okoz, hogyan deríthető fel, mit tapasztalható vele kapcsolatban, tehát abban bíznak, hogy a vírus későbbi kiirtása is lehetséges.

Tudatos gondatlanság esetén az illető bíz benne, hogy a rendszer használhatatlanná válása előtt vírusirtóval majd megfékezi a vírus terjedését, ám ha ez valamilyen oknál fogva mégsem sikerül, és a rendszer tönkremegy vagy működése akadályozott lesz, máris kész a tudatos gondatlanság esete.

A szándékos mulasztásos bűncselekmény esetén az elkövető tud a vírus megjelenéséről – adott esetben akár maga telepítette –, csak hogy nem avatkozik be, mert azt

akarja, hogy a vírus elterjedve kárt okozzon.

Egyes vírustípusoknál az illető egyéb műveletek (végtelen ciklusos lemez vagy memóriaművelet) végzésével a vírus fajtájától függően a számítástechnikai rendszerben tárolt, feldolgozott, kezelt vagy továbbított adatot jogosulatlanul megváltoztatja, törli vagy hozzáférhetővé teszi, a rendszer működését egyéb művelet végzésével jogosulatlanul akadályozza (a rendszert lelassítja, lassúságával üzemi használatra alkalmatlanná teszi).

A kérdés a szöveg olvastán magától adódik: lehet-e egy rendszer működését jogosultnak akadályozni? A válasz kézenfekvő: természetesen igen, gondoljunk csak a háttérben futó mentésre egy kiszolgálón, amelyet a jogosult rendszergazda indított el, és amely adott esetben az ügyfelek hangos tiltakozását okozza a rendszer lassúsága miatt. Még jó, ha nem ragadtatják magukat súlyosabb cselekményre! Igaz, itt felvetődik a szakmai kérdés: mikor kell ezeket a kapacitásigényes eljárásokat végezni, azaz rendelkezik-e róla a belső szabályzat vagy szokás, illetve mit mond a szakmai etika: illik-e feltartanom a többiekét? A szolgáltatásnak az elvárt szinten kell működnie – ez a szakmai etika alapkövetelménye. A törvényszöveg kapcsán felvetődő másik kérdés, hogy ki és mire jogosult? Ennek megválaszolásával azonban majd legközelebb foglalkozunk.



Grane István

Elektronikai műszerész, kajak-kenu-edző és immár Linux-rajongó is. 1998 óta helyi hálózatok tervezésével és kiszolgálóépítéssel foglalkozik, valamint a JPTE harmadéves joghallgatója. Szeret síelni, biciklizni, úszni – és még keresi az igazi nőt.

## Netcraft

A Netcraft webkiszolgáló-felmérése rendszerint örömteli hírekkel szolgál a Linux hívei számára, ám a legutóbbi, 2002. márciusi jelentésről ez nem mondható el.

A <http://www.netcraft.com/survey> weboldalon található grafikonokon látható az a küzdelem, amely az Apache és a Microsoft IIS webkiszolgálói között folyik 1998 óta. 2001-ben az IIS jelentősen csökkentette lemaradását az Apache-hoz képest, amely a webkiszolgálók piacának több mint hatvan százalékát uralta, végül azonban úgy tűnt, hogy 2002 februárjában a folyamat a viszályra fordul. Ám márciusban az IIS részesedése 4,89 százalékkal nőtt, míg az Apache-é 4,67 százalékot esett, így a fejlesztők ranglistáján (Top Developers) 57,36 százalékon áll az Apache és 34,02 százalékon az IIS.

A Netcraft szerint ez azt jelenti, hogy közel kétfélmillió webhelyen történt váltás „elsősorban annak eredményeként, hogy a register.com és a Network Solutions tartomány-

parkoló szolgáltatása windowsos kezelőfelületre költözött. A Register.com szolgáltatása eddig Apache kiszolgálón és Linux-rendszeren futott, jelenleg azonban a Windowsra való áttérés zajlik” (idézet a Netcraft jelentéséből).

A leparkolt tartományok szolgáltatásai természetesen sokban elmaradnak a tevékeny tartományokétól, így ez az adat a kiszolgálói oldalról nézve valószínűleg nem mond eleget a Világháló valós gyakorlati felhasználásáról. Mindazonáltal bosszantó, ha csak pár százalékponttal is kevesebbel dicsekedhetünk.

Talán ha befejeződik a nagy tartománynev-kibocsátók átállása a Sötét oldalra, az Apache részesedésének gyengülése is megszűnik, sőt, akár meg is fordul.

Doc Searls

Linux Jorunal, 2002. május, 97. szám