Dr. Papp Tibor LL.M.

TITKOS ADATSZERZÉS ÉS NEMZETKÖZI EGYÜTTMŰKÖDÉS A SZOFTVEREK JOGOSULATLAN LETÖLTÉSÉNEK ÉS TELEPÍTÉSÉNEK BIZONYÍTÁSA KÖRÉBEN

1. BEVEZETÉS

A szoftverekkel kapcsolatos, vagyoni természetű szerzői jogok büntetőjogi védelmének jogszabályi alapját a Büntető Törvénykönyvről szóló 1978. évi IV. törvényt (a továbbiakban: Btk.) módosító 1993. évi XVII. törvény 72. §-a teremtette meg. A jogalkotó az ezen célt szolgáló tényállást (Btk. 329/A. §) keretdiszpozícióként – vagyis másik jogágazathoz tartozó norma megsértéseként – fogalmazta meg, eredetileg „szerzői és szomszédos jogok megsértése" elnevezéssel, amelyet a szerzői jogról szóló 1969. évi III. törvény rendelkezései töltöttek meg tartalommal. Az új tényállás alkalmazása eleinte nem volt zökkenőmentes, de hamarosan letisztult a gyakorlat. Voltak persze olyan gondok is, amelyek megoldására többet kellett várni, például a tényállás címében szereplő „és" kötőszót – amely a jogalkotó eredeti szándékától eltérő jelentést hordozott, és ebből adódóan komoly értelmezési problémákat okozott – csak az 1999. évi CXX. törvénnyel cserélték „vagy"-ra.[1]

A számítástechnika és az információtechnológia további fejlődése, valamint az internethasználat hétköznapivá válása sok tekintetben új helyzetet teremtett, ezért nemcsak a jogalkotónak kellett újragondolnia az illegális szoftverhasználat visszaszorítását célzó szabályozást, hanem a bűnüldöző szerveknek is fel kellett készülniük a kihívásokra. Ebben a szellemben számos, a jogszabályi hátteret érintő változás következett be. A Btk. a 2001. évi CXXI. törvénnyel történt módosítás óta „szerzői vagy szerzői joghoz kapcsolódó jogok megsértése" néven határozza meg a bűncselekményt,[2] a tényállás szövege szabatosabb, a szabályozás pedig differenciáltabb lett. Időközben hatályba lépett a korábbi szerzői jogi törvényt felváltó 1999. évi LXXVI. törvény (a továbbiakban: Szjt.), a büntetőeljárásról szóló 1998. évi XIX. törvény (a továbbiakban: Be.), és az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban: Eht.) is. A legnagyobb változást azonban az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezménye eredményezte, amelyet hazánkban a 2004.

[1] A „vagy" kötőszó alkalmazása egyébként sokkal inkább összhangban van a bűncselekmény törvényi egységként való megfogalmazásával. Ahogyan arra a Legfelsőbb Bíróság is rámutat (BH 2000. 288.), a Btk. 329/A. §-a szerinti tényállás úgynevezett összefoglalt bűncselekmény: egyrészt a „szerzői jogok", másrészt pedig az ehhez hasonló és ezzel rokon „kapcsolódó jogok" megsértőit rendeli büntetni. Ez a törvényszakasz tehát külön-külön is önálló deliktumnak minősülő törvényi tényállásokat foglal egybe (esetleges együttes előfordulásuk esetére), kizárva ezzel a bűnhalmazat megállapításának lehetőségét.

[2] Az egyezmény hivatalos magyar nyelvű szövege még mindig szomszédos jogokat említ annak ellenére, hogy az Szjt. 2002. január 1-je, a Btk. pedig 2002. április 1-je óta szerzői joghoz kapcsolódó jogokról szól, és az egyezmény angol nyelvű szövege is a „related rights" kifejezést használja.

évi LXXIX. törvénnyel hirdetettek ki. Az egyezményt 2001. november 23-án, Budapesten írták alá, hatálybalépésére azonban csak 2004-ben került sor. A magyar jogalkotó igyekezett az átültetéssel, és már a 2002. évi I. törvénnyel megpróbálta az egyezmény rendelkezéseihez igazítani a hazai szabályozást.

A Btk. 329/A. §-a nem sorolja fel a lehetséges elkövetési magatartásokat, a bűncselekmény ugyanis bármely olyan magatartással megvalósítható, amely a szoftverrel kapcsolatos vagyoni természetű szerzői jogokat haszonszerzés végett vagy vagyoni hátrányt okozva megsérti.[3] Annak megítélésénél, hogy egy cselekmény illeszkedik-e a törvényi tényállás keretei közé, szem előtt kell tartani a Btk. 329/A. §-ának – már említett – keretdiszpozíció-jellegét. Rendkívül fontos, hogy az Szjt. 59. §-ának (2) bekezdése szerint a felhasználási szerződésben sem zárható ki, hogy a felhasználó egy biztonsági másolatot készíthessen a szoftverről, ha az a felhasználáshoz szükséges. A biztonsági másolat készítésével tehát a felhasználó nem követ el bűncselekményt.[4] Emellett arra is figyelemmel kell lenni, hogy mivel az Szjt. számos diszpozitív rendelkezést tartalmaz, így elképzelhető, hogy bizonyos megengedett felhasználási módokat a szerződés kizár, vagy a szerző jogosultságai közül egyeseket átruház, ezért a bűncselekmény megvalósulását mindig csak a konkrét felhasználási szerződés ismeretében lehet megállapítani. Ennek jogszabályi alapját az Szjt. 9. §-ának (6) bekezdése teremti meg, amelynek értelmében a jogszerző a vagyoni jogokkal (így a többszörözés, a terjesztés és a nyilvánossághoz közvetítés jogával) csak a jogok átruházására irányuló szerződés eltérő kikötése hiányában rendelkezhet a továbbiakban. A gyakorlatban persze az a jellemző, hogy a szerzői jog jogosultja igyekszik minél szűkebbre szorítani a felhasználási lehetőségeket, és szinte minden esetben kiköti, hogy a felhasználó a vagyoni jogok nagy részével nem rendelkezhet. Mindezek alapján azt mondhatjuk, hogy a szoftverek interneten keresztül, jogdíjfizetés nélkül, akár egyetlen példányban történő letöltése és telepítése rendszerint még abban az esetben is bűncselekménynek minősül, ha azt az elkövető nem forgalomba hozatal vagy jövedelemszerzés céljából, hanem kizárólag saját felhasználásra végzi, feltéve, hogy fennáll a haszonszerzési célzat, vagy bekövetkezik a vagyoni hátrány.[5]

---

[3] Az egyezmény 10. cikke szerint a részes államoknak a szerzői jogok megsértését csak abban az esetben kell büntetendővé nyilvánítaniuk, ha azt szándékosan, kereskedelmi méretekben és számítástechnikai rendszer útján követik el. Első ránézésre úgy tűnhet, hogy a magyar szabályozás nem szigorúbb, mint amelyet Magyarországnak az egyezmény alapján ki kell alakítania, hiszen a Btk. 10. §-a (2) bekezdésének és a 329/A. §-a (1) bekezdésének összevetésével megállapítható, hogy csak a szándékos elkövetés jelent bűncselekményt, a szoftverek letöltése és telepítése pedig egyébként is csak számítástechnikai rendszer útján lehetséges. Az egyezmény 10. cikke azonban az alapeset megvalósulásához megkívánja a kereskedelmi méretekben történő (magyar szóhasználattal: üzletszerű) elkövetést, míg a hazai szabályozás szerint a cselekmény enélkül is büntetendő, hiszen az üzletszerűséget külön minősített esetként kezeli a Btk.

[4] Ezzel összhangban jegyzi meg a Legfelsőbb Bíróság (BH 2003. 101.), hogy téves az az álláspont, amely szerint a számítógépi program egy példányban való magáncélú másolása a forgalomba hozatal vagy jövedelemszerzés célzata nélkül is minden esetben sérti a szerzői jogokat. Ha ugyanis a program megvásárlásával a jogdíjat megfizetik, a vásárló a magáncélú másolat készítésével nem sérti meg a szerző jogos érdekeit, mivel ilyen esetben a hordozó árában benne rejlő „üreskazetta-díj" kompenzálja annak jogos igényeit.

[5] BH 2000. 288.; BH 2003. 101.

Amennyiben a bizonyítékok rendelkezésre állnak, a szoftver telepítésének megtörténte viszonylag könnyen megállapítható. Az az igazán érdekes, hogy milyen módon szerezhetők meg a letöltést valószínűsítő bizonyítási eszközök, és hogyan képesek együttműködni a hatóságok a határokon átívelő internetbűnözés megfékezésében. Éppen ezért jelen cikk keretei között azt vizsgáljuk, miként valósul meg a titkos adatszerzés és a nemzetközi kooperáció a szoftverek interneten keresztül történő jogellenes megszerzése legjellemzőbb formájának, az úgynevezett warez-oldalakról[6] történő letöltések esetében.

2. TITKOS ADATSZERZÉS

2.1. A TITKOS ADATSZERZÉSBEN REJLŐ LEHETŐSÉGEK

2.1.1. Általában

A titkos adatszerzés az egyéb bűncselekmények bizonyításában is komoly segítséget jelent a hatóságoknak, a leghatékonyabban azonban az internetes környezetben megjelenő bűncselekmények vonatkozásában alkalmazható. Ennek oka az internetszolgáltató[7] titkos adatszerzésben való közreműködését előíró szabályokban keresendő. Ezek alapján a szolgáltató minden olyan adatot jogosult és köteles kezelni, amelyekből nagy biztossággal megállapítható az elkövető személye, és bizonyítható a bűncselekmény megtörténte, így a hatóságok feladata meglehetősen leegyszerűsödik.

Az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezménye 20. és 21. cikke alapján a tagállamok kötelesek megteremteni annak jogszabályi alapját, hogy hatóságaik kötelezhessék a szolgáltatókat a forgalmi adatok[8] valós idejű összegyűjtésére és a tartalomra vonatkozó adatok kifürkészésére. Az ezt lehetővé tevő szabályokat a magyar jogalkotó a Be.

---

[6] A warez-oldalon olyan honlapokat értünk, amelyen keresztül rendszerint jogszerűtlenül letöltésre kínált szoftverek, hangfelvételek, képek, filmalkotások stb. érhetők el. A letöltés a legtöbb esetben nem ingyenes, a felhasználónak általában emelt díjas sms-t kell küldenie az oldalon feltüntetett telefonszámra, amiért egy korlátozott ideig használható, az adatokhoz való hozzáférést biztosító jelszót kap.

[7] Az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezménye 1. cikkének *c)* pontja szerint szolgáltató minden olyan közjogi és magánjogi alany, amely a szolgáltatásait igénybevevőknek biztosítja egy számítástechnikai rendszer általi érintkezés lehetőségét, és minden más olyan alany, amely a kommunikációs szolgáltatásnak, illetve az azt igénybevevők részére számítástechnikai adatokat feldolgoz vagy tárol. Az Eht. nem használja az internetszolgáltató kifejezést, a 188. § 14. pontja ehelyett az elektronikus hírközlési szolgáltató fogalmát határozza meg. Ennek minősül az elektronikus hírközlési hálózat üzemeltetője, valamint az elektronikus hírközlési szolgáltatást nyújtó természetes, illetve jogi személy vagy jogi személyiséggel nem rendelkező gazdasági társaság.

[8] Az egyezmény 1. cikkének *d)* pontja szerint forgalmi adat minden olyan, a számítástechnikai rendszeren átmenő és a számítástechnikai rendszer mint a kommunikációs lánc egyik eleme által létrehozott, kommunikációra vonatkozó adat, mely jelzi a kommunikáció eredetét, rendeltetési helyét, útvonalát, idejét, napját, terjedelmét és időtartamát vagy a szolgáltatás típusát. Ezekhez az Eht. 157. §-ának (2) bekezdése – egyebek mellett – hozzáteszi a díjfizetéssel és a díjtartozással összefüggő adatokat, valamint tartozás hátrahagyása esetén az előfizetői szerződés felmondásának eseményeit.

bírói engedélyhez kötött titkos adatszerzésről szóló, V. címében helyezte el, de ugyanilyen fontosak az Eht. idevágó rendelkezései is.[9]

2.1.2. A szolgáltató által kezelt adatok

2.1.2.1. A forgalmi adatok

Az Eht. a Forgalmi és számlázási adatok cím alatt rendezi a forgalmi adatok átadásának esetköreit. A 157. § (6) bekezdésének *c)*, valamint (2) bekezdésének *b)–c)*, és *f)–g)* pontja szerint a közvádas bűncselekmények üldözése céljából az internetszolgáltató átadhatja azon adatokat a hatóságoknak, amelyekből megállapítható az előfizetői állomás azonosítója, az előfizető címe és az állomás típusa, a szolgáltatás típusa, iránya, kezdő időpontja, illetve a továbbított adat terjedelme, az IP-azonosító[10] és a szolgáltatás dátuma. Ezek az információk már önmagukban is komoly segítséget jelentenek a hatóságoknak, hiszen ezekből megállapítható, hogy ki volt az internetszolgáltatás igénybevevője, mikor, és mekkora adatállományt töltött le a warez-szerverről.

2.1.2.2. A tartalomra vonatkozó adatok

Bár a forgalmi adatok nélkülözhetetlenek a vádemelés megfelelő megalapozásához, a legfontosabb bizonyítékot mégis a tartalomra vonatkozó adatok jelentik. Ezekből derül ki ugyanis, hogy mit töltött le az elkövető, vagyis a tartalomra vonatkozó adatok segítségével azonosítható be a bűncselekmény elkövetési tárgya, a szoftver. Csak ezen adatok ismeretében nyílik mód a jogaiban sértett szerző személyének meghatározására és a vagyoni hátrány megállapítására.

Az egyezmény 21. cikke – felismerve a tartalomra vonatkozó adatok kifürkészésében megnyilvánuló hatósági túlsúlyt – tartalmaz egy fontos megszorítást: ezen eszköz alkalmazásának csak a belső jogban meghatározott, súlyos bűncselekmények esetén van helye.

---

[9] E sorok szerzőjének véleménye szerint az egyezmény 20. és 21. cikkének átültetése nem sikerült tökéletesen, hiszen a Be. – az egyezménnyel ellentétben – nem különíti el egymástól a forgalmi adatok és a tartalomra vonatkozó adatok megszerzésének intézményét, holott a kettő között jelentős a fogalmi különbség. A magyar jogalkotó azonban más tekintetben is következetlen. A Be. ugyanis – szintén az egyezménytől eltérően – nem csupán a tartalomra vonatkozó adatok kifürkészésének, hanem forgalmi adatok megszerzésének is csak meghatározott esetekben enged teret. Első ránézésre úgy tűnhet, hogy ezzel a magyar szabályozás a hatóságok túlsúlyát igyekszik ellensúlyozni, ha viszont szemügyre vesszük a titkos adatszerzés elrendelésének lehetséges eseteit, kiderül, hogy a jogalkotó inkább növeli a hatósági dominanciát.

[10] Az IP-cím az internetre csatlakozó számítógépek egyedi azonosítója. A jelenlegi szabvány szerint négy, pontokkal elválasztott decimális számból áll (aaa.bbb.ccc.ddd), ahol az egyes számok értéke 0-tól 255-ig terjedhet.

2.2. A TITKOS ADATSZERZÉS ALKALMAZÁSÁNAK TÁRGYI ÉS SZEMÉLYI KÖRE

A Be. 200. §-a (1) bekezdésének *c)* pontja szerint az ügyész és a nyomozóhatóság bírói engedély alapján az elkövető kilétének, tartózkodási helyének megállapítása, elfogása, valamint bizonyítási eszköz felderítése érdekében a nyomozás elrendelésétől a nyomozás iratainak ismertetéséig az érintett tudta nélkül a számítástechnikai rendszer[11] útján továbbított és tárolt adatokat megismerheti és felhasználhatja.

Titkos adatszerzésnek csak meghatározott esetekben van helye.[12] Tekintettel arra, hogy a szoftverek letöltése sokszor külföldi szerverekről történik (márcsak azért is, mert a legszélesebb körben használt programokat nem hazánkban fejlesztik), ráadásul gyakran továbbértékesítés céljából, a titkos adatszerzésnek a (2) bekezdés *b)* és *d)* pontjában meghatározott esetekben van a legnagyobb jelentősége. Eszerint az ügyész és a nyomozóhatóság titkos adatszerzést alkalmazhat, ha az eljárás országhatáron átnyúló bűnözéssel kapcsolatos, illetve sorozatban vagy szervezett elkövetéssel megvalósuló (ideértve az üzletszerűen, bűnszövetségben vagy bűnszervezetben történő elkövetést is) bűncselekmény vagy ilyen bűncselekmény kísérletének, illetőleg előkészületének gyanúja miatt folyik.[13]

---

[11] Az egyezmény 1. cikkének *a)* pontja szerint számítástechnikai rendszer minden olyan eszköz, illetőleg egymással kapcsolatban lévő vagy összekötött eszközök összessége, amelyek, illetőleg amelyeknek egy vagy több eleme egy adott programnak megfelelően adatok automatikus feldolgozását végzi. A Btk. 300/F. §-ának (3) bekezdése is tartalmaz egy definíciót, amelyet a 2001. évi CXXI. törvény iktatott be. Eszerint számítástechnikai rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés vagy az egymással kapcsolatban lévő ilyen berendezések összessége. A módosító törvény indoklása megemlíti, hogy a fogalommeghatározás összhangban van az egyezmény idevágó rendelkezésével, holott az más definíciót tartalmaz. Emellett a Btk. fogalommeghatározása nem általánosan, hanem csak a 300/C. § (Számítástechnikai rendszer és adatok elleni bűncselekmény) és a 300/E. § (Számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása) vonatkozásában irányadó. A gyakorlatban számítástechnikai rendszernek tekintendők a számítástechnikai adatfeldolgozásra épülő, memóriával rendelkező olyan egységek is, amelyek megjelenésükben nem hagyományos számítógépet jelentenek. Ebbe a körbe tartoznak a közcélú távbeszélő-szolgáltatás, illetve közcélú mobiltelefon-szolgáltatás igénybevételére szolgáló elektronikus kártyák, a közcélú mobiltelefont vezérlő mikroszámítógépek, valamint a számítástechnikai berendezések felhasználásával működő hírközlési, telekommunikációs rendszerek is. A számítástechnikai rendszer fogalma azonban nemcsak az egyes berendezésekre terjed ki, hanem felöleli az azok összekapcsolása révén létrejött hálózatot, valamint az adattovábbítást, a kapcsolatfelvételt biztosító műszaki berendezéseket is. Az egyes berendezések közötti kapcsolat nem jelent feltétlenül fizikai összekapcsoltságot. A számítástechnikai rendszerek között az összeköttetés létrejöhet elektronikus vagy optikai jeleket továbbító kábelek vagy vezetékek útján, valamint rádióhullámok, infravörös, illetve rövidhullámok segítségével vagy műholdas sugárzás igénybevételével is. A fentiekből kitűnik, hogy maga az egyes számítógép-konfiguráció (tehát az alapgép a hozzá tartozó bemeneti és kimeneti perifériákkal együtt) is számítástechnikai rendszernek minősül.

[12] Természetesen az ügyészség a Be. 201. §-ának (1) bekezdésben meghatározott bűncselekmények mellett a Be. 28. §-a (4) bekezdésének *e)* pontja alapján magához vont, a Be. 29. §-ában meghatározott kizárólagos hatáskörébe, valamint a Be. 474. §-ának (2)-(4) bekezdése szerint a katonai ügyész hatáskörébe tartozó ügyekben is végezhet titkos adatszerzést.

[13] A magyar jogalkotó különös megoldást alkalmaz a tartalomra vonatkozó adatok kifürkészése (és az elhatárolás már említett hiánya miatt a forgalmi adatok megszerzése) tekintetében. Erre ugyanis az egyezmény 21. cikke alapján csak a belső jogban meghatározott súlyos bűncselekmények esetén kerülhet sor, a magyar jogszabály viszont nem konkrét tényállásokat határoz meg, hanem az elkövetési tárgyra, az elkövetés módjára és a bűncselekmény passzív alanyára vonatkozó ismérvek, illetve a büntetési tétel alapján teszi lehetővé a továbbított adatok tartalmának megismerését. A feltételek vagylagosak, tehát önmagukban elegendőek a titkos adatszerzés elrendeléséhez. Ez azt jelenti, hogy egy játékprogram saját használat céljára történő, egyszeri letöltése egy amerikai szerverről olyan súlyos bűncselekménynek minősül, amellyel kapcsolatban titkos adatszerzésre kerülhet sor. Ez a szabályozás tehát csakugyan figyelembe veszi az internetbűnözés gyakran emelgetett – és az egyezmény szövegében is megjelenő – határokon átívelő jellegét, ugyanakkor kissé túlzónak tűnik.

A Be. 202. §-ának (1)–(2) bekezdése határozza meg azt a személyi kört, amelyekkel szemben titkos adatszerzést lehet folytatni. Ez elsősorban a gyanúsított, illetve az a személy, aki a bűncselekmény elkövetésével a nyomozás addigi adatai alapján gyanúsítható, másodsorban pedig az, akinek az előbb említettekkel való bűnös kapcsolattartására adat merült fel, vagy ilyen kapcsolat megalapozottan feltehető. A titkos adatszerzésnek nem akadálya, ha az kívülálló személyt elkerülhetetlenül érint. Látható, hogy a Be. meglehetősen tágan állapítja meg a potenciális érintettek körét.

2.3. AZ INTERNETSZOLGÁLTATÓ KÖZREMŰKÖDÉSÉRE VONATKOZÓ TOVÁBBI SZABÁLYOK

A Be. 204. §-ának (1)–(2) bekezdése értelmében a titkos adatszerzést a külön törvényben meghatározott szervezet hajtja végre. A számítástechnikai rendszer útján rögzített adatok továbbítását, feldolgozását, kezelését végző szervezetek kötelesek a titkos adatszerzés végrehajtását biztosítani, és a titkos adatszerzésre jogosult hatóságokkal együttműködni [a szolgáltató ugyanezen kötelezettségét rögzíti az Eht. 92. §-ának (1) bekezdése is].

A szolgáltató az Eht. 92. §-ának (2) bekezdése alapján a szolgáltatás megkezdésével egyidejűleg az általa használt, működtetett berendezések, helyiségek és az együttműködő személyek tekintetében köteles biztosítani az elektronikus hírközlési hálózatban továbbított küldemények, közlések, továbbá a szolgáltató által kezelt adatok titkos adatszerzéssel történő megismeréséhez szükséges eszközök és módszerek alkalmazási feltételeit. Ezenkívül a Nemzetbiztonsági Szakszolgálat kérésére a szolgáltatás műszaki jellemzői alapján a szükséges mértékben köteles biztosítani a bevezetett szolgáltatással kapcsolatban a titkos adatszerzés eszközeit a kilépési pontig.

Az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezménye 20–21. cikke a szolgáltatókat azok műszaki lehetőségeihez mérten kötelezi az adatok rögzítésére és átadására. Az Eht. ennél szigorúbban fogalmaz, amikor a (3) bekezdésben rögzíti, hogy az előbb említett kötelezettségei teljesítése érdekében a szolgáltató köteles megfelelő műszaki rendszert – így különösen alapkiépítésű monitoring alrendszert – létesíteni, és ennek elérhetőségét hálózatában a kilépési pontig biztosítani a Nemzetbiztonsági Szakszolgálat részére az erre vonatkozó igényről való írásbeli tudomásszerzéstől számított hat hónapon belül. Az alapkiépítésű monitoring alrendszer valamennyi költségét a szolgáltató viseli. A (4) bekezdés szerint az adatszolgáltatás teljesítése térítésmentes.

2.4. GARANCIÁLIS SZABÁLYOK

A titkos adatszerzés jellegéből adódik, hogy annak végzése és a nyert információk felhasználása különös eljárási biztosítékokat igényel. Az egyezmény 20–21. cikkei külön kiemelik, hogy a titkos adatszerzés csak a 15. cikkben rögzített garanciális rendelkezések betartása mellett folytatható.

A Be. 205. §-ának (1), (3) és (5) bekezdései alapján a titkos adatszerzés során keletkezett és rögzített adatok megóvásáról az ügyész, illetve a titkos adatszerzést folytató nyomozóhatóság az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvényben szabályozottak szerint gondoskodik. A bíró megkeresésére a titkos adatszerzés során a megkeresés időpontjáig beszerzett adatokat az ügyész köteles bemutatni. Ha a bíró megállapítja, hogy az engedély kereteit túllépték, a titkos adatszerzést megszünteti, más törvénysértés esetén a titkos adatszerzést megszüntetheti. Az ügyész a titkos adatszerzés tényéről – annak befejezését követően – értesíti a bírói engedélyben érintettet, ha az érintett ellen nem indult büntetőeljárás, és az értesítés a büntetőeljárás sikerét nem veszélyezteti. Ugyanezt írja elő az ügyész számára a védelőkészítéssel, a nyomozás törvényessége feletti felügyelettel és a vádemeléssel kapcsolatos ügyészi feladatokról szóló 11/2003. (ÜK. 7.) LÜ utasítás 62. §-ának (3) bekezdése is.

2.5. A TITKOS ADATSZERZÉS EREDMÉNYÉNEK FELHASZNÁLÁSA

Ha az ügyész a titkos adatszerzés eredményét a büntetőeljárásban bizonyítékként kívánja felhasználni, a Be. 206. §-a alapján a titkos adatszerzés engedélyezése iránti indítványt, a bíróság határozatát és a titkos adatszerzés végrehajtásáról készített jelentést csatolja a nyomozás irataihoz. A jelentés az okiratra vonatkozó szabályok szerint használható fel bizonyítékként. A már említett LÜ utasítás 62. §-ának (1) bekezdése szerint a titkosan szerzett adatot az ügyész a büntetőeljárásban bizonyítékként akkor használja fel, ha az mással nem pótolható.

3. NEMZETKÖZI EGYÜTTMŰKÖDÉS

3.1. A NEMZETKÖZI EGYÜTTMŰKÖDÉS JELENTŐSÉGE

A tömegszerűen használt operációs rendszerek, irodai szoftverek és játékprogramok külföldi fejlesztésűek, így azok a legkönnyebben az interneten keresztül kerülhetnek jogszerűtlenül hazánkba. A magyar warez-oldalak üzemeltetői az általuk illegálisan forgalmazott szoftvereket általában külföldi szerverekről töltik le, és csak ezután mellékelnek hozzájuk (esetleg) magyar nyelvű leírásokat, kiegészítőket. Az illegális szoftverletöltés tipikusan olyan cselekmény, amelynek vonatkozásában az országhatárok nem jelentenek akadályt. Éppen ezért elkerülhetetlenné vált egy olyan hatékony, közös kriminálpolitika kidolgozása, amely meg tud felelni a számítástechnikai bűnözés ezen formája által állított kihívásoknak. Ehhez pedig nemcsak a nemzeti szabályok összehangolására és egységes nyomozási intézkedések kidolgozására van szükség, hanem a nemzetközi együttműködés továbbfejlesztésére is.

3.2. A NEMZETKÖZI EGYÜTTMŰKÖDÉSRE VONATKOZÓ LEGFONTOSABB JOGSZABÁLYOK

A hatékony együttműködés kereteinek kialakítása érdekében több hazai és nemzetközi jogforrás született. Az előbbiek körébe tartozik a nemzetközi bűnügyi jogsegélyről szóló 1996. évi XXXVIII. törvény (a továbbiakban: Nbjtv.), az Európai Unió bűnüldözési információs rendszere és a Nemzetközi Bűnügyi Rendőrség Szervezete keretében megvalósuló együttműködésről és információcseréről szóló 1999. évi LIV. törvény, valamint az Európai Unió tagállamaival folytatott bűnügyi együttműködésről szóló 2003. évi CXXX. törvény is. A már sokszor említett, az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezménye mellett a nemzetközi jogforrások közé tartozik a 1994. évi XIX. törvénnyel kihirdetett, Strasbourgban, 1959. április 20-án kelt, a kölcsönös bűnügyi jogsegélyről szóló európai egyezmény, valamint a 2005. évi CXVI. törvénnyel kihirdetett, az Európai Unió tagállamai közötti kölcsönös bűnügyi jogsegélyről szóló, 2000. május 29-én kelt egyezmény.

Tekintettel arra, hogy az illegális szoftverletöltés vonatkozásában az említett jogszabályok közül csak az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezménye tartalmaz speciális rendelkezéseket[14] – és az is mindössze a kiadatás és az eljárási jogsegély vonatkozásában –, csupán ezeknek a kifejtésére szorítkozunk, utalva az Nbjtv.-vel való összefüggésekre. Megjegyzendő, hogy az egyezmény a nemzetközi együttműködés szabályozása tekintetében más megoldást követ, mint amit az egyéb szabályozási tárgykörök esetében. Míg a többi előírás javarészt jogalkotási kötelezettséget telepített az aláíró államokra, vagyis azt határozta meg, hogy milyen tartalmúnak kell lenniük a nemzeti jog vonatkozó részeinek, addig a nemzetközi együttműködésre vonatkozó normák többsége közvetlenül az egyezményt kihirdető 2004. évi LXXIX. törvény rendelkezéseinek alkalmazásával érvényesül.

3.3. KIADATÁS

3.3.1. Kiadatás Magyarországról

Az Nbjtv. 11. §-ának (1) bekezdése szerint Magyarországon tartózkodó személy külföldi állam megkeresésére büntetőeljárás lefolytatása, szabadságvesztés-büntetés, illetőleg szabadságelvonással járó intézkedés végrehajtása céljából adható ki. Illegális szoftverletöltés miatt az egyezmény 24. cikk 1. bekezdésének *a)* pontja alapján csak abban az esetben kerülhet sor kiadatásra, ha az mindkét érintett állam jogszabályai szerint legalább egy év vagy ennél

[14] Mindez természetesen nem jelenti azt, hogy az egyezmény ne venné figyelembe az egyéb megállapodásokban rögzített szabályokat; 23. cikke kifejezetten arra utal, hogy a kooperáció a részes államok a büntetőjogi tárgyú nemzetközi együttműködésre vonatkozó nemzetközi szerződései, az egységes vagy kölcsönös jogi szabályozásukon alapuló megállapodásai, valamint a nemzeti jogok alkalmazásával történik.

súlyosabb szabadságvesztéssel büntetendő. Tekintettel arra, hogy a Btk. 329/A. §-a a bűncselekmény alapesetét is két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel fenyegeti, magyar oldalról adottak a kiadatás feltételei. Az Nbjtv. 11. §-ának (2) bekezdése további feltételeket határoz meg. Eszerint büntetőeljárás lefolytatása céljából akkor van helye kiadatásnak, ha az a cselekmény, amely miatt a kiadatást kérik, mind a magyar törvény, mind a megkereső állam törvénye szerint egy évet meghaladó szabadságvesztéssel büntetendő, szabadságvesztés-büntetés vagy szabadságelvonással járó intézkedés végrehajtás céljából pedig akkor, ha a kiszabott szabadságvesztés vagy az alkalmazott intézkedés még végrehajtható része a hat hónapot meghaladja.

Az Nbjtv. 18., 20. és 26. §-ai megosztják a feladatokat az igazságügyminiszter és a bíróság között. A kiadatás iránti megkereséseket az igazságügy-miniszter fogadja, és – amennyiben az nem jár a Magyar Köztársaság felségjogainak csorbításával, biztonságának veszélyeztetésével, illetve közrendjének sérelmével – haladéktalanul megküldi a Fővárosi Bíróságnak. A bíróság meghallgatja a kiadni kért személyt, és a kiadatás feltételeinek fennállása esetén elrendeli kiadatási letartóztatását. A kiadatás kérdésében az igazságügy-miniszter dönt. Ha a bíróság határozatában azt állapította meg, hogy nem állnak fenn a kiadatás törvényben meghatározott feltételei, az igazságügy-miniszter a kiadatást a bíróság határozatára utalással tagadja meg.

Az Nbjtv. 27. §-a (1) bekezdésének értelmében a kiadott személy átadásáról az Országos Rendőr-főkapitányság Interpol Magyar Nemzeti Iroda a rendőrség közreműködésével gondoskodik.

Az Nbjtv. 30. §-ának (1) bekezdése alapján a Fővárosi Bíróság engedélyezheti olyan tárgyak átadását a megkereső állam részére, amelyek a kiadatás iránti megkeresés alapjául szolgáló bűncselekmény eszközéül szolgáltak, vagy azokat az elkövető e bűncselekmény útján szerezte meg, illetőleg a bűncselekmény útján megszerzett tárgyak helyébe léptek, vagy tárgyi bizonyítás eszközéül szolgálhatnak. Erre akkor is lehetőség van, ha a kiadatást engedélyezték, de a kiadni kért személy átadására nem került sor.

3.3.2. Külföldi állam megkeresése kiadatás iránt

Az Nbjtv. 31–33. §-ai alapján kiadatás iránti megkeresés büntetőeljárás lefolytatása, szabadságvesztés-büntetés, illetőleg szabadságelvonással járó intézkedés végrehajtása érdekében terjeszthető elő külföldi államnál. Ha külföldön tartózkodó olyan terhelt ellen kell büntetőeljárást lefolytatni, akivel szemben kiadatásnak van helye, a bíróság elfogatóparancsot bocsát ki, és az iratokat megküldi az igazságügy-miniszternek. A kiadatási kérelem előterjesztéséről az igazságügy-miniszter dönt, és döntéséről értesíti az elfogatóparancsot kibocsátó bíróságot.

3.4. AZ ELJÁRÁSI JOGSEGÉLY

3.4.1. Az eljárási jogsegély tárgyi köre

Az Nbjtv. nem határozza meg pontosan az eljárási jogsegély fogalmát, csupán példálózó jelleggel rögzíti annak lehetséges tárgyi körét. A 61. § (2) bekezdése szerint az eljárási jogsegély kiterjedhet különösen nyomozási cselekmények teljesítésére, bizonyítási eszközök felkutatására, a terhelt és a tanú kihallgatására, a szakértő meghallgatására, szemlére, házkutatásra, motozásra, lefoglalásra, Magyarországon való átszállításra, a büntetőeljárással kapcsolatos iratok és tárgyak megküldésére vagy iratok kézbesítésére, külföldön büntetőeljárás alá vont magyar állampolgár bűnügyi nyilvántartásban szereplő személyes, illetve egyéb adatairól való felvilágosítás adására és az ideiglenes átadásra.

3.4.2. Az eljárási jogsegély speciális formái

Az egyezmény nem használja ugyan az „eljárási jogsegély" kifejezést, azonban számos olyan, az illegális szoftverletöltés nyomozásának és bizonyításának szempontjából különös jelentőségű együttműködési formát szabályoz, amely a bizonyítási eszközök felkutatására irányul, és így beleillik az Nbjtv. példálózó felsorolásába.

3.4.2.1. Tárolt számítástechnikai adat gyors megőrzése

A tárolt számítástechnikai adat[15] gyors megőrzését az egyezmény úgynevezett ideiglenes intézkedésekkel kapcsolatos jogsegélynek tekinti, amely megelőzi a voltaképpeni jogsegélykérelem előterjesztését. Az egyezmény 29. cikke alapján a megkereső állam a másik félhez fordulhat annak érdekében, hogy az rendelje el, illetve kényszerítse ki a területén található számítástechnikai rendszer útján tárolt adatok gyors megőrzését, amelyekkel kapcsolatban az átvizsgálásra, az azokhoz való hozzáférésre, azok lefoglalására, illetve átadására vonatkozóan a megkereső állam jogsegélykérelmet kíván előterjeszteni. Ezzel a megelőző lépéssel hatékonyan biztosítható a warez-szerver változatlan állapotban való megőrzése, és így az egyik legfontosabb bizonyítási eszköz megóvása.

Előfordulhat, hogy – a megkeresett állam megítélése szerint – a megőrzés nem biztosítja megfelelően az adatok későbbi hozzáférhetőségét, veszélyezteti a megkereső állam által folytatott nyomozás titkosságát, illetve más módon hátrányosan befolyásolja azt. A megkeresett állam erről haladéktalanul értesíti a megkereső felet, aki dönt arról, hogy mindezek ellenére kéri-e a kérelem teljesítését.

[15] Az egyezmény 1. cikkének *b)* pontja szerint számítástechnikai adat tényeknek, információknak, illetőleg fogalmaknak minden olyan formában való megjelenése, mely számítástechnikai feldolgozásra alkalmas, ideértve azon programot is, mely valamely funkciónak a számítástechnikai rendszer által való végrehajtását biztosítja.

A megőrzés célja csupán az, hogy lehetővé tegye az adatok átvizsgálására, lefoglalására stb. irányuló megkeresés előterjesztését. Erre való tekintettel a megőrzés legfeljebb 60 napig tarthat. A kérelem megérkezését követően az adatokat meg kell őrizni annak elbírálásáig.

3.4.2.2. Megőrzött forgalmi adat gyors átadása

Az egyezmény 30. cikke szintén egy ideiglenes intézkedéssel kapcsolatos jogsegélyformát szabályoz, amely tulajdonképpen a tárolt számítástechnikai adat gyors megőrzésére irányuló megkeresés speciális esete. Alkalmazására akkor kerülhet sor, ha a megkeresett állam a meghatározott kommunikációhoz kapcsolódó forgalmi adat megőrzésére irányuló megkeresés teljesítése esetén megállapítja, hogy a kommunikáció továbbításában egy másik államban található szolgáltató is részt vett. Ekkor a megkeresett fél a kommunikáció továbbítására igénybe vett útvonal és a szolgáltató azonosítása érdekében megfelelő mennyiségű forgalmi adatot haladéktalanul átad a megkereső államnak.

3.4.2.3. Tárolt számítástechnikai adathoz való hozzáférésre vonatkozó jogsegély

Az egyezmény a 31. cikkben – továbbá a 32–34. cikkekben – szabályozott jogsegélyformát úgynevezett nyomozati jogkörrel kapcsolatos jogsegélynek tekinti. Ez a jogsegélykérelem arra irányul, hogy a megkeresett állam a területén található számítástechnikai rendszer útján tárolt adatokat vizsgálja át, azokhoz férjen hozzá, illetve azokat foglalja le, szerezze meg vagy adja át, ideértve természetesen azon adatokat is, amelyek megőrzését a megkereső állam korábban a 29. cikk alapján kérte. Ezen intézkedés alkalmazásával nyílik lehetőség az előzőleg már biztosított warez-szerveren tárolt adatok megszerzésére.

3.4.2.4. Forgalmi adat valós idejű összegyűjtésével kapcsolatos, valamint a tartalomra vonatkozó adat kifürkészésére vonatkozó jogsegély

A 33–34. cikkek alapján az egyezményben részes államok kölcsönösen jogsegélyt nyújtanak egymásnak a számítástechnikai rendszer útján továbbított, meghatározott kommunikációval összefüggő forgalmi adatok, illetve tartalomra vonatkozó adatok valós idejű összegyűjtésében és rögzítésében. A titkos adatszerzés kapcsán már utaltunk arra, hogy a tartalomra vonatkozó adatok kifürkészésének lehetősége biztosítja a legfontosabb eszközt az illegális szoftverletöltés nyomozásában és bizonyításában. A nemzetközi együttműködés körében ugyanekkora jelentőségű a jogsegély ezen formája.

3.4.3. Az eljárási jogsegély nyújtásának és a külföldi hatóság megkeresésének szabályai

Az eljárási jogsegély nyújtására az Nbjtv. 61. §-ának (1) bekezdése alapján a külföldi hatóság megkeresése alapján kerülhet sor.

A jogsegélykérelem alapján számítástechnikai eszközök és a titkos adatszerzésről készített jelentés is átadásra kerülhetnek. Ezen bizonyítási eszközök épségének megőrzése érdekében az Nbjtv. 67. §-a alapján a megküldés feltételéül szabható, hogy azokat az átadáskorival azonos állapotban szolgáltassák vissza.[16]

Az Nbjtv. 70. §-ának értelmében az eljárási jogsegély iránti megkereséseket a legfőbb ügyész fogadja, és – ha fennállnak a jogsegély teljesítésének előfeltételei – gondoskodik azoknak az általa a jogsegély teljesítésére kijelölt ügyészhez történő eljuttatásáról. Ha a külföldi igazságügyi hatóság az eljárási jogsegélynek kifejezetten bíróság által történő teljesítését kéri, vagy ha az a magyar jog szerint a bíróság által teljesíthető, a legfőbb ügyész a jogsegélykérelmet megküldi az igazságügy-miniszternek, aki azt a teljesítés végett az illetékes bíróságnak továbbítja. A megkeresés teljesítését követően, illetőleg ha a megkeresés teljesítése elháríthatatlan akadályba ütközik, vagy ha a megkeresés teljesítése során olyan körülmények merülnek fel, amelyek folytán nincs helye az eljárási jogsegély iránti megkeresés teljesítésének, az iratokat az akadály megjelölésével az ügyész a legfőbb ügyésznek, a bíróság pedig az igazságügy-miniszternek küldi meg.

Az eljárási jogsegély teljesítéséről az Nbjtv. 71. §-a alapján a legfőbb ügyész, illetőleg az igazságügy-miniszter értesíti a megkeresést előterjesztő igazságügyi hatóságot. Ugyancsak értesíti e hatóságot – az ok megjelölésével – arról is, ha a jogsegély iránti megkeresés nem, vagy csak részben volt teljesíthető.

Az Nbjtv. 72. §-a a külföldi hatóság magyar részről történő megkeresésének esetére is az eljárási jogsegély nyújtására vonatkozó előírásokat rendeli alkalmazni. A külföldi igazságügyi hatósághoz intézett megkereséseket az Nbjtv. 73. §-a alapján a bíróság az igazságügy-miniszternek, az ügyész a legfőbb ügyészhez küldi meg továbbítás végett.

3.5. A NEMZETKÖZI EGYÜTTMŰKÖDÉST SZOLGÁLÓ INFORMÁCIÓCSERE, HOZZÁFÉRÉS AZ ADATOKHOZ AZ ÉRINTETT ÁLLAM ENGEDÉLYE NÉLKÜL

3.5.1. Általában

Az illegális szoftverletöltés és a számítástechnikai úton elkövetett egyéb bűncselekmények nyomozása, valamint az államok ezen a téren megvalósuló nemzetközi együttműködése során különös jelentősége van a gyors információáramlásnak. Ha a különböző államok hatóságai közti információcsere akadozik, az könnyen a büntetőeljárás sikerének meghiúsulásához vezethet. Ezt felismerve az egyezmény több olyan lehetőséget is biztosít, amelynél fogva egyrészt gördülékenyebbé és folyamatossá válhat a társhatóságok kommunikációja, másrészt a bűnüldöző szervek – meghatározott feltételek fennállása esetén – az idegen állam engedélye nélkül is hozzáférhetnek bizonyos adatokhoz.

[16] A tárgyak megküldése természetesen nem érinti az azokon fennálló tulajdonjogot és egyéb jogokat.

3.5.2. A 24/7 hálózat

A gyors információcsere legfontosabb intézményesült formája az úgynevezett 24/7 hálózat. Az egyezmény 35. cikke egy éjjel-nappal, a hét minden napján elérhető kapcsolattartási pont kijelölésére kötelezi a részes államokat annak érdekében, hogy lehetővé tegyék a számítástechnikai adatokkal és rendszerrel összefüggő bűncselekményekre vonatkozó nyomozásokkal vagy a bűncselekményekre vonatkozó elektronikus bizonyítékok összegyűjtésével kapcsolatos azonnali segítségnyújtást. Ez a segítségnyújtás lényegében az egyes nyomozási cselekmények, illetőleg kényszerintézkedések gyors foganatosításának megkönnyítését, elősegítését jelenti, de magába foglalja a technikai és jogi tanácsadást is. Az egyezmény külön előírja, hogy az államok kötelesek biztosítani a késedelem nélküli kapcsolattartáshoz szükséges eszközöket, valamint a képzett és megfelelően felszerelt személyzetet.

Magyarország az Országos Rendőr-főkapitányságon működő Nemzetközi Bűnügyi Együttműködési Központot jelölte ki kapcsolattartási pontként. A 4/2002. (I. 30.) BM-PM együttes rendelet 7. §-ának *b)* és *d)* pontja alapján a Nemzetközi Bűnügyi Együttműködési Központ feladata a külföldi bűnüldöző szervekkel bűnügyekben folytatott kapcsolattartás, együttműködés és információcsere, valamint az említett szervektől átvett megkeresések továbbítása a hatáskörrel rendelkező hazai bűnüldöző szervekhez.

3.5.3. Megkeresés nélküli tájékoztatás

Az internet országhatárokon átívelő jellegére tekintettel gyakran előfordul, hogy valamely állam az általa folytatott nyomozás során olyan információkhoz jut, amelyek egy másik állam eljárását is nagymértékben segíthetnék. Annak érdekében, hogy az érintett állam minél hamarabb elvégezhesse a szükséges nyomozási cselekményeket, illetve előterjeszthesse a jogsegélykérelmet, az egyezmény 26. cikke intézményesíti a különböző államok büntetőügyben eljáró hatóságai közötti önkéntes információcserét. Az információk átadása előtt az átadó állam kérheti azok titokban tartását, illetve meghatározott feltételekhez kötheti a felhasználásukat. Amennyiben a címzett nem tud eleget tenni ezen kritériumoknak, akkor erről tájékoztatnia kell az átadót, aki ennek ismeretében dönt arról, hogy az információkat mindezek ellenére átadja-e. Ha viszont a címzett elfogadja a feltételeket, úgy ezután csak azokkal összhangban járhat el.

3.5.4. Tárolt számítástechnikai adathoz való hozzáférés határokra tekintet nélkül, hozzájárulás vagy nyilvános elérhetőség esetén

Olyan adatok is előmozdíthatják a büntetőeljárás sikerét, amelyek bárki számára hozzáférhetőek, illetve amelyek átadására a külföldi állam joga feljogosít valamely személyt. Indo-

kolatlan lenne és az eljárást is szükségtelenül lassítaná, ha az eljáró államnak ilyen esetben is a külföldi állam engedélyét kellene kérnie ahhoz, hogy az adatokhoz hozzájuthasson. Éppen ezért az egyezmény 32. cikke rögzíti, hogy az eljáró állam a másik fél engedélye nélkül hozzáférhet a nyilvánosság számára elérhető módon (nyílt forrású) tárolt számítástechnikai adathoz, függetlenül az adat földrajzi elhelyezkedésétől. Arra is lehetősége van, hogy – amennyiben beszerzi az adat számítástechnikai rendszer útján történő átadására jogszabályban feljogosított személy önkéntes és jogszerű hozzájárulását – hozzáférjen a másik fél területén tárolt számítástechnikai adathoz, vagy azokat a területén levő számítástechnikai rendszer útján megszerezze.

4. KRITIKAI ÉSZREVÉTELEK

Láthattuk, hogy a internetszolgáltató közreműködésével történő titkos adatszerzés rendkívül hatékony eszköz a számítástechnikai bűnözés visszaszorítása terén, hiszen a releváns adatok a szolgáltató rendelkezésére állnak, aki gondoskodik azok megőrzéséről és a hatóságok részére való átadásáról. Ezen információk birtokában lényegesen könnyebbé válik az elkövető azonosítása és a bűncselekmény bizonyítása.

Mindez azonban komoly aggályokat is felvet. Ezek egyik legfontosabb oka, hogy a magyar előírások nem mindenben követik az egyezmény cizellált szabályozását. Ahogyan arról szó esett, az egyezmény a tartalomra vonatkozó adatok kifürkészését csak a belső jogban meghatározott súlyos bűncselekmények tekintetében engedi, a Be. viszont – a szabályozás formai sajátosságai mellett – a kellő differenciálás hiányában túl nagy teret biztosít ennek, hiszen egy játékprogramnak egy külföldi szerverről való egyszeri letöltése esetén is lehetővé teszi a titkos adatszerzés elrendelését. Az átültetés során nagyobb figyelmet kellett volna fordítani arra, hogy az egyezmény a szerzői jogokat sértő cselekményeken kívül egyéb, a társadalomra sokkal nagyobb veszélyt jelentő bűncselekményeket is szabályoz (például a gyermekpornográfiával kapcsolatos cselekmények), amelyekre vonatkozóan valóban indokolt lehet a titkos adatszerzés alkalmazási körének kiterjesztése. Garanciális szempontból megnyugtatóbb megoldást jelenthetne, és az egyezmény logikájához is jobban illeszkedne egy taxatív felsorolás beiktatása a Be.-be, amelyben valóban csak a kiemelkedő tárgyi súlyú bűncselekmények szerepelnének (egy készülő emberölés vagy terrorcselekmény megakadályozása céljából a társadalom védelme mindenképpen indokolja a tartalomra vonatkozó adatok kifürkészésének lehetővé tételét).

Az is aggályos, hogy az internetszolgáltatónak – műszaki adottságaiból következően – elvileg módjában áll minden, a hálózatán keresztül továbbított adatot megismerni, és ennek folytán a közlésben részt vevő személyekről jóformán bármit megtudni. Az adatok védelméről gondoskodik ugyan a Be., de csak a nyomozóhatóságra és az ügyészségre rendeli alkalmazni az államtitokról és a szolgálati titokról szóló törvény rendelkezéseit. A 205. § alapján

az engedély kereteinek túllépése esetén a bíróság megszünteti a titkos adatszerzést, ez azonban nem jelent megoldást internetszolgáltató által korábban már megszerzett adatok védelmének problémájára. Az Eht. XVII. fejezete részletes adatkezelési szabályokat tartalmaz, a Btk. 177/A. §-a pedig bünteti a személyes adatokkal való visszaélést, a garanciákat e sorok szerzője mégsem érzi kielégítőnek, különös tekintettel arra, hogy az internetszolgáltató nem az alkotmányos keretek közé szorított állam közhatalmi szerve, hanem egy, az adatokhoz elsőként hozzáférő, nyereségérdekelt gazdasági társaság. Ebből adódóan kétséges az esetleges visszaélések ismertté válása, enélkül pedig a szankciók alkalmazására sem nyílik lehetőség.

A nemzetközi együttműködésre vonatkozó rendelkezéseket sikeresebb törvényalkotási munkának tekinthetjük. Az eljárási jogsegély speciális formáinak beiktatása igazán korszerű szabályozást eredményezett, amely figyelemmel van a számítástechnikai környezetben elkövetett bűncselekmények különös jellegére, emellett pedig megfelelően részletes. A leghasznosabb újítás a 24/7 hálózat kiépítése, hiszen ez nemcsak az egyes nyomozási cselekmények nyújtásában jelent segítséget, hanem nagymértékben előmozdíthatja a hatóságok alkalmazottainak műszaki és jogi felkészülését is. A megkeresés nélküli tájékoztatás intézményesítése gördülékenyebbé teheti az információcserét, ezáltal pedig nőhet a büntetőeljárás sikerének valószínűsége. Problémaként csak az Nbjtv. kissé talán bürokratikus eljárási szabályai említhetők, valamint az, hogy esetleg célszerű lenne az új jogsegélyformákat is beépíteni az eljárási jogsegély esetköreit taglaló példálózó felsorolásba.

A titkos adatszerzés alkalmazásával és a nemzetközi együttműködés nyújtotta lehetőségekkel a hatóságok a korábbinál jóval hatékonyabban tudnak fellépni a szoftverek illegális letöltése, telepítése és használata ellen, annak ellenére, hogy az egyezmény rendelkezéseinek átültetése nem minden tekintetben kifogástalan. Az alkalmazásbeli ellentmondásokat és a jogszabályi hiányosságokat a gyakorlat idővel ezen a téren is fel fogja oldani, illetve át fogja hidalni.