Tószegi Zsuzsanna

A biztonságos internethasználat egyes kérdéseiről

A közpénzekből gazdálkodó könyvtáraknak fokozottan kell ügyelniük a közvagyon részét képező informatikai rendszerek biztonságára. Jó esetben hozzáértő szakemberek alakítják ki az infrastruktúrát és üzemeltetik az eszközöket, de a rendszer logikáját és koherenciáját (összefüggéseit) a könyvtárosoknak is meg kell érteniük, hogy partnerek lehessenek a könyvtári szolgáltatások informatikai hátterét nyújtó rendszer tervezése és működtetése során. Az internetbiztonság számtalan összetevőből álló, rendkívül bonyolult kérdés, amelyet több oldalról is górcső alá lehet venni. Ebben a cikkben az internetbiztonságot főként a könyvtárak szemszögéből vizsgáljuk – kevésbé elvi, mint inkább gyakorlati megközelítésben.

Elsőként a világhálózatot működtető ágensek – eszközök, felhasználók, tartalom – felől közelítsünk a kérdéshez, és tekintsük át a három fő területet: mi az, ami

- az *eszközöket* veszélyezteti,
- a *felhasználókra* nézve jár – főként anyagi – kockázattal,
- az *ártalmas*, illetve *jogellenes tartalmak* miatt morális és/vagy jogi szabályokba ütközik.

Az eszközöket veszélyeztető tényezők közül a leggyakoribb a hardver-, illetve szoftverhiba, az emberi mulasztás, valamint a szándékos károkozás. Ritkán ugyan, de előfordulhatnak elemi csapás okozta károk is.

A felhasználóknak okozott anyagi károkról elég gyakran hallani. Az online csalások – főként a bankszámlák „lecsapolására irányuló kísérletek" – az érdeklődés homlokterében állnak, de a vírustámadások, férgek és egyéb kártevők is kisebb-nagyobb kárt okoznak a támadást elszenvedőknek. A kéretlen küldemények többsége elsősorban nem a felhasználóknak okoz anyagi veszteséget, de a spam-ek elleni védekezés – a mára már elterjedtnek mondható szélessávú hozzáférések miatt – a szolgáltatói oldalon jelentős erőforrásokat köt le. A számítógépes kártevők egy része viszont kéretlen levélben érkezik; kellő óvatosság híján ezek is jelentős károkat okozhatnak a felhasználó gépében és/vagy a helyi hálózatokon.

A káros tartalmak főként a gyermekeket veszélyeztetik. A kiskorúak harmonikus fejlődésének elősegítése törvényi kötelesség, amely fokozottan vonatkozik az iskolai és gyermekkönyvtárakra. Az utóbbi években Magyarországon is nagyobb hangsúlyt kapott az *Európai Unió* által szorgalmazott *Biztonságosabb Internet Program*, amelyről külön fejezetben esik majd szó.

A jogellenes, illetőleg a pedofil tartalom internetes közzététele büntetőjogi kategória. Jogellenesnek minősül a szerzői jogi védelem ellen vétő tartalom mellett az erőszakos tartalom, a személyes adatok jogosulatlan felhasználása, a személyiségi jogsértés és az újabban különösen elharapódzó, képmással való visszaélés.

Egyre erősebb a nyomás a tekintetben, hogy az illegális, jogellenes tartalmaknak ne csak a fel-, de a letöltése is legyen büntethető. Óriási befektetéseket áldoznak annak a technológiának a kidolgozására, amely alkalmas az illegális tartalmak feltöltésének szankcionálására, illetve a letöltések nyomon követésére.

Adatvédelem – adatbiztonság

Ebben a fejezetben az adatvédelem–adatbiztonság szemszögéből nézzük át a jelentős értéket képviselő adatok, információk szempontjából, hogy melyek a biztonságos internethasználatot veszélyeztető tényezők:

- katasztrófahelyzet (elemi károk: tűz, víz, villámcsapás, egyéb vis maior esetek),
- hardverhiba (géphiba, feszültségkimaradás és -ingadozás stb.),
- szoftverhiba (pl. hibás program),

- emberi mulasztás (gondatlanság, tájékozatlanság),
- jogellenes magatartás (főként illegális tartalmak fel- és letöltése),
- szándékos károkozás (vírustámadás, adathalászat, adatlopás stb.).

A hardver- és szoftvereszközök védelme

Az eszközök biztonságos működéséről a lehető legnagyobb odafigyeléssel kell gondoskodni. A teljesség igénye nélkül felsoroljuk az informatikai rendszer fizikai, logikai és adminisztratív védelmét szolgáló, legfontosabb biztonsági intézkedéseket:

- az informatikai rendszer fizikai környezetének és infrastruktúrájának célszerű kialakítása, amelyben fontos szerepet játszik
  - az épület, a helyiségek építészete és épületgépészete,
  - a hálózat fizikai kialakítása,
  - a belépés szabályozása,
  - a környezeti tényezők (hőmérséklet, páratartalom, por) megfelelő szinten tartása;
- vagyonvédelmi rendszabályok kidolgozása és betartása
  - elemi károk, lopás stb. elleni óvintézkedés;
- a hardver- és szoftverhibák elleni védekezés, úgymint
  - a szünetmentes tápegységek használata,
  - az adatok több példányban való tárolása, archiválása (pl. lemeztükrözés, tükörszerver beállítása, cserélhető merevlemezek elkülönített – más helyszínen, pl. páncélszekrényben való – őrzése);
- az emberi mulasztások kivédése
  - a rendszerüzemeltetésben szereplők kötelezettségeinek, jogainak és lehetőségeinek pontos meghatározása,
  - a felhasználók képzése, tájékoztatása,
  - a hozzáférési jogosultságok átgondolt kiosztása,
  - a programok tesztelése, az „éles” és a teszt-adatbázis különválasztása;
- a szándékos károkozás megakadályozása
  - vírusirtó, spamszűrő, adathalászat elleni stb. eszközök telepítésével és állandó frissítésével.

Az informatikai biztonság megfelelő kialakítását – az ISO 27001 információbiztonsági alapszabvány[1] mellett – számos további szabvány szolgálja, amelyek felsorolása a *Magyar Szabványügyi Testület* honlapján található meg.[2]

A fenti kérdésekre vonatkozó előírásokat az intézmények – köztük a könyvtárak – „Informatikai biztonsági szabályzat”-ban rögzítik. Egyes könyvtárak az interneten is közzétették az informatikai biztonsági szabályzatukat; érdemes ezeket alaposan áttanulmányozni.[3]

A felhasználók képzése, tájékoztatása

Az informatikai rendszerek biztonságát leginkább az szolgálja, ha nemcsak az informatikusok képzettek kellőképpen, de a felhasználók is tudatában vannak azoknak a veszélyeknek, amelyeknek vagy az eszközök, vagy ők maguk vannak kitéve, ha nem járnak el kellő gondossággal. A gyorsan fejlődő technológia megköveteli, hogy a szakemberek mellett a felhasználók tudásának folyamatos karbantartásáról is gondoskodjunk. Az alábbiakban dióhéjban felsoroljuk, mi mindent kell a felhasználókkal megismertetnünk az informatikai rendszerek biztonságos működtetése érdekében.

Többszintű védelem

A szabályrendszer és az autentikáció mellett a többszintű védelem elemei a fájl-szintű és a hozzáférési szintű védekezés.

Hozzáférési jogosultságok, autentikáció

Az intézményi szervereken általában sok, különböző funkciójú alkalmazás fut. Képzeljünk el egy közepes méretű könyvtárat, ahol a szerveren az operációs rendszer mellett megtalálható a hálózati szoftver, a könyvtári integrált rendszer adatbáziskezelője és különböző moduljai – köztük az OPAC –, a könyvtár honlapja, a levelezőrendszer, a személyzeti és munkaügyi nyilvántartások, a könyvtár által digitalizált állományok és így tovább.

Az intézményi szerveren tárolt adatok gyakorlatilag pótolhatatlan értéket képviselnek; védelmük érdekében minden lehetséges óvintézkedést meg kell hozni. Az alkalmazások védelme szempontjából rendkívül fontos:

- a hozzáférési jogosultságok megfelelő szabályozása,
- a többszintű védelem kialakítása.

A hozzáférés szabályozása magába foglalja a rendszer egyes elemeihez való hozzáférés szabályainak kidolgozását és rögzítését.

A hozzáférési jogosultságok kiosztása egy nagyobb szervezetben átgondolt tervezést kíván. Az intézmény dolgozói a munkaköri feladataik alapján vannak felruházva bizonyos adatok kezelésére, az egyes adatbázisokhoz való hozzáférésre stb.

A jogosulatlan hozzáférést úgy lehet megakadályozni, hogy az eszközök bekapcsolásakor (a helyi hálózatra való csatlakozáskor) a felhasználónak le kell folytatnia egy autentikációs eljárást, vagyis azonosítania kell magát. Az autentikáció azt jelenti, hogy egy művelet elvégzése előtt megvizsgáljuk a cselekményt megkísérlő személy illetékességét, jogosultságát.

A legelterjedtebb autentikációs módszer a jelszavak használata. A jelszavas bejelentkezés nemcsak azt oldja meg, hogy a hálózatot/számítógépet csak az arra jogosult használhassa, hanem egy esetleges mulasztás/vétség esetén visszakereshetővé teszi: ki és mikor követte el a negatív következményekkel járó hibát.

Érdemes a rendszert úgy beállítani, hogy a felhasználóknak rendszeresen (pl. havonta) változtatniuk kelljen a jelszavukat.

Ha a könyvtár az interneten szabad böngészést enged a használóknak, megfontolandó, hogy engedje-e az anonim módon való hálózati csatlakozást. Az egyéni autentikáció lehetővé teszi, hogy egy esetleges jogsértés következményeit ne a vétlen felhasználóknak kelljen viselniük, hanem megtaláljuk az elkövetőt. Tudván tudva, hogy a könyvtárhasználók adatait csak bizonyos, törvény által előírt keretek között kezelhetjük, illetve, hogy az információkhoz való hozzáférés az alkotmányos alapjogokból levezethető, hogyan járhatunk el jogszerűen ebben a kényes esetben?

A fennálló jogrenddel összhangban lévő szabályzatok kidolgozásával és ezeknek a könyvtárhasználókkal való megismertetésével minimálisra lehet csökkenteni a kockázatot. Ha felhívjuk a könyvtárhasználók figyelmét arra, hogy az informatikai rendszer az internetes böngészés során keletkező információkat – a törvény által engedélyezett ideig és célhoz kötötten – tárolja, és jogellenes magatartás, de főként bűncselekmény gyanúja esetén a bűnüldöző szervek visszakereshetik a könyvtárhasználók adatait, bízvást számíthatunk arra, hogy egy jól kidolgozott intézményi „policy” önszabályozó rendszerként fog működni.[4]

Hasonló a helyzet a könyvtár munkavállalóinak esetében is: pontos, részletes előírások kidolgozásával, illetve azok elfogadtatásával, valamint a dolgozók megfelelő képzésével és tájékoztatásával lehet szabályozni a munkahelyi eszközök használatát, egyúttal a minimálisra csökkenteni az esetlegesen elkövetett hibák negatív következményeit.

Van még egy érdekes kérdés: hogyan lehet ellenőrizni (netán szabályozni?), mit keres(het) a könyvtárhasználó az interneten, amikor tudjuk, hogy a szellemi/gondolati szabadság korlátozása tilos – legalábbis addig, amíg a véleménynyilvánításra és a szólásszabadságra vonatkozó törvénybe nem ütközik? Erre e kérdésre a későbbiekben még visszatérünk.

Fájlszintű védelem

A fájlszintű védelem az egyes állományokra vonatkozik. A fájlok védelmének célja az állományok véletlen módosításának, törlésének kiküszöbölése. Például egy írásvédett (Read Only) attribútummal ellátott fájl nem törölhető. A Digital Right Management (DRM) körébe tartozó megoldás a fájlok másolás elleni védelme.

Hozzáférési szintű védelem

További fontos intézkedés a hozzáférési szintű védelem, amely azt jelenti, hogy a felhasználó csakis a számára engedélyezett szerverterületen dolgozhat. Az előző felsorolásból példaként felhozhatjuk az olvasószolgálatos könyvtárost, aki csak a kölcsönzési modulhoz kap jogosultságot, így ő láthatja a beiratkozott olvasók adatait, de a könyvtárosokról készült nyilvántartást nem – és fordítva: a humánpolitikai munkatárs a könyvtárosok munkavállalói adatait kezeli, de az olvasókét nem.

És ha már az olvasók, illetve a könyvtárosok személyes adatainál tartunk, tekintsük át, mely jogok tartoznak a személyiségi jogok körébe, és hogyan védi ezen jogokat a magyar jogrend.

Személyiségi jogok

A magyar jogrendszer a személyiségi jogot az emberi méltósághoz való jogként fogalmazza meg. Az Alkotmányból levezetett jog tartalma:

- a személyiség szabad kibontakoztatásához való jog,
- az általános cselekvési szabadság,
- a magánszférához való jog,
- az önrendelkezés szabadsága.

A Polgári Törvénykönyv (Ptk.) konkrétan nevesíti a név, a jó hírnév, a képmás és hangfelvétel védelmét, a titokjogot, valamint az információs önrendelkezés jogát.[5] A könyvtári gyakorlatban főleg ezeknek a jogoknak az alkalmazásával kell tisztában lennünk, ugyanis a Ptk. 75. § értelmében a személyhez fűződő jogokat mindenki köteles tiszteletben tartani, e jogok a törvény védelme alatt állnak.

A névhasználat joga a saját név használatának jogára, a névbeli egyezésekből adódó félreértések kiküszöbölésére, illetve a visszaélések elkerülésére vonatkozik. A más nevével – és nem csak természetes személyek nevével – való visszaélést a törvény tiltja. Ha tudományos, művészeti vagy irodalmi tevékenységet folytató személynek azonos, vagy összetéveszthető neve van egy, a területen már korábban tevékenykedő személlyel, az időben később pályára lépő szereplő – az érintett kérésére – a tevékenysége során csakis megkülönböztető toldással (elhagyással) használhatja saját nevét. (A könyvtárosok számára jól ismert jelenség a névazonosság, amelynek kezelésére számos megoldást dolgoztak ki.)

A névhasználat bizonyos előjogokat is nyújt a doménnév bejegyzése során. Egy hivatalos név viselője, egy védjegy jogosultja stb. a *prioritási szabály* alapján megvétózhatja azt a doménnévigénylést, amely az övével azonos vagy összetéveszthető nevet kíván bejegyeztetni. Az elsőbbség az intézményeknek nemcsak a teljes, hanem a hivatalosan nyilvántartott rövid nevére is érvényes. Az *Internet Szolgáltatók Tanácsa* honlapján olvasható szabályzat részletesen ismerteti, vita esetén milyen okiratokkal kell alátámasztani a prioritási igényt.[6]

A közszereplők, alkotók felvett neve (művészneve) haláluk után sem bitorolható – bár ez az eset már nem a személyiségi, hanem a szerzői jog hatálya alá tartozik (Szjt. 12. §). A szerzői álnevek önkéntes, közhitelű nyilvántartását az ARTISJUS vezeti.[7]

A jó hírnévhez való jog gyakorlása, illetve esetleges megsértése látszólag távol áll a könyvtári világtól – egészen addig, amíg nem kerülünk olyan helyzetbe, amikor az intézmény jó hírnevét sérti meg valaki, vagy netán a késedelembe eső könyvtárhasználók nevét akarnánk közzétenni – ez utóbbi egyértelműen törvénybe ütköző.
Sokkal gyakoribb eset, hogy a könyvtárak képmásokat, hangfelvételeket kívánnak az interneten közzétenni – például a könyvtári események dokumentálása vagy a helytörténeti gyűjtemény digitalizálása kapcsán. Az emberek külső megjelenését reprezentáló, a személyiség külvilág felé való megnyilvánulását jelentő képmás és hangfelvétel akkor *készül* jogszerűen, ha az érintett – akár csak hallgatólagosan – azt tudomásul vette. A *nyilvánosságra hozatalhoz* (esetünkben az internetes közzétételhez) azonban az érintett *kifejezett hozzájárulása* szükséges; az alól a szabály alól csak a nyilvános közszereplés jelent kivételt.

Ki minősül közszereplőnek? „… *az a személy, aki közhatalmat gyakorol, gyakorolt vagy közhatalom gyakorlásával járó tisztségre jelölték, illetve aki a politikai közvéleményt feladatszerűen alakítja vagy alakította*.” A fogalmat a 2003. évi III. tv. (az ún. ügynöktörvény) 1.§ (1) bekezdés 13. pontja vezette be a magyar jogba.[8] Ennek értelmében tehát azt a fotót, amely a polgármesterről egy hivatalos eseményen készült, közzé lehet tenni az interneten, de az író-olvasó találkozó résztvevőiről csak akkor, ha a képen látható személyek hozzájárultak a közzétételhez.

A lelkiismeret szabadsága

A személyiség kibontakozásának, önmegvalósításának fontos eleme a lelkiismeret szabadsága, ezért többnyire tilos bármiféle kényszerítés vagy tiltás a vallásosság/ateizmus, a párttagság/pártonkívüliség, az életmód/életvitel és más hasonló lelkiismereti kérdésekben. A lelkiismeret szabadsága magában foglalja a tudat szabadságát, amelynek szerves része a szabad gondolkodás és véleménynyilvánítás, a korlátozásmentes tudományos és művészeti meggyőződés, a sajtószabadság, a tájékoztatáshoz, illetve a bírálathoz való jog.

A személyazonosító adatok kezelése

Az Alkotmány 59. § (1) bekezdése szerint „a Magyar Köztársaságban mindenkit megillet a jóhírnévhez, a magánlakás sérthetetlenségéhez valamint a magántitok és a személyes adatok védelméhez való jog”.

A természetes személyek azonosítására szolgáló adatok két nagy csoportba oszthatók: a személy-

azonosító adatok mellett a törvény ún. különleges adatokat is megnevez. Az adatvédelmi törvény nem sorolja föl a természetes személy azonosítására szolgáló konkrét adatokat. A „természetes személyazonosító adat" a közigazgatásban használatos jogi fogalom, amelynek körébe a következők tartoznak:

- családi és utónév,
- születési családi és utónév,
- nem,
- születési hely és idő,
- anyja születési családi és utóneve,
- állampolgárság,
- lakó- és tartózkodási hely.

A személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény 4. §-a szerint: „Természetes személyazonosító adat a polgár

a) családi és utóneve, születési családi és utóneve,
b) születési helye,
c) születési ideje és
d) anyja születési családi és utóneve."

A törvény a személyes adatok körén belül megkülönbözteti az ún. *különleges adatokat*, úm. a faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más meggyőződésre, az egészségi állapotra, a kóros szenvedélyre, a szexuális életre, valamint a büntetett előéletre vonatkozó adatokat. A különleges adatok kezelése során a törvény szigorúbb követelményeket támaszt.

Az adatvédelmi törvény szerint személyes adatot jogszerűen csak az érintett hozzájárulásával vagy törvényi előírásra[9], különleges adatokat viszont csakis az érintett *írásos hozzájárulása* esetén lehet kezelni. Az érintett írásbeli hozzájárulásától csak nemzetközi egyezmény alapján, az Alkotmányban biztosított alapvető jogok érvényesítése érdekében, továbbá a nemzetbiztonság, a bűnmegelőzés vagy a bűnüldözés érdekeit szolgáló törvényi felhatalmazás esetén lehet eltekinteni.

Miért is fontos mindezt tudnunk?

A beiratkozáskor elkérjük az olvasók személyazonosító adatait, amelyeket – célhoz kötötten, és a cél által meghatározott ideig – kezelünk. Ugyanezen olvasóknak lehetővé teszünk internet-hozzáférést a könyvtári hálózatba kapcsolt gépeken – ez ma már általános könyvtári szolgáltatás. Az internetet működtető eszközök alkalmasak arra – és ezt meg is teszik –, hogy valamennyi egérkattintást rögzítsék és tárolják. A „clickstream" adatok rögzítik a felhasználó gépének IP címét, az általa meglátogatott oldalakat, az oldalon belül megtekintett elemeket, az ott töltött időt, a további navigálás adatait – vagyis tulajdonképpen minden olyan adatot, amelyet a törvény „különleges" adatként nevez meg. Az internetelérést nyújtó szervereken ezek az adatok az ún. logfájlokból visszakereshetők.

Az adatvédelmi biztos, *Jóri András* a következőkre mutat rá: „… a magyar törvény szerint nem lényeges, hogy az adatalany és az adat helyreállítását az adatkezelő vagy más személy képes elvégezni: ha a kapcsolat helyreállítható, az adat személyes adatnak minősül. A valamely szolgáltatást nyújtó szerveren naplófájlban rögzített, a szolgáltatást igénybe vevő felhasználó számára a szolgáltatója által dinamikusan kiosztott IP-cím pl. akkor is személyes adat, ha kizárólag a felhasználó Internet-szolgáltatója képes a személy és az adott időpontban használt IP-cím között kapcsolatot teremteni, a szerver üzemeltetője nem. Az adat mindaddig megőrzi személyes adat jellegét, ameddig az Internet-szolgáltató képes az adott felhasználó által adott időpontban használt IP-cím meghatározására; az ezt lehetővé tévő naplófájl törlése után az adat nem személyes adat többé."[10]

A rendőrségről szóló törvénybe[11] nemrég bekerült az a rendelkezés, amely lehetővé teszi, hogy a rendőrség egyes esetekben, ha súlyos (például gyermekkorú ellen irányuló, kábítószerrel kapcsolatos, fegyveres elkövetéssel megvalósuló stb.) bűncselekményről van szó, és erre bírói engedélye van, hozzájuthasson az elektronikus levelek tartalmához. Súlyos bűncselekmény gyanúja esetén a rendőrség titkos információgyűjtést is folytathat.[12]

Ha tehát a könyvtár szabad internet-hozzáférést enged az olvasóinak, akkor ezt a helyzetet is kezelnie kell.

Szándékos károkozás

Az internethasználatot tekintve talán erről a kérdéskörről hallunk a legtöbbet: nincs nap, amely vírustámadásról, adatlopásról, kémprogramokról és más hasonlókról szóló, a felhasználók számára

gyakran kevéssé érthető, ám a veszélyérzetet növelő hírek nélkül telne el. Bár sokan túlzónak ítélik e cselekmények médiavisszhangját, és fölmerül az a gyanú is, hogy a kárelhárító szoftverek gyártói a saját üzleti hasznuk növelése érdekében manipulálják a médiát, azért nem szabad a szándékos károkozásból adódó veszélyeket lebecsülni, sőt: kötelező ezek ellen védekezni.

A vírus

A vírus egy végrehajtható programban foglalt utasítás-sorozat, amely képes arra, hogy manipulálja a számítógép operációs rendszerének funkcióit, célja a számítógép erőforrásainak felhasználása vagy megrongálása. A felhasználóknak annyit mindenképpen érdemes a vírusokról tudniuk, hogy formázatlan szöveges üzenetben, nem futtatható programokban nem kaphatunk vírust – kivéve, ha az adott fájl VisualBasic kódot vagy egyéb makrókat tartalmaz, ezeket ugyanis az alkalmazás (például a Word vagy az Excel) automatikusan lefuttatja. Az automatikus futtatás ellen a legegyszerűbb megoldás a makrók letiltása.

A vírusok ellen meglehetős hatékonysággal lehet védekezni – például azzal, hogy ahányszor csatlakozunk az internethez, automatikusan lefuttatjuk a vírusirtó program legújabb változatát. Mivel a legtöbb vírus e-mailek csatolmányában terjed, az e-mailben küldött mellékletek megnyitása előtt vírusirtóval meg kell vizsgáltatni az adott fájlt. Érdemes a legelterjedtebb levelezőrendszereket használni, amelyek folyamatosan figyelik és szűrik a levelezőszerveren keresztülmenő forgalmat, és csak akkor engedik egy levél mellékletét megnyitni, ha a vírusirtó program nem jelzett abban hibát.

A kéretlen elektronikus küldemények (spam-ek)

A spam fogalma nincs pontosan definiálva, de abban egyetértés van, hogy olyan, általában valamilyen reklámot tartalmazó elektronikus küldeményről van szó, amelyet a felhasználó nem kért[13]. A spam feladói tömegesen bocsátják útjára a kéretlen leveleket, ezzel jelentős sávszélességet, tárkapacitást kötnek le, és az ellenük való védekezés szintén jelentős erőforrásokat igényel.

Az elmúlt években Magyarország a „spam-ranglista” élére került – e negatív rekord egészen elképesztő számaránynak köszönhető: 2010 májusában az összes elektronikus levél 95,4%-a kéretlen küldemény volt. Az ismert internetbiztonsággal foglalkozó cég, a Symantec által közzétett adatok alapján 2010 júniusában ez az arány kicsit javult: 94,8% volt Magyarországon.[14]

A kéretlen küldemények ellen *spamszűrő programokkal* lehet hatékonyan védekezni. A spamszűrőt az intézmények levelezését bonyolító szerverekre szokták telepíteni. A legnépszerűbb, ingyenes levelezőrendszerek is eredményes védekezést folytatnak a kéretlen küldemények ellen. Általános megoldás, hogy a beállítások alapján a program által spam-nek minősített küldemény egy „karanténba” kerül, ahonnan a címzett átirányíthatja azokat a leveleket, amelyeket valóban meg akar tekinteni.

Adatlopás

A szándékos károkozás jelentős hányada irányul a bankszámlák fölötti rendelkezési jog megszerzésére. A sok negatív hír dacára az online bankolás gyorsan terjed, így potenciálisan egyre többen vannak kitéve annak, hogy illetéktelenek megszerzik az adataikat, amelyek birtokában hozzáférhetnek a bankszámlához. Az adatlopás elleni védekezés azokban a könyvtárakban fontos feladat, ahol az olvasók szabadon használhatják az internetet. Ha valaki egy könyvtári számítógépen intézi a banki ügyeit, és a gyorsítótárból (cache-ből) nem törli az adatait, más személy ezzel visszaélhet. Föl kell hívni erre az olvasók figyelmét, de még jobb, ha gondoskodunk arról, hogy minden használat után törlődjön a cache.

Illegális és káros tartalom

Az internetes tartalomra vonatkoztatva a címben szereplő szókapcsolat az utóbbi évtizedekben jelent meg, elsőként az Európai Bizottság 1996. évi közleményének címében: *Illegális és káros tartalom az interneten*[15]. Amíg az „illegális tartalom” alatt közmegegyezés alapján a jog által tiltott tartalmat értjük, addig a „káros tartalom” fogalma máig sem pontosan tisztázott.[16]

A kiskorúak védelméről és az emberi méltóságról szóló „Zöld Könyv” szerint az illegális tartalom mindenki számára tilos, a káros tartalom viszont a kiskorúak fizikai és mentális fejlődésére lehet veszélyes.[17] Az *Európai Parlament* médiabizottságának jelentése szerint „… *alapvető különbséget kell tenni a jogellenes tartalom között, amely a jog területére tartozik, és a káros tartalom között, amely kiskorúakat érint és elsősorban az erkölcs területére tartozik.*”[18] Ebből kiindulva eljutunk a szabályozási kérdésekig: a jogellenes tartalom szabályozá-

sa elsősorban az *állam* feladata; a káros tartalom esetében részben az *önszabályozás*, részben központi szabályozás hozhat megoldást – a médiában kötelezően bevezetett korhatár-jelölőkhöz, vagy a reklámtörvény bizonyos előírásaihoz hasonlóan.

A káros tartalom esetén az Európai Unió ösztönzi a gazdasági és a civil szféra, valamint a felhasználók együttműködésével megvalósuló önszabályozás előtérbe kerülését, illetve a hatékony szűrőrendszerek elterjesztését.[19] A szűrők – sokak által kötelezően javasolt – alkalmazása azonban már jogi aggályokat is fölvet: a véleménynyilvánítási szabadság elvéből fakadóan kötelező jelleggel csak jogszabály alapján vagy bírói ítélettel lehet korlátozni a közléseket.

A szolgáltatók felelőssége

Az illegális tartalmak esetében az első kérdés: kié a felelősség? Hosszú évekbe telt, amíg az új médium szereplőinek felelőssége tisztázódott, és végül a tartalomszolgáltatók elfogadták, hogy az általuk közölt tartalomért felelősséggel tartoznak. A web 2.0 viharos gyorsaságú terjedése azonban új kérdéseket vet föl, hiszen a fórumokon, blogokban, társalgókban egyre több jogellenes és/vagy sértő tartalom tűnik fel. Ha az internetszolgáltatók moderálják az itt közzétett tartalmat, azzal átlépik a számukra előírt szerepkört. A szolgáltatók – különösen a tárhelyszolgáltatók – bizonyos felelősséggel azért tartoznak az általuk működtetett szerveren elhelyezett tartalmakért.

Önszabályozás vagy öncenzúra?

Bayer Judit véleménye szerint az önszabályozás pozitív formája, ha a szolgáltatók az állami beavatkozás helyett önként tagadják meg a közreműködést az illegális vagy a gyűlöletkeltő tartalom nyilvánosságra hozatalában, de vannak, akik ezt káros öncenzúrának tartják.

Az ártalmas, illetve jogellenes tartalmak elleni küzdelem

Az interneten legálisan, illetve a jogtulajdonosok engedélye nélkül közzétett szerzői művek aránya nehezen volna felmérhető, de az illegális források letöltésére vonatkozóan vannak becslések: szakértők szerint a világ internetes forgalmának 50-75 százalékát az illegális letöltések teszik ki.[20] Az internetbiztonságról szóló cikkben e kérdés taglalásának is helye volna, de terjedelmi okokból most éppen csak megemlítjük; a TMT az elmúlt években több olyan cikket is közölt, amelyek a szerzői jogi kérdéseket járták körül.

Az internet – éppen rendkívüli összetettségének, tartalmi gazdagságának köszönhetően – nem csak hasznosat, szépet és jót kínál a felhasználóknak. Számos veszély fenyegeti főleg a gyermekeket, de a kezdő, tapasztalatlan felhasználókat is, akiket kötelességünk minden legális eszközzel megóvni a testi és lelki egészségükre káros hatásoktól.

Az Európai Unió Biztonságosabb Internet Programja

Az Európai Bizottság 1999-ben indította útjára a *Biztonságosabb Internet Programot* (*Safer Internet Program = SIP*), melynek célja az internet és más új online technológiák – különösen a gyermekek és kiskorúak általi – használatának biztonságosabbá tétele, valamint a jogellenes tartalom, illetve a felhasználók által nem kért küldemények (spam) elleni hatékony küzdelem.[21]

A 2009–2013 közötti új programperiódus célkitűzései változatlanok maradtak, de a program kidolgozói erőteljesebben koncentrálnak a web 2.0 terjedésével jelentkező újabb veszélyhelyzetekre.

A közösségi oldalak – vitathatatlan előnyeik mellett – számtalan veszélyt rejtenek a gyermekek és a fiatalok számára. Mind gyakrabban fordul elő, hogy a felnőttek ártó szándékkal közelednek a gyermekekhez (ez a jelenség *grouming* néven vált ismertté). Mindezek elkerülése érdekében a SIP az alábbi főbb tevékenységeket támogatja:

- a megelőzés technológiai feltételeinek kialakítása – beleértve a szolgáltatók ösztönzését és segítését a címkézés kidolgozásában;
- a nemzetközi szintű együttműködés, a legjobb gyakorlatok széles körű terjesztése;
- tudatosságnövelés a szülők, illetve a gyermekekkel hivatásszerűen foglalkozók számára a jogellenes tartalom és a káros online magatartás elleni küzdelemben;
- az érdekeltek ösztönzése, hogy megfelelő önszabályozó rendszereket alakítsanak ki és valósítsanak meg;
- az online gyermekbántalmazás tanulmányozásának előmozdítása;

- a gyermekek által használt jelenlegi és jövőbeni technológiák hatásáról szerzett ismeretek gyarapítása.

Az Európai Unió 2008-ban határozatot fogadott el az internetet és egyéb kommunikációs technológiákat használó gyermekek védelméről.[22]

Természetszerűleg Magyarország is csatlakozott az EU programjához. A *Biztonságos Böngészés Program* az Európai Unió programjával összhangban, annak szelleme szerint jött létre, céljait a rendőrség is támogatja. A portál címe: *http://www.biztonsagosbongeszes.hu/hu/*

Erről az oldalról ingyenesen le lehet tölteni egy magyar fejlesztésű szűrőprogramot, amely a folyamatos bővítésnek köszönhetően képes arra, hogy kiszűrje a gyermekek számára káros szövegeket, képeket: *http://www.biztonsagosbongeszes.hu/hu/letoltes_iskolaknak.php*

Az ugyancsak ingyenes családi változatot fölkészítették arra is, hogy a szülő kapjon értesítést, ha a gyermeke a neten keresztül találkozót beszél meg valakivel.

A *Puskás Tivadar Közalapítvány* és a *CERT-Hungary Központ* által létrehozott *biztonságos internet* portál feladata a magyar internetezők biztonsági tudatosságának növelése és az internet biztonságos használatának elősegítése. A közérthetően megfogalmazott tudnivalókat közel húsz almenübe rendezték: itt a böngészőktől a játékokon át az online vásárlásig és bankolásig az összes népszerű szolgáltatás helyes használatáról tájékoztatják az internetezőket. A portál címe: *http://www.biztonsagosinternet.hu*

Tartalomszűrés

Az internet egyik legkényesebb és legtöbbet vitatott kérdésköre a tartalomszűrés. Ha valaki szóba hozza ezt a témát, sokan már a nélkül is cenzornak kiáltják ki, hogy az illetőnek módjában állna kifejtenie: milyen tartalomra, illetve milyen célközönségre gondol. Szögezzük le gyorsan: nem a gondolat- és véleményszabadság és nem az információhoz jutás szabadságának korlátozását jelenti, ha az adófizetők pénzén fenntartott közösségi helyeken csak a törvény általi korlátozás alá nem eső tartalomhoz engedünk hozzáférést, illetve mindent megteszünk annak érdekében, hogy a könyvtári informatikai rendszeren keresztül ne lehessen feltölteni a világhálóra a morális és jogi értelemben kifogásolható tartalmakat.

Az internetes tartalomszűrésre különböző szinteken kerülhet sor: nemzeti szintű korlátozást rendelhet el egy állam, a dolgozók internet-hozzáférését korlátozhatja egy munkáltató, a tanulókét egy iskola, az olvasókét egy könyvtár, de leggyakrabban a szülők élnek a gyermekeik által hozzáférhető tartalomra vonatkozó korlátozásokkal.

A tartalomszűrésre számtalan szoftveres megoldást fejlesztettek ki. Vannak olyan internet-szolgáltatók, amelyek a szervereikre telepítik a szűrőprogramokat, és ismeretesek lokális gépekre installálható szoftverek. Ez utóbbiak egyre népszerűbbek például az Egyesült Államokban: a kliensoldali alkalmazásokat a családok mellett a könyvtárak is előszeretettel telepítik a számítógépeikre. A legnagyobb keresőszolgáltatók – köztük a Google – lehetővé teszik a tartalomszűrő aktiválását, a Yahoo, a Lycos és más keresőmotorok gyermekbarát változatokat kínálnak az ügyfeleiknek.

A szűrőprogramok mellett és ellen rengeteg érvet lehet felhozni. A legtöbb panasz a túl erősre beállított szűrés miatt érkezik; nemcsak az egészségügyi tájékoztató, felvilágosító programok akadhatnak fenn a szűrőn, de egész angliai grófságok (Essex, Sussex) egyetemi, intézményi honlapjaihoz is lehetetlenné válhat a hozzáférés, ha a tartomány neve az URL-ben szerepel.

A magyar könyvtárak gyakorlata

Az *Információs Társadalom- és Trendkutatásért Alapítvány* kérdőíves felmérést végzett a magyar könyvtárak körében az információs társadalom erősítésében játszott szerepükről. A 2006-ban, majd 2009-ben végzett kutatás rendkívül tanulságos, de itt a megállapítások közül csak a témánkhoz szorosan kapcsolódó megállapítást idézzük: „Az internet-szolgáltatónak, vagyis a könyvtárnak joga és lehetősége van arra is, hogy korlátozza, megszűrje a megnézhető oldalakat is. Ez sokszor morális és pedagógiai kötelessége is egyben. Ezzel a lehetőségével csak a könyvtárak fele (51 százalék) él, másik fele egyáltalán nem korlátozza, mely oldalakat lehet megnézni."[23]

A kérdőíves felmérés a tartalomszűrésre is kitért. A válaszokból kiderül, hogy a magyar könyvtárak 37%-a él ezzel a lehetőséggel, kétharmaduknál nincs ilyen gyakorlat.

Jegyzetek és irodalom

[1] MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények [2010. szeptember 4.]

[2] Az információbiztonság magyar nemzeti szabványai és előszabványai. *http://www.mszt.hu/dokumentumok/kozinfbiztonsag.pdf* [2010. szeptember 4.]

[3] Fővárosi Szabó Ervin Könyvtár ideiglenes informatikai biztonsági szabályzata. 2005. július. *http://www.fszek.hu/?tPath=/view/&documentview_type=save&documentview_site=1&documentview_id=6470* [2010. szeptember 11.]
Kisfaludy Károly Megyei Könyvtár Informatikai Biztonsági Szabályzata *http://www.kkmk.hu/kozerdeku/II_6.pdf* [2010. szeptember 11.]

[4] Az internet-önszabályozás más téren – például a tartalomszűrésben – is jelen van.

[5] GYENGE Zsolt: Személyiségi jog. Kommunikációtudományi Nyitott Enciklopédia. *http://ktnye.akti.hu/index.php/Szem%C3%A9lyis%C3%A9gi_jog* [2010. augusztus 28.]

[6] Domainregisztrációs szabályzat. *http://www.domain.hu/domain/szabalyzat/szabalyzat.html* [2010. szeptember 4.]

[7] A Tanácsadó Testület 1/2003. (IV. 22.) Elvi Állásfoglalása *„A közszereplő (előadóművész) művésznevével egyező névválasztások jogszerűsége”* tárgyában. Internet Szolgáltatók Tanácsa. *http://www.domain.hu/domain/tt/elvi_allasfoglalasok/elvi_allasfoglalasok_1_2003.html* [2010. augusztus 28.]

[8] SARKADY Ildikó: A közszereplők személyiségvédelme a bírói gyakorlatban. Médiakutató. 2006 ősz. *http://www.mediakutato.hu/cikk/2006_03_osz/06_kozszereplok_szemelyisegvedelme* [2010. augusztus 28.]

[9] továbbá törvény felhatalmazása alapján, meghatározott körben, helyi önkormányzat rendelete alapján

[10] JÓRI András: Az adatvédelemről rendszergazdáknak. *http://www.jogiforum.hu/publikaciok/15#axzz10jmDIrzh* [2010. augusztus 28.]

[11] 1994. évi XXXIV. törvény a Rendőrségről. *http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99400034.TV* [2010. augusztus 28.]

[12] JÓRI i.m.

[13] FARKAS György: Kéretlen reklámüzenetek fogalma, jellemzői és az általa hordozott veszélyek. *http://www.hm.gov.hu/hirek/kiadvanyok/kutatas/doktorandusz/farkas_gyorgy* [2010. szeptember 4.]

[14] Magyarország a spammel leginkább fertőzött: Harmadszorra is Magyarország került a spamranglista élére. *http://terminal.hu/Hirek/Bejegyzes/62389/Magyarorszag-a-spammel-leginkabb-fertozott* [2010. augusztus 28.]

[15] Illegal and Harmful Content on the Internet: Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. COM(96) 487, 1996. – Idézi Bayer

[16] BAYER Judit: A háló szabadsága – Az internet tartalmának szabályozási problémái a véleménynyilvánítás szabadsága tükrében. Doktori értekezés. Budapest, ELTE, 2004. *http://mek.oszk.hu/03800/03845/03845.htm* [2010. szeptember 10.]

[17] Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services COM(96)483 – Idézi Bayer

[18] BAYER i.m.

[19] BAYER i.m.

[20] Sikeres hadjárat a kalózok ellen! - Sok svédet elrettentett az illegális letöltéstől a kalózkodás elleni törvény. *http://www.jogiforum.hu/hirek/21402#ixzz10kpKY9VE* [2010. szeptember 4.]

[21] A Biztonságosabb Internet program angol nyelvű összefoglalója. *http://ec.europa.eu/information_society/doc/factsheets/018-safer-internet.pdf*

[22] Az Európai Parlament és a Tanács határozata az internetet és egyéb kommunikációs technológiákat használó gyermekek védelmére irányuló többéves közösségi program létrehozásáról 2008/0047 (COD). *http://biztonsagosbongeszes.hu/hu/pdf/LexUriServ.pdf* [2010. szeptember 11.]

[23] A könyvtárak szerepe az információs társadalomban. Információs Társadalom- és Trendkutatásért Alapítvány. Budapest, 2009. 36. p. *http://www.ittkalapitvany.hu/menet_docs/konyvtarak_szerepe.pdf* [2010. szeptember 11.]

Beérkezett: 2010. X. 14-én.

Tószegi Zsuzsanna
a Kaposvári Egyetem docense,
a Magyar Szabadalmi Hivatal
szakmai főtanácsadója.
E-mail: zsuzsanna.toszegi@hpo.hu