PARTI KATALIN

Harc az online illegális tartalom ellen

Az internet és az új médiák proliferációja számos technikai kérdést vet fel. Ám ezzel együtt olyan nem technikai kérdések is megjelennek, mint az állam felelőssége állampolgárai megóvásában az illegális tartalmaktól, a tartalomblokkolás alapvető emberi jogi kérdései, valamint a magánszférába való beavatkozás miként je és terjedelme. Jelen tanulmány számot vet az internet ellenőrzésében szerephez jutó fórumok és szervek, úgymint az állam és az internetszolgáltatók jogosultságaival és felelősségi kérdéseivel az internet ellenőrzésében, valamint jogellenes tartalmaktól való megtisztításában. A német és a magyar joggyakorlatra koncentrálva arra a konklúzióra jut, hogy az illegális tartalmak értesítési-levételi eljárásban való kezelése nemcsak technikailag járhatóbb út az internet központi szabályozásával összehasonlítva, de jobban respektálja a magánélet tiszteletben tartásához fűződő, valamint más demokratikus jogokat is.

Módszerek az illegális tartalmak távoltartására. Az internetblokkolás[1]

Az illegális tartalom kiszűrésére mind az önszabályozás, mind pedig a koreguláció kínál lehetőségeket.[2] Az önszabályozás körébe tartozik a felhasználói, *elsődleges szintű* védekezés tűzfallal, szűrőszoftverekkel. Inkább közösségi szinten óvja a felhasználókat az intézményi védekezés, amikor például egy iskola, könyvtár vagy munkahely szűri a tartalmat látogatói köre (tanulók, könyvtárlátogatók, munkavállalók) érdekében.

[1] Az internetblokkolás a felhasználók illegális online tartalmaktól való megóvásának eszköze. Ez magában foglalja a felhasználók korlátozását bizonyos tartalmak elérésében, illegális tartalmat közvetítő IP-címek, doménnév-kiterjesztések hozzáférhetetlenné tételét, illegális weboldalak eltávolíttatását a *host provider*rel, vagy szűrőszoftverek alkalmazását annak érdekében, hogy a gépünk ne engedjen át nem kívánt kulcsszavakat tartalmazó weboldalakat.

[2] Az Európai Parlament, a tanács és a bizottság 2003 decemberében kötött megállapodása (Interinstitutional Agreement on Better Lawmaking Official Journal C321 of 31. 12. 2003) célul tűzi ki a kevesebb, de jobb minőségű uniós szintű jogalkotást és ezzel párhuzamosan a tagállamokban az önszabályozás és a koreguláció támogatását. A koreguláció a kormányok által bizonyos privát vagy civilszervezetekre ruházott hatalom, amelynek segítségével a civilszervezetek jobban együttműködhetnek a kormánnyal, ám végső soron, a szabályozás szintjében és irányában a kormány döntései érvényesülnek (top-down szabályozás). Az önszabályozás ezzel szemben a saját szabályok összességét takarja, amelyek a civilszervezetek, illetve a nem kormányzati szervek egységes belső magatartási szabályai: nincs kötőerejük, de egységesítik a résztvevő felek magatartását (bottom-up szabályozás).

A *második szint*, amikor az internetszolgáltató telepít a rendszerébe olyan szűrőprogramot, amely nem engedi át a felhasználókhoz a kéretlen reklámot, levélszemetet. Ugyancsak szolgáltatói szinten érvényesül a több szolgáltató által kibocsátott és közös működési elvek *(code of conduct)* alapján alkalmazott közös szűrőrendszer bevezetése. Az ilyen szűrők minőségbiztosításként is működnek, egyfelől a szolgáltatás minőségét, másfelől azt hivatottak garantálni, hogy a felhasználó azonosan magas színvonalú szolgáltatást kapjon – kéretlen levelek és reklámok nélkül.

A *harmadik szint* az illegális tartalmak – vagy azok egy meghatározott csoportjának – állami szinten előírt blokkolása. Ennek során az állam súlyos bűncselekményt megvalósító tartalmak kiszűrésére kötelezi az internetszolgáltatókat, központi intézkedésként.

Míg az első két módszer az önszabályozás, addig a harmadik szint a koreguláció körébe tartozik. Mindkettőnek megvannak az előnyei és a hátrányai. Az önszabályozás nem egységes, mivel nem lehetünk biztosak abban, hogy minden közintézmény telepített szűrőszoftvert, vagy egyes módszerek nem alkalmasak az illegális tartalmak teljes körű kiszűrésére.

Tipikusan ilyen a felhasználók által alkalmazott kulcsszavas szűrés, amelynél fennáll a veszély a túl-, illetve az alulszűrésre, valamint sokszor az egyéni felhasználói tájékozottság és képességek szabják meg a kereteit.[3]

Ezzel szemben a koreguláció keretében bevezetett centrális szűrési megoldások hatástalansága vetekszik a felhasználói szintű szűrésével, és még az állampolgári alapjogokat is sérthetik.

A szűrési szintekkel kapcsolatos aggályok kiindulópontja, hogy kinek a kezében legyen a döntés arról, mi a helyes és mi a helytelen – azaz milyen tartalmakat tekinthet meg a felhasználó. A felhasználó, aki a saját számítógépét védi, maga állítja be a szűrési feltételeket, tehát ő maga dönti el, milyen tartalmakkal nem szeretne szembesülni. Az intézményi szűrésnél azonban a munkáltató, a klub, az iskola, a könyvtár vagy maga az állam szabja meg, mi a nem kívánatos tartalom a felhasználók számára.[4]

[3] Parti K.: „10 dolog, amit utálok benned", avagy a kormányzati szintű internet-blokkolás kritikája a német törvény kapcsán. Infokommunikáció és Jog, 2010. június, 97–104. o.

[4] Tous, J.: Government filtering of online content. e-Newsletter on the Fight Against Cybercrime, vol. 1, no. 2, 2009, pp. 14–20.; Callanan, K. – Gercke, M. – de Marco, E. – Dries-Ziekenheimer, H.: Internet Blocking. Balancing Cybercrime Responses in Democratic Societies. Aconite Internet Solutions, 2009, pp. 11–20.

Megoldások az illegális tartalom blokkolására

Honnan ered az internetblokkolás szükségessége?

Az internet robbanásszerű fejlődésével elszaporodtak az úgynevezett tartalombűncselekmények. Ilyen a kábítószerrel és egyéb, az emberi szervezetre káros anyagokkal visszaélés, az extrém tartalmak (idegengyűlölet, terrorszervezetet népszerűsítő, terrorszervezetbe toborzó weboldalak, fanatikus vallási szekták weboldalai, étkezési rendellenességek weboldalai, pornográfia), valamint a speciális társadalmi csoportokat sértő tartalmak (gyermekek online szexuális kizsákmányolása, gyermekek egészséges erkölcsi fejlődését sértő tartalmak). Az Európai Unió Tanácsa és az Európa Tanács korán felismerte a káros tartalmak online terjesztésében rejlő veszélyt, így már az 1990-es évek végén megkezdődött az ellenük való összehangolt védekezés alapjainak lefektetése, ahogy látható ez a gyermekek szexuális kizsákmányolása[5], a számítástechnikai bűnözés[6], a terrorizmus elleni globális küzdelem[7], az információs rendszerek elleni támadások[8], valamint a szervezett bűnözés[9] terén született európai és nemzetközi jogszabályok arzenáljából – hogy csak a legfontosabbakat említsük. Az alapvető kérdés az állam büntetőjog-érvényesítési kötelezettségével kapcsolatos, nevezetesen: hol az a határ, ahol valamely illegális tartalom már oly mértékben elszaporodottnak – következésképpen zavarónak – tekinthető, hogy ellene a lehető legmagasabb, centrális szinten kell intézkedéseket hozni. Mivel erre a kérdésre rendkívül sokféle válasz lehetséges[10], vizsgáljuk meg az illegális tartalmak elleni védekezés másik láncszemét, az internetszolgáltató oldalát!

---

[5] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse of 25. 10. 2007 (ETS No. 201); A Tanács 2004/68/IB kerethatározata (2003. december 22.) a gyermekek szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről. HL L 013, 20/01/2004 P. 0044–0048; Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision. 2004/68/JHA, Brussels, 29. 3. 2010, COM(2010) 94 final.

[6] Convention on Cybercrime of the Council of Europe of 23. 11. 2011 (ETS No. 185).

[7] A Tanács 2002/475/IB kerethatározata (2002. június 13.) a terrorizmus elleni küzdelemről. HL L 164., 2002. 6. 22., 3. o.; A Tanács 2008/919/IB kerethatározata (2008. november 28.) a terrorizmus elleni küzdelemről szóló 2002/475/IB kerethatározat módosításáról. HL L 330/21 of 9. 12. 2008.; Council of Europe Convention on the Prevention of Terrorism of 16. 5. 2005 (ETS No. 196).

[8] A Tanács 2005/222/IB kerethatározata (2005. február 24.) az információs rendszerek elleni támadásokról. HL L 69/67., 16. 3. 2005.

[9] United Nations Convention Against Transnational Organized Crime of 8. 1. 2001. (A/Res/55/25).

[10] Feinberg, J.: The Moral Limits of Criminal Law Volume 1: Harm to Others. Oxford University Press, New York, 1984

A szolgáltató felelőssége a felhasználói tartalomért

A közvetítő szolgáltató *(intermediary service provider,* a továbbiakban: ISP) olyan szolgáltató, amely a hozzáférést, illetve az információ átvitelét, a tárhelyet, a gyorsítótárat és/vagy a keresőszolgáltatást biztosítja a tartalom szolgáltatója (azaz esetünkben a felhasználó) számára.

Az ISP felelősségét európai uniós szinten elsődlegesen a 95/46/EK irányelv az adatvédelemről[11], valamint a 2000/31/EK irányelv az elektronikus kereskedelemről[12] szabályozza.

A szolgáltató, amely puszta összeköttetést *(mere conduit),* gyorsítótárazó *(caching)* vagy tárhely *(hosting)* szolgáltatást nyújt, alapesetben sem büntetőjogi (szerzői jog vagy magántitok megsértése), sem polgári jogi értelemben (károkozás miatti vagy egyéb kompenzációs kötelezettség) nem felel a felhasználó által feltöltött tartalomért, feltéve, ha nem ő maga kezdeményezte a feltöltést/hozzáférhetővé tételt/átvitelt, ha nincs szerepe a fogadó felek kiválasztásában, továbbá ha nem szelektálta vagy módosította (szerkesztette) a felhasználó által feltöltött tartalmat. Ez magában foglalja az adatok automatikus átvitelét, valamint közbenső, illetve átmeneti tárolását is, amennyiben a szolgáltatás kizárólag az adatátvitelre/-tárolásra terjedt ki, valamint az így továbbított adatot a szolgáltató nem tárolta tovább az átvitelhez minimálisan szükséges időnél.[13]

Az ISP illegális tartalommal kapcsolatos kötelezettségét érintve az elektronikus kereskedelmi irányelv kimondja, hogy a tagállam bírósága vagy közigazgatási hatósága a jogsértés megszüntetésére vagy megelőzésére kötelezheti a szolgáltatót.[14]

Az ISP-nek ezekben az esetekben a jogsértés megszüntetése érdekében kötelező együttműködnie a hatóságokkal a jogsértés megelőzése vagy megszüntetése érdekében. A tárhelyszolgáltatók vonatkozásában pedig a tagállamok eljárásokat alakíthatnak ki a jogsértő információ eltávolítására vagy a hozzáférés megszüntetésére.[15]

---

[11] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (adatvédelmi irányelv). HL L 281., 23/11/1995, P. 0031–0050.

[12] Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem egyes jogi vonatkozásairól (elektronikus kereskedelemről szóló irányelv). HL L 178., 17/7/2000. P. 0001–0016.

[13] Preambulum (46) és 12-14. cikk; elektronikus kereskedelmi irányelv; 25. cikk (2) bek.; adatvédelmi irányelv.

[14] 12. cikk (3) bek.; 13. cikk (2) bek.; 14. cikk (3) bek.; elektronikus kereskedelmi irányelv.

[15] 14. cikk (3) bek.; elektronikus kereskedelmi irányelv.

A 2006/24 EK irányelv az adatmegőrzésről[16] (a továbbiakban: adatmegőrzési irányelv) *„[a] nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtóinak vagy a nyilvános hírközlő hálózatok szolgáltatóinak az általuk előállított vagy általuk feldolgozott adatok megőrzésére vonatkozó kötelezettségeit szabályozza, annak biztosítása érdekében, hogy ezen adatok az egyes tagállamok nemzeti joga által meghatározott súlyos bűncselekmények kivizsgálása, felderítése és üldözése céljából rendelkezésre álljanak"*[17]. Az irányelv kötelezi az ISP-t a forgalmi, a helymeghatározási és az ezzel kapcsolatban keletkező felhasználói adatok rögzítésére és azok 6–24 hónapig történő megőrzésére.

Ha a nyomozó hatóságtól vagy a bíróságtól adatszolgáltatás iránti megkeresést kap, a büntetőeljárás céljaira köteles átadni az általa megőrzött adatokat. Radikális kritikusok ezt az ISP monitorozási kötelezettségének bevezetésére tett kísérletként értelmezik. Ezek a hangok azonban nem számolnak azzal, hogy az ISP valójában rögzítés és megőrzés nélkül is képes lenne monitorozni a felhasználói tevékenységet, mindazonáltal az adatmegőrzési irányelv nem mondja ki kifejezetten az ISP monitorozási kötelezettségét. Ellenkezőleg: hangsúlyozza, hogy az ISP – irányelvben előírt kötelezettségének teljesítése keretében – csupán „visszatartja" *(retain)* a szóban forgó adatokat a törléstől, legfeljebb az irányelvben meghatározott időre. Mindazonáltal a legtöbb, az adatmegőrzési irányelvben nevesített adatfajta úgynevezett számlázáshoz szükséges adat *(Charging Data Record,* azaz CDR), amelyet az ISP automatikusan rögzít. Ezek a szolgáltatás teljesítéséhez, valamint ellentételezéséhez szükséges adatok.

A tagállamokban heves viták tárgya, hogy az adatmegőrzési irányelvet a belső jogba átültető jogszabályok mennyiben tartják tiszteletben a digitális állampolgári jogokat *(digital civil rights* mint az online magánélet tiszteletben tartásához való jog, az online szólás- és véleménynyilvánítás szabadsága, valamint az online adatvédelem joga). A kritikusok leginkább azt az érvet hangoztatják, hogy a jogalkotók a szükségesség és az arányosság követelményének nem megfelelően, a cél nélküli adatrögzítés előírásával az úgynevezett készletező adatrögzítést írták elő az ISP-knek. Ezek az érvek számos tagállamban alkotmányos vitákhoz vezettek.[18]

Alkotmányos viták ide vagy oda, az leszögezhető, hogy az irányelv nem kötelezi a felhasználói tartalmak monitorozására vagy azok utáni „nyomozásra"

[16] Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról (adatmegőrzési irányelv). HL L 105/54., 13. 4. 2006.

[17] 1. cikk (1) bek.; adatmegőrzési irányelv.

[18] 2009-ben Romániában, 2010-ben Németországban és 2011-ben Csehországban.

az ISP-ket. Ez tehát egyértelműen kizárja a felhasználói tartalmak puszta tárolásáért vagy továbbításáért való felelősséget.

A legfrissebb európai jogszabály egyértelműen behatárolja az ISP felelősségét: a 2009/136/EK irányelv[19] megerősíti, hogy az ISP nem felel a felhasználó által előállított információ puszta továbbításáért *(mere conduit* szabály), valamint leszögezi, hogy nem az ISP feladata annak meghatározása, hogy valamely tartalom, alkalmazás vagy szolgáltatás jogszerű vagy jogellenes. Az irányelv szerint az ISP-t továbbra sem terheli monitorozási kötelezettség, így csak külön erre vonatkozó értesítésre kell eltávolítania a kérdéses tartalmat.

Az online közzétett tartalomért tehát elsősorban a tartalom feltöltője/szolgáltatója felelős. Így, ha a tartalom közzététele szerzői jogot sért, vagy nem tartja tiszteletben más felhasználó magánélethez fűződő jogait, akkor elviekben csak a tartalom feltöltője felel az okozott károkért. Alapesetben a tartalom szolgáltatója az az egyéni felhasználó, aki ebbéli minőségében családi videóját tölti fel valamely online videomegosztó csatornára, képeit tölti fel social network site-ra, véleményét közli blogban vagy fórumon, vagy egyéb módon kreál online tartalmat (például weboldalt szerkeszt).

Kérdés, hogy mikor minősül maga a szolgáltató is tartalomszolgáltatónak. Például tartalomszolgáltatói *(content provider/editor)* felelősséggel tartozik-e, hogyha a személyes tartalmat nem ő töltötte fel ugyan, ám valamilyen elv alapján (tetszési index, megfeleltetési kérdőív stb.) szelektálta, kiválasztotta a megjelenítendő tartalmat? Tartalomszolgáltatónak minősül-e a szolgáltató, ha a felhasználó által feltöltött tartalomhoz más tartalmat is hozzáadott (hiperlinkelte, hirdetést, reklámot fűzött hozzá)? Ez utóbbi eset tovább bontható a felhasználói tartalommal tartalmilag rokon és nem rokon – attól függetlenül, de azonos oldalon megjelenő –, valamint a profitorientált és nem bevételnövelő hirdetésekre is.

Abban az esetben, ha az ISP kizárólag a tartalomfeltöltés vagy az internethozzáférés technikai platformját és feltételeit teremti meg, az a kérdés, mely esetben felel a felhasználó által feltöltött tartalomért: ha tudomása volt arról, hogy a tartalom illegális és meghatározott időn belül nem távolította el (további kérdés

[19] Az Európai Parlament és a Tanács 2009/136/EK irányelve (2009. november 25.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról. HL L 337., 18. 12. 2009, P. 0011–0036.

ilyen esetben, hogy meg kell-e várnia a sértett értesítését és levételi kérelmét, vagy enélkül kell eltávolítania az illegális tartalmat); vagy ha nem volt tudomása arról, hogy a tartalom illegális, de szerkesztette, címkézte vagy továbbította a tartalmat; illetve ha nem volt tudomása arról, hogy a tartalom illegális, és a közzétételéhez pusztán a technikai platformot adta.

Utóbbi két esetben megválaszolandó az a kérdés is, hogy a *jogalkalmazói gyakorlat szerint* valóban elvárt-e a szolgáltatótól a monitorozási kötelezettség, azaz ellenőriznie kell-e a platformján közzétett tartalmak jogszerűségét.

Erre az Európai Bíróság esetjoga szolgál némi tisztázó gyakorlattal, különösen a *Google v. Louis Vuitton*-ügyben hozott döntés[20], valamint a *L'Oréal v. eBay*-ügyben a bíróság előzetes döntéshozatali eljárása.[21]

Az első esetben a bíróság emlékeztetett arra, hogy a semlegességi elv a felelősség alóli kivétel alapja. A második esetben a bíróság kifejtette, hogy ha az adásvételi tevékenységet folytató weboldal operátora (üzemeltetője, „hostja") aktív szerepet vállal a tranzakciók lebonyolításában, akkor tárhelyszolgáltatóként nem illeti meg az elektronikus kereskedelmi irányelv 14. cikke szerinti felelősség alóli mentesség.[22]

A bíróság továbbá kijelentette, hogy *„Ellenben ahol az operátor a kérdéses ajánlat megjelenéséhez és kereshetőségéhez optimalizáló vagy reklámozó szolgáltatást is csatol, megfontolás tárgyát képezi, hogy szerepe továbbra is neutrálisnak tekintendő-e a vevő és az eladó, valamint a potenciális vásárlók viszonylatában, vagy ehelyett inkább aktívan részt vesz az adott ajánlatok adatainak szerkesztése, kiegészítése és az adatok feletti kontroll révén. Éppen ezért a szóban forgó adatokkal kapcsolatban (az operátor) szerepe nem tekinthető az elektronikus kereskedelmi irányelv 14. cikk (1) bekezdés szerint neutrálisnak."*[23]

---

[20] European Court of Justice. Judgment of the Court (Grand Chamber) of 23 March 2010 (reference for a preliminary ruling from the Cour de cassation – France). Google France, Google, Inc. v Louis Vuitton Malletier (C-236/08), Viaticum SA, Luteciel SARL (C-237/08), Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08). OJ C 134., 22. 5. 2010, p. 2.

[21] European Court of Justice. Case C-324/09. Judgment of 12 July 2011. http://curia.europa.eu [2011. 07. 18.]

[22] L'Oréal v. eBay, para. 123.

[23] *"Where, by contrast, the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 2000/31."* European Court of Justice, Case C-324/09. Judgment of 12 July 2011, para. 116.

Ha tekintetbe vesszük, hogy a mai, világkereskedelmi nagyvállalatok által üzemeltetett internetplatformok a web 2.0 generációhoz tartoznak, különösen nagy szükség lenne a meglévő szabályozási keretek felülvizsgálatára, nevezetesen hogy szolgáltathat-e a hatályos szabályozás megfelelő válaszokat az új helyzetekre.

Jääskinen bíró a *L'Oréal v. Google*-ügyben kifejtett véleményében a szolgáltató semlegességi elv alóli kivételének jogát nem a *Google v. Louis Vuitton*-ügyben az imént idézett alapokon kritizálta. Szerinte el kell kerülni a szolgáltató felelősségének üzleti-kereskedelmi ügyletekben történő, fő szabály szerinti kizárását, ehelyett inkább minden esetben az *aktivitásának jellegét* kell vizsgálni. A bíró kifejti, hogy *„Amíg bizonyos cselekmények esetében – az irányelv céljának érvényesítése érdekében – ugyan egyértelműen kizárt a (szolgáltató) felelőssége, addig más (szolgáltatói) cselekvések esetében a tagállamok »megszokott« felelősségi szabályai lehetnek alkalmazandók"*[24].

A kérdés tehát továbbra is megválaszolatlan: vajon a web 2.0 érában továbbra is alapszabály lehet-e az ISP-t (a weboldalak hostolásáért, fenntartásáért, szerkesztéséért, az adatok továbbításáért) megillető semlegességi elv, amely szerint az ISP tevékenysége „pusztán technikai, automatikus és passzív természetű", és hogy az ISP-nek *„az általa továbbított és tárolt információ természetére vonatkozóan sem tudása, sem ellenőrzési joga nincsen"*[25]? A felelősség alóli kivétel jogi status quóként jelent meg az idézett esetekben. Az ISP elektronikus kereskedelmi irányelv szerinti felelőssége és az internet-blokkolási intézkedések viszonyát illetően azonban újabb kérdések merülhetnek fel:

- Értesítenie kell-e az ISP-nek a felhasználóit arról, hogy a szolgáltatást illegális tartalmak blokkolásának kötelezettsége terheli?
- Fel kell-e világosítania a felhasználókat arról, milyen (jellegű) tartalmakat nem fognak tudni elérni (általános szerződési feltételek), illetve milyeneket ne töltsenek fel (felvilágosítási, edukációs jellegű tájékoztatás)?
- Felelős-e azért, ha az eltávolított tartalom újra megjelenik (más néven), és azt nem teszi hozzáférhetetlenné?
- Felelős-e az ISP a túlszűrésért? (Ez az alkalmazott blokkolási módszeren alapul: ha nem hatol elég „mélyre" a tartalom vizsgálatában – mélyzsebvizsgálat –, akkor valószínű, hogy túlszűr vagy alulszűr az adott blokkolási módszer.)
- Felelős-e az ISP a felhasználók *tájékoztatásáért* a lehetséges túlszűrési kockázatokról?

[24] *"while certain activities [...] are exempted from liability, as deemed necessary to attain the objectives of the directive, all others [...] remain in the 'normal' liability regimes of the Member States"*. Advocate General Jääskinen, Opinion on the case L'Oreal v. Google, para. 149.

[25] Google v. Louis Vuitton: i. m. para. 113.

– Végül: van-e bejelentési kötelezettsége a hatósághoz – feketelistás szűrés esetén –, ha új, a listán nem található illegális tartalmat talál?

A tanulmány következő része bemutatja az alkalmazott internet-blokkolási megoldásokat, és az előbbi kérdéseket (legalábbis részben) megválaszoló gyakorlatot.

Internet-blokkolási megoldások és az ISP felelőssége az Európai Unióban

Németország

A német jog a multimédia-törvényben (Telemediengesetz; TMG § 10) implementálta az elektronikus kereskedelmi irányelv *mere conduit* szabályát. E szerint az ISP nem felel a felhasználói tartalomért, hacsak nem hanyag gondtalanságból vagy esetleges szándékkal kerülte el a figyelmét annak illegális mivolta. Ugyanerre az analógiára (Teledienstgesetz; TDG, Mediendienstestaatsvertrag; MDStV) az árverésszervező weboldalakon a felhasználó által harmadik személynek okozott kárért a hozzáférésszolgáltató alapszabály szerint nem felel.

Emellett viszont bizonyos esetekben megállapítható bűnrészesi járulékos felelőssége. E szerint nem csupán a közvetlen tettes (a felhasználó) felel az általa harmadik személynek okozott kárért, hanem az a szolgáltató is, amelyik akár esetleges szándékkal részt vett harmadik fél jogának megsértésében – feltéve, ha a szolgáltatót monitorozási, tartalom-felülvizsgálati kötelezettség terhelte. A szövetségi legfelsőbb bíróság döntése értelmében, amint az ISP tudomást szerez harmadik fél jogának sérelméről, *azonnal* gondoskodnia kell a jogsérelem megismétlődésének elkerüléséről: a tartalom eltávolításáról, a jogsértő felhasználó kizárásáról, illetve felhasználói jogainak felfüggesztéséről.

Németországban 2009. május 5-én látott napvilágot a kommunikációs hálózatokon továbbított gyermekpornográf felvételek internetszolgáltatók általi szűrésére és blokkolására[26] vonatkozó törvényjavaslat.[27] A javaslat szerint a Szövetségi Bűnügyi Hivatal (Bundeskriminalamt; a továbbiakban: BKA) listát kell hogy vezessen az olyan FQDN-ekről[28], IP-címekről és multimédiás anyagok elérési útvonalairól, amelyek a német büntető törvénykönyv (StGB § 184b) értelmében gyermekpornográfiát

[26] Bár szemantikailag a szűrés és a blokkolás mást jelent – míg a szűrés (filterezés) a megfigyelésre, a blokkolás a már azonosított tartalom továbbjutásának megakadályozására vonatkozik –, a tanulmányban szinonimaként használjuk ezeket a fogalmakat.

[27] Entwurf eines Gesetzes zur Bekampfung der Kinderpornographie in Kommunikationsnetzen. Drucksache 16/12850, 05. 05. 2009; Gesetzesbeschluss des deutschen Bundestages. Drucksache 604/09, 19.06.09. http://www.bundesrat.de/cln_090/SharedDocs/Drucksachen/2009/0601-700/604-09,templateId=raw,property=publicationFile.pdf/604-09.pdf [2012. február 20.]

[28] Full Qualified Domain Name, azaz teljes vagy abszolút doménnév, amely a doménnév helyét abszolút pontossággal meghatározza a tartománynév-hierarchiában.

tartalmaznak, vagy amelyek ilyen tartalmakra mutatnak, hivatkoznak. A BKA a törvény hatálya alá tartozó nagyobb internetszolgáltatóknak minden munkanap aktualizált blokkolási listát bocsát rendelkezésére. Az üzemszerűen legalább tízezer felhasználónak szolgáltatást nyújtó ISP-k e lista alapján legkésőbb hat órán belül kötelesek megtenni a *„megfelelő és elvárható műszaki lépéseket a listában szereplő multimédiás tartalmakhoz való hozzáférés megnehezítésére"*. A blokkolásnak *„legalább a domének szintjén"* kell megtörténnie. A szolgáltató az illegális tartalmat közzétevő felhasználót *„stopközlemény"* formájában értesíti a blokkolás okáról és a BKA elérhetőségeiről arra az esetre, ha a tartalom közzétevője kifogásolná a blokkolást. A blokkolást végző szolgáltatók jogosultak a személyes adatok gyűjtésére és felhasználására, amilyen mértékig az szükséges a blokkoláshoz, valamint kötelesek átadni az adatokat a nyomozó hatóságnak, büntetőeljárás céljára.

A javaslatot a német parlament a 2009. június 18-i ülésén elfogadta. A törvény azonban végül nem vált végrehajthatóvá, mivel számtalan vitát generált.[29] A törvényt érő támadásoknak az alapja az, hogy hatékonysága nem kielégítő, miközben aránytalanul beavatkozik az alapvető állampolgári jogok gyakorlásába, továbbá az internetszolgáltatók jogosultságait sem kíméli.

Az olyan egyszerű szűrési/blokkolási módszer, amilyen a német megoldás (a domének DNS-szintű manipulációja), nem túl hatékony, mivel ennek során nem különíthetők el egyértelműen az azonos doménnévhez tartozó *illegális és legális tartalmak.* Ugyanezen okból gyakran túlszűrnek: legális tartalmakat vagy legális weboldalakat is blokkolhatnak a felhasználók elől. Az alulszűrés hatására továbbra is elérhetők az illegális tartalmak, a túlblokkolás viszont sérti a felhasználók információhoz jutási szabadságát. Emellett a német megoldás kuriózuma, hogy csak a nagyobb (a több mint tízezer felhasználót kiszolgáló) német hozzáférés-szolgáltatókon keresztül elérhető tartalmakra vonatkozott volna, így az, aki kisebb vagy külföldi szolgáltatókon keresztül éri el az internetet, továbbra is hozzáfért volna az illegális tartalmakhoz.[30] Ez a helyzet világosan mutatja, hogy mindenütt jelenlevősége miatt az internet mennyire nehezen kontrollálható, és koregulációs,

[29] 2011 februárjában a német Internetblokkolás és Cenzúra Elleni Szervezet (AK Zensur) benyújtotta alkotmányjogi panaszát az internetblokkolását előíró törvény ellen. 2011 áprilisában a német konzervatív és liberális kormánypártok koalíciós bizottsági ülésükön egyetértésre jutottak abban, hogy az internet blokkolását előíró törvény annak ellenére is elfogadhatatlan, hogy elsődlegesen a gyermekpornográf tartalmak elleni védekezést szolgálja. German Internet blocking law to be withdrawn.
http://www.edri.org/edrigram/number9.7/germany-internet-blocking-law [2011. november 1.]

[30] Az internet-blokkolási rezsimek megbízhatóságáról lásd: http://www.opendns.com [2012. február 20.]

felülről jövő szabályozással – amelyek kikényszeríthetősége az államhatárokon belül marad – mennyire nehezen szabályozható.[31]

A blokkolás hatékonysága nem arányos az alkotmányos és emberi jogokba és alapvető szabadságokba való beavatkozás mértékével – ugyanis az információhoz jutás és a véleménynyilvánítás szabadsága sérül, miközben a sértettek és a felhasználók megfelelő védelme nem garantált.

A doménalapú blokkolás egyik hasznos hozadékaként fogalmazódik meg, hogy ilyen módon a felhasználók webes böngészései is nyomon követhetők, ami pedig lehetőséget ad a gyermekpornográfia iránt érdeklődők elleni büntetőeljárás indítására. A koncepció lényege az, hogy mivel a feketelistán szereplő domének mind gyermekpornográf tartalomra mutatnak, így mindazon felhasználók ellen, akik csak *megpróbálják kijátszani* a centrális blokkot – például más szolgáltatóhoz csatlakoznak –, automatikusan büntetőeljárást lehetne indítani. A blokk megkerülése ugyanis igazolná a megszerzés előkészületének (elkövetési magatartás) szándékosságát.[32]

További aggályként merült fel a német törvénnyel szemben, hogy bírói jóváhagyás nélkül lehetett volna összeállítani és frissíteni a blokkolási listát, hiszen nem volt kijelölve olyan független testület, amely felülbírálhatta volna a nyomozó hatóság döntését. Amellett, hogy a lista folyamatos megújítása és alkalmazása óriási erőfeszítés, nem is lenne célszerű kihagyni a bíróságot mint független kontrollfunkciót a lista frissítéséből.

A blokkolásra kötelezett ISP felelősségét a hivatkozott német törvény nem tisztázta kellő részletességgel. Nem derült ki, mi a szolgáltató kötelessége, hiszen a törvény a domének „minimális" blokkolását írta elő a szolgáltatók számára. Hogy ezen felül még milyen kötelesség terhelte a szolgáltatót, arra a törvény nem tért ki.[33] A törvény (TMG § 8a) szerint, ha az ISP előírásszerűen valósította meg a blokkolást, akkor az átengedett illegális tartalmak tekintetében megillette volna a felelősség alóli mentesség (*mere conduit* elv). Csakhogy a törvény nem részletezte, milyen lépéseket tegyen a szolgáltató a megfelelően teljesített, ámde *eredmény nélkül maradt blokkolás után.* Nem tisztázta, hogy elveszti-e a szolgáltató a felelősség alóli mentességét, ha olyan blokkolási intézkedéseket tesz, amelyek nem (vagy továbbra sem) vezetnek eredményre.

---

[31] Maier, B.: How has the law attempted to tackle the borderless nature of the Internet? International Journal of Law and Information Technology, vol. 18, no. 2, 2010, pp. 142–175.

[32] Sieber, U.: Sperrverpflichtungen gegen Kinderpornographie im Internet. Juristen Zeitung, Bd. 64, Nr. 13, 2009, S. 657.

[33] Uo.

Emellett az sem volt világos, hogy az információszolgáltatók élhetnek-e az állammal szemben kártérítési igénnyel *legális tartalom járulékos blokkolása* esetén.

A törvény (TMG § 8a. 5. bek.) előírta volna a hozzáférés-szolgáltatóknak, hogy a feketelistában szereplő doméneken illegális tartalmat közzétevő felhasználók adatait rögzítsék és azokat bűnüldözési célra adják át a nyomozó hatóságnak. Így azonban nemcsak a tartalmat közzétevők adatait, de a tartalmat *lekérdezők* IP-címeit is megismerhette volna a nyomozó hatóság. Ezzel a szolgáltató egyfelől beavatkozott volna a felhasználók információkkal való szabad rendelkezési jogába, másfelől a feketelistás tartalmak lehívása a felhasználókra kompromittáló, a nyomozó hatóság számára pedig félrevezető információt szolgáltathatott volna. Hiszen olyan esetekben is elrendelhettek volna nyomozást, amikor a felhasználó által keresett, egyébként legális weboldal olyan illegális linket tartalmazott, amely szerepelt a feketelistában. A lehívott weboldalakon szereplő tartalom az illegális linkkel együtt megtalálható a felhasználó számítógépén, az automatikus letöltések között (a gép gyorsítótárában), ami szintén hamis nyom lehet.

A bemutatott, feketelistás, doménalapú internet-blokkolási technológia és a rá épített koncepció az elérni kívánt céllal nem arányos: a túlszűrés miatt drasztikusabban avatkozik be az állampolgárok alapvető szabadságjogaiba, mint amilyen sérülést a megelőzni kívánt magatartás okozna. Fontos megérteni, hogy a tartalomszolgáltatók véleményszabadsága és a felhasználók információszabadsága nem az illegális tartalmak blokkolása miatt sérül, hanem mert a doménalapú blokkolás legális tartalmakat és olyan funkciók használatát is ellehetetlenítheti, mint a levelezés (vagy például az IGroups szolgáltatások). A blokkolási listák folyamatos bővülésével párhuzamosan pedig mind több legális tartalom és internetfunkció is elveszhet.

Nem állnak rendelkezésre kutatások a tekintetben, hogy milyen valódi károkat okoz a gyermekpornográfiával való szembesülés – sem a felnőtt, sem a gyermekkorú internetezők számára. Az viszont egyértelmű, hogy csak és kizárólag központi szűréssel nem lehet megóvni a felhasználókat attól, hogy illegális anyagokkal találkozzanak. Éppen ezért mindenféle internetszűrést az adott korcsoportra specializált, megfelelő tájékoztatásnak (ismeretterjesztés, oktatás, veszélytudatosítás) kellene kiegészítenie.[34] A gyermekpornográfia és a hozzá kapcsolódó, a gyermekek kizsákmányolását célzó jelenségek azok közé a legsúlyosabb bűncselekmények közé tartoznak, amelyekre az Emberi Jogok Európai Bírósága (a továbbiakban:

[34] Lásd még: A Google és a Yahoo is az ausztrál internet-ellenőrzési tervek ellen. Sg.hu, 2010. február 18. http://www.sg.hu/cikkek/72596/a_google_es_a_yahoo_is_az_ausztral_internetellenorzesi_tervek_ellen

EJEB) is különös figyelmet fordít. Nagyon fontos azonban megérteni azt, hogy az illegális webtartalmak blokkolása *nem mint* a bűncselekmények elkövetőinek szólás- és véleményszabadságát sértő intézkedés, illetve *nem mint* az illegális információhoz jutás szabadságának sérelme kifogásolható. A centrális (kormányzati szintű) blokkolási intézkedések azért elfogadhatatlanok, mert általában doménszintű blokkolást vezetnek be – ahogy azt az iménti német esetben is bemutattuk –, ami nemcsak az illegális tartalmakat tartja távol a felhasználóktól, hanem adott esetben az ilyen oldalakra linkelt legális tartalmakat is, valamint ellehetetleníti az önmagukban véve nagyon is legális e-mail- és más online alkalmazások működését. A feketelisták folyamatos bővítésével pedig egyre több legális tartalmat és internetfunkciót zárnak el a normakövető felhasználók elől.

Annak ellenére, hogy az internetblokkolásra vonatkozó, előbbiekben bemutatott jogszabályok nem léptek hatályba, Németországban eseti intézkedésként van gyakorlata az illegális online tartalom blokkolásának. Ilyen volt 2002-ben a Düsseldorfi Regionális Közigazgatási Bíróság által kiadott blokkolási utasítás, amely arra kötelezte a németországi hozzáférés-szolgáltatókat, hogy ne engedjék át az Egyesült Államokban található szerverekről érkező náci propagandát hirdető weboldalakat.[35] A blokkolási utasítást a Münsteri Fellebbviteli Közigazgatási Bíróság helybenhagyta, és indoklásában kifejtette, hogy a szóban forgó blokkolási utasításra a német szélsőjobboldali ideológia újjáéledésének megfékezése érdekében igenis szükség van. Az ilyen blokkolási utasításnak azonban meg kell felelnie az arányosság és a technikai kivitelezhetőség követelményeinek. (Ilyen például a hozzáférés-szolgáltatókat esetenként terhelő IP-cím-blokkolási, doménnévszerver-módosítási, valamint proxyszerver-alkalmazási bírói utasítás.) Időközben a Német Szövetségi Bíróság 2000-ben egy olyan iránymutató döntést *(Grundsatzurteil)* hozott, amely szerint például egy Ausztráliában található szerverre feltöltött holokausztagadó weboldal tartalomszolgáltatója *Németországban* akkor is felel a bűncselekmény (holokausztagadás) elkövetéséért, ha nem német (hanem az adott esetben ausztrál) állampolgár. Az ítélet azonban egyértelműen kizárta az illegális tartalmat hostoló ISP felelősségét.[36]

Magyarország

Magyarországon az elektronikus kereskedelmi irányelv rendelkezéseit a 2001. évi CVIII. törvény az elektronikus kereskedelemről, valamint a 2001. évi XXXV. törvény az elektronikus aláírásról implementálta.

[35] Bezierksregierung Düsseldorf, Aktenzeichen 21.50.30, 6 Februar 2002.
www.artikel5.de/rohetexte/sperrverfueg.pdf [2011. október 12.]

[36] 1 StR 184/00 vom 12. Dezember 2000
www.rechtsanwaltmoebius.de/urteil/bgh_auschwitzluege.pdf [2011. október 12.]

A szabályozás biztosítja a *mere conduit* princípium érvényesülését a hostszolgáltatók, valamint a keresőmotor-szolgáltatást üzemeltetők számára egyaránt, ám a hiperlinkekért való felelősség nem privilegizált. Az értesítési-levételi eljárást (notice-and-takedown, a továbbiakban: N&TD) az elektronikus kereskedelemről szóló törvény részletesen szabályozza. Az internet kormányzati szintű blokkolására ez idáig nem volt kísérlet az országban.

A 2011. január elsején hatályba lépő médiatörvény elviekben lehetővé teszi az internet centrális szintű kontrollját, mivel a korábbi törvénytől eltérően, nem tesz megkülönböztetést a hagyományos és az új médiák között: mindre egyöntetűen szigorú standardok kötelezők. A megfogalmazott kritikák szerint kiterjeszti a tartalommal szembeni védelmet a gyűlöletbeszédtől kezdve az uszításig és a szándékolatlan becsületsértésig. Az internetes sajtóorgánumokon, weboldalakon, fórumokon közölt tartalomért az ISP úgy felel, mintha elektronikus kereskedelemmel összefüggő szolgáltatást nyújtana (így az elektronikus kereskedelmi szolgáltatásokról szóló törvényben meghatározott felelősségi alakzatok érvényesek rá). Tehát ha az ISP a sértett vagy a médiafelügyeleti hatóság felszólítására nem távolítja el a sérelmezett tartalmat, akkor úgy felel, mintha ő maga lenne a tartalomszolgáltató. Jelenleg azonban még nincs gyakorlat a médiatörvényből eredő viták eldöntésére.

A Szegedi Fellebbviteli Bíróság az egyik ügyében megállapította a hostszolgáltató felelősségét szerzőijog-sértésben, mert egy felhasználó szerzőijog-védett recepteket tett közzé a weboldalán, a szolgáltató pedig ezekre mutató hiperlinkeket helyezett ki, amelyek segítségével a nagyközönség számára elérhetővé tette a szerzőijog-védett recepteket. A bíróság szerint a szolgáltatónak megvolt a *lehetősége* arra, hogy szelektáljon a jogvédett és a nem jogvédett receptek között, így, hogy ezzel éppen a szerzőijog-védett tartalmak tekintetében nem élt, felelőssé teszi őt a bűncselekmény elkövetésében.[37]

Egy másik ügyben a Legfelsőbb Bíróság kimondta, hogy a védjegybitorlást nem csupán az a felhasználó követte el, aki egy már létező márkára nagyon emlékeztető doménnevet regisztráltatott, hanem a doménnevet regisztráló *hatóság* is, amelynek tudnia kellett a két védjegy elnevezésének nagyfokú hasonlóságáról. A bíróság tehát a szolgáltatót nem tekintette pusztán adminisztratív funkciót betöltő szervnek, így a felhasználó tevékenységéért a szolgáltató felelősségét is megállapította, mivel érdemi tevékenységével aktívan hozzájárult a bűncselekmény elkövetéséhez.[38]

[37] Spindler, G.: Study on the Liability of Internet Intermediaries. Country Report – Hungary, 2007 http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf [2012. február 21.]
[38] Uo.

A következőkben kiskorúak képmásait illegálisan felhasználó (azokkal visszaélő) honlap hostszolgáltatójának felelősségét vizsgáljuk. A magyar nyelvű *pedomaci.hu* honlap kiskorúak más tárhelyre – közösségi oldalra – feltöltött képeinek az „újrahasznosításával" foglalkozott: azokat szexuális töltetű címmel és kommentekkel látta el, így tette közzé a honlapon. A honlap közvetlen célja azonban nem a sértetteknek való károkozás volt (még ha becsületsértő, illetve személyes adattal visszaélő tevékenységével végső soron ezt érte is el), hanem a honlapon elhelyezett reklámokból, hirdetésekből való bevételek szerzése.

A honlap hostszolgáltatója úgynevezett anonimizáló szolgáltató volt, amely a nála hostolt weboldalak feltöltőinek anonimitást ígért. 2009-ben és 2010-ben az illegális tartalmak bejelentésére szolgáló hotline-hoz és a rendőrséghez is számos bejelentés érkezett a felvételeken szereplő gyermekkorúak szüleitől, mivel a képeket a weboldal a hozzájárulásuk nélkül, továbbá becsületsértő, rágalmazó, megalázó kommentekkel ellátva szerepeltette. A honlap doménnevének eltávolítása a regisztrációs hatóság által – a hotline és civil jogvédő szervezetek felszólítására – megtörtént, mondván, önmagában a weboldal *elnevezése* is jogsértő, mivel kiskorúak szexuális kizsákmányolására utal. Mindamellett a hotline felhívására a host provider eltávolította a sértő tartalmat, ám ezután a weboldalt egy másik, immár egy egyesült államokbeli székhelyen működő hostszolgáltatónál *pedomaci.net* néven újra feltöltötték, így a weboldal – hasonló tartalommal és célzattal – továbbra is elérhető maradt.

Mivel az uralkodó jogértelmezés szerint magának a tartalomszolgáltatónak a tevékenysége nem valósít meg bűncselekményt (a sértettek „tevékeny közreműködése" miatt), így homályban marad, hogyan ítélné meg a bíróság a honlap hostszolgáltatójának felelősségét, valamint a honlapon hirdetéseit elhelyező többi felhasználó (szerkesztői) felelősségét, akik a hirdetéseik népszerűsítéséhez a botrányos honlap magas látogatottsági mutatóit használják fel. Felmerülhetne továbbá a közvetítő (anonimizáló) szolgáltató felelőssége is, ám mivel az nem köteles a szolgáltatását igénybe vevők tevékenységének monitorozására, így az általános szerződési feltételekben meghatározott, az illegális tevékenységtől tartózkodásra való kötelező figyelmeztetéssel és a felelősség kizárásával a mentesülés megoldott. A honlap eltávolításával kapcsolatban tett egyetlen hivatalos lépés a honlap nevének a doménnév-regisztrációs hatóság általi bevonása volt. Az azonban leszögezhető – ahogy arra a honlap üzemeltetőjének a doménregisztráló hatósághoz benyújtott panaszlevele is utal –, hogy önmagában a weboldal elnevezése nem egyértelműsítette a visszaélésszerű tartalmat.

A példák sok megoldatlan kérdést vetnek fel, amelyek alapján megállapítható, hogy az online visszaélések jogi szabályozása számos kiskaput hagy, így a jövőben

kiegészítésre szorul. A helyzet rendezésében a legtöbbet a civil jogvédő szervezetek, valamint az illegális tartalmak bejelentésére szolgáló hotline-ok tettek, ami azt mutatja, hogy a joghézagok betömésére online tartalommal kapcsolatos jogviták esetén sokkal alkalmasabbak az informális, önszabályozó jellegű intézkedések.

További európai megoldások

Az internet szabadságának kiterjesztett értelmezésére szolgáltat példát az EJEB a *K.U. v. Finland*-esetben.[39] Pontosabban szólva kiterjeszti az ISP bizalmi szabadságának határait – anélkül azonban, hogy deklarálná, hogy a szólásszabadság védelme a bűncselekményekre is vonatkozna. Egy 12 éves gyerek nevében, a gyermek tudta és beleegyezése nélkül az elkövető hirdetést tett közzé egy online ismerkedőfelületen. A hirdetésben szerepelt a sértett néhány személyes adata (neve, telefonszáma, személyes weboldala fotóval és egyéb részletekkel) és egy szexuális tartalmú felhívás. A sértett minderről úgy értesült, hogy üzeneteket kapott potenciális randevúpartnerektől, akik szexuális szolgáltatásait szerették volna igénybe venni. Az akkor hatályban lévő finn jogi szabályozásnak megfelelően, az ISP nem adta át a hatóságnak az elkövető IP-címét, mivel kötötte a „telekommunikációs szolgáltatásokban érvényesülő bizalmi elv". A Helsinki Kerületi Bíróság pedig visszautasította a szolgáltató kötelezését az IP kiadására, amely a szolgáltatás körében tudomására jutott titoknak minősült, amelynek feloldására a hatóság nem szolgáltatott megfelelő alapot. A finn jog szerint ugyanis rosszindulatú megtévesztésnek *(malicious misrepresentation)* minősülő magatartás nem olyan súlyú bűncselekmény, amely felhatalmazná a rendőrséget arra, hogy az ilyen ügyekben lekérhessék a szolgáltatótól a telekommunikációs azonosító adatokat. Ezt a döntést a magasabb szintű finn bíróságok is fenntartották. Végül a sértett soha nem jutott hozzá a róla hitelrontó hirdetést szerkesztő elkövető adataihoz, továbbá a hirdetést hostoló weboldal vezetőjének felelőssége sem volt megállapítható, mivel a cselekmény büntetendősége elévült.

Az EJEB úgy találta, hogy az eset sértette az Európai emberi jogi egyezmény 8. cikkébe foglalt magánélet tiszteletben tartásának jogát, azaz a *„valamely személy fizikai és morális integritását felölelő gondolatot".*[40] A bíróság indokolása szerint a 8. cikkben megfogalmazott jog nem pusztán az állam negatív, be nem avatkozási kötelezettségére utal, hanem *„elősegíti a magánélet tiszteletben tartásához fűződő jog széles körben való elfogadtatásának pozitív előírását, nem csupán az állam szintjén, hanem az egyének között is".*[41]

[39] Judgment of 2 December 2008, K.U. v Finland, application no. 2872/02.
[40] Court's judgment, para. 41.
[41] Uo. para. 43.

A bíróság amellett, hogy kinyilvánította, *„a szólásszabadság és a kommunikáció bizalma elsőbbséget élveznek, és a telekommunikációs szolgáltatások és az internet felhasználói magánéleti és véleménynyilvánítási szabadságának a tiszteletben tartása érdekében garanciális szabályokra szükség van”*, azt is kimondta, hogy *„az ilyen garancia nem lehet abszolút, és tekintettel más jogelvekre, eseti mérlegelésre szorul, mint amilyen a szabályszegések és a bűncselekmények megelőzése, vagy a mások jogainak és alapvető szabadságainak a védelme”*.[42]

Értesítési-levételi eljárás: az illegális tartalom eltávolítása önszabályozással

Az illegális online tartalmak blokkolása a legtöbb kritikát amiatt kapja, hogy nem törli, csupán – ideig-óráig – hozzáférhetetlenné teszi a feketelistás illegális tartalmakat. Az illegális tartalmak elleni küzdelem azonban csak akkor lehet sikeres, ha a hostszervereken tárolt tartalmat *törlik* is. Ezt a forródrótok (*hotline*-ok)[43] nemzetközi rendszere mozdítja elő, amely jogellenes tartalmakról fogad bejelentéseket. A forródrótok felszólítást küldenek a szolgáltatónak, amelyben felhívják, távolítsa el szerveréről az illegális tartalmat (N&TD eljárás).

Meg kell különböztetni a hostszolgáltató közvetlen, valamint közvetett értesítésén alapuló N&TD eljárást. Ha a nyomozó hatóság először a hotline-t értesíti az illegális tartalomról, amely a szolgáltatóhoz fordul a tartalom eltávolíttatása érdekében, ez sokkal gyorsabb reagálást tesz lehetővé. A legnagyobb nemzetközi ernyőszervezet, az INHOPE eleve azzal a feltétellel veszi fel tagjait, ha azok helyi, illetve országos szinten a nyomozó hatóság támogatását élvezik, hiszen ekkor garantált a gyors és zökkenőmentes értesítési láncolat és a levételi felhívásra való gyors reagálás. Ehhez képest az úgynevezett közvetett értesítési eljárás nem tartalmazta a hotline-t, tehát minden alkalommal a rendőrségnek kellett megkeresnie az ISP-t a tartalom eltávolítása érdekében.

E korábbi eljárás azért volt jóval nehézkesebb, mert az ISP-nek esetileg egyenként, részletesen meg kellett vizsgálnia, hogy az adott tartalom ténylegesen megfelel az eltávolítás követelményeinek, azaz ténylegesen bűncselekményt valósít-e meg. Az újabb, közvetlen eljárás azért jóval egyszerűbb, mert az ISP-nek ezt az eseti vizsgálati eljárását kikapcsolja.

---

[42] Uo. para. 49.

[43] A legnagyobb nemzetközi forródróthálózat az 1999-ben létrejött INHOPE, amelynek mára 33 országban van nemzeti forródrótja. Németország 1999, Magyarország 2005 óta tagja. Németországban jelenleg három, hazánkban egy hotline működik, amely az INHOPE tagja. A tagok listája: https://www.inhope.org/en/hotlines/facts.html [2011. október 12.]

Az ISP ahelyett, hogy minden esetet külön vizsgálna, automatikusan, vizsgálat nélkül eltávolítja a nemzeti hotline által előzetesen, standard kritériumok alapján megvizsgált tartalmakat.

A nemzeti hotline-ok mint az INHOPE tagszervei standard kritériumok alapján vizsgálják a tartalmakat. A gyorsaság és közvetlenség[44] garantálásához azonban az is kellett, hogy a hotline-ok finanszírozását ellátó Európai Bizottság 2010-ben kötelezővé tegye a hotline-ok számára az N&TD eljárás és a hozzá fűződő legjobb gyakorlatok alkalmazását.[45] A forródrótok hálózata tehát az önszabályozás jó példája. Olyan informális kapcsolatrendszert teremt, amely az INHOPE koordinációs tevékenysége nyomán standardizált eljárási szabályok szerint lép kapcsolatba a hostszolgáltatóval, amely köteles eltávolítani az illegális tartalmat.[46]

Az N&TD eljárás jelentőségét a tagállamok egyre több bűncselekménnyel kapcsolatban elismerik és promotálják. Így az Európa Tanács számítástechnikai bűnözésről szóló egyezménye kiegészítő dokumentumaként elfogadott ajánlás a káros tartalmak önszabályozásának előmozdításáról már 2001-ben a felhasználói szintű *(voluntary based)* internetszűrést támogatta, úgymint weboldalcímkézés, életkori minősítőrendszer, valamint a személyes azonosító kódok kiadása.[47]

Ezzel ellentétes tendenciaként, az EU 2004/68/EC irányelvének felváltására irányuló javaslat[48] már előírná az EU-tagállamok számára a gyermekek szexuális kizsákmányolására irányuló weboldalak kötelező *blokkolását.* Ennek ellenére az unió Polgári Szabadságjogi Bizottsága 2011. január 12-én tartott tárgybani vitáján 12 képviselőből 11 ellenezte a blokkolás kötelezővé tételét a tagállamok számára. Az indokok között szerepelt, hogy egyre kevesebb a statikus felület (weboldal),

[44] Az INHOPE 2010-ben közölt statisztikája szerint az N&TD eljárás belföldön, illetve az EU tagállamában található szolgáltató esetén 12–36 órát vesz igénybe, míg az Egyesült Államokban hostolt tartalom esetén 24–48 óra az eltávolítási eljárás átlagos ideje. INHOPE Annual Report 2010. http://www.inhope.org/Libraries/Annual_reports/2010_Annual_report.sflb.ashx [2011. október 12.]

[45] Részletekért lásd: http://www.inhope.org/system/files/INHOPE+BROCHURE.pdf [2011. október 12.]

[46] Moore, T. – Clayton, R.: The Impact of Incentives on Notice and Take-down. Seventh Workshop on the Economics of Information Society (WEIS 2008). June 25-28, 2008. http://weis2008.econinfosec.org/papers/MooreImpact.pdf [2011. október 12.]

[47] Council of Europe Committee of Ministers Recommendation Rec(2001) 8 of the Committee of Ministers to member states on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services). https://wcd.coe.int/wcd/ViewDoc.jsp?id=220387&Site=CM [2011. október 12.]

[48] Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision. 2004/68/JHA, Brussels, 29. 3. 2010, COM(2010) 94 final.

amelyet a gyakorlatban blokkolni lehetne, és a gyermekpornográfia terjesztői már nem az interneten, hanem inkább P2P hálózatokon cserélik a felvételeket, amelyekre pedig technikailag nem terjedhet ki a blokkolás. Ha pedig a szolgáltató mégiscsak elérhetetlenné tenne egy weboldalt, ez azonnal riasztaná a bűnelkövetőket, és lehetetlenné tenné a velük szembeni akció sikeres előkészítését.[49]

Az N&TD eljárás lehetővé teszi azt is, hogy a tartalomszolgáltatók (felhasználók, állampolgárok) tisztában legyenek jogaikkal. A jogállamiság egyik alapvető kritériuma a szabályok átláthatósága, amelynek nyomán az állampolgári viselkedés következményei kiszámíthatók, valamint a tisztességes eljáráshoz való jog, amely az átláthatóságon és a kifogás emelésének jogán (fegyveregyenlőség elve) nyugszik. A törlési eljárás bevezetése – a blokkolási helyett[50] – nemcsak átláthatóbbá tenné az eljárást, hanem a bíróságokat is tehermentesítené: a bíróságoknak csak azokat az eseteket kellene vizsgálniuk, amelyekben a tartalomszolgáltató kifogást emelt a tartalom eltávolítására irányuló felhívás ellen. Az N&TD általános bevezetése valószínűleg erősítené az állampolgári önkéntességet és altruizmust, amely az internet szabályozásának alapja. Az internetet nem lehet „kívülről", külső entitás által szabályozni. A *felhasználók közössége* tehet a legtöbbet az internet tartalmának „tisztasága", a jogszerűség megteremtése érdekében. Ehhez viszont első lépésként az szükséges, hogy a felhasználók értesülhessenek arról, ha az *általuk közölt tartalom* illegális.

Összegzés

A blokkolás technikáját, szintjét és ideológiáját körültekintően kell megválasztani ahhoz, hogy az alapvető jogok sértetlenek maradjanak, de a blokkolás is elérje a célját. Az internetszűrés technikái különösen alapvető jogokba való beavatkozásuk miatt aggályosak: a tartalomgazdák véleményszabadsága, a felhasználók információhoz jutási szabadsága, valamint a blokkolási technikától függően a távközlési titok is sérülhet. Az internet természetéből adódóan szinte minden blokkolási módszer megkerülhető, így nem igazán hatékony.

---

[49] A Polgári Szabadságok Bizottságának az uniós szintű internetblokkolás bevezetéséről folytatott nyilvános vitáját lásd: EDRi-gram Number 9.1, 12 January, 2011.
http://www.edri.org/book/export/html/2491 [2011. október 12.]

[50] Stellungnahme: Aktuelle Berichterstattung zu „Löschen statt Sperren".
http://www.eco.de/verband/202_8112.htm [2011. október 12.]; Löwenstein, S.: Löschen von Kinderpornos gelingt selten. Frankfurter Allgeimeine Politik.
http://www.faz.net/aktuell/politik/inland/internetseiten-loeschen-von-kinderpornos-gelingt-selten-11008405.html [2011. október 12.]

Amellett, hogy igen súlyos bűncselekmények megakadályozásának érdeke forog kockán, fontos megérteni azt is, hogy milyen lehetőségei vannak a megkerülésnek és hogy mi a kockázata a túlszűrésnek. Az állami szintű blokkolás nem nyújthat teljes védelmet, ráadásul hiányosságoktól szenved, továbbá – részben e hiányosságaiból adódóan – nem respektálja az alapvető digitális jogokat. Ám azt is láttuk, hogy a szolgáltatók által alkalmazott önszabályozó megoldások sem alkalmasak önmagukban az illegális tartalmak kiszűrésére. Az internet szabályozása nem oldható meg kizárólagosan sem ön-, sem pedig központi szabályozás keretében: a két terület szereplőinek összefogásával jöhet létre a megfelelő megoldás.

Ez az összefonódás a tekintetben is szükségszerű, hogy az állam internetblokkolásra vonatkozó törekvései nem valósulhatnak meg az ISP-k aktív közreműködése nélkül. De a kapcsolat fordítva is igaz: az ISP-k önszabályozó mechanizmusai csak az állam, illetve a piaci szféra politikai, illetve anyagi támogatásával működhetnek megfelelően.

Az EU egyértelműen szabályozza a közvetítő szolgáltató felelősségét. Látva azonban, mennyire széles területet ölel fel a kérdés, és milyen eltérő esetjogot alakított ki a direktívák értelmezésére az államok belső joga, a szabályalkalmazás gyakorlata korántsem ilyen egyértelmű. Éppen ezért szükség lenne az elektronikus kereskedelmi irányelv felülvizsgálatára, a gyakorlatban felmerülő kérdések tisztázására és egységesítésére.[51] Ezt az igényt maga az Európai Bizottság is felismerte, és 2010-ben nyilvános konzultációra hívta a feleket.[52]

A szubszidiaritás elvének érvényesülése, valamint a hatékonysági mutatók növelése érdekében az államnak teret kell engednie olyan önszabályozási megoldásoknak, amelyek evolúciója egyidős a globális elektronikus hálózatok kialakulásával, alkalmazásuk előmozdítja a közösségi bűnmegelőzést, a digitális írástudás fejlődését, valamint a felhasználói tudatosságot, miközben tiszteletben tartja az alapvető digitális jogokat. Ezeknek az önszabályozási megoldásoknak az egyik legkidolgozottabb és legelterjedtebb formája az értesítési-levételi eljárás, amelyet Európa számos országában alkalmaznak nagy sikerrel.

[51] Cunha, M. V. de A. – Marin, L. – Sartor, G.: Peer-to-peer privacy violations and ISP liability: Data protection in the user-generated web. EUI Working Paper LAW 2011/11, European University Institute, Florence, Department of Law, 2011

[52] Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC).
http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm [2011. október. 10.]

Irodalom

Callanan, K. – Gercke, M. – de Marco, E. – Dries-Ziekenheimer, H.: *Internet Blocking. Balancing Cybercrime Responses in Democratic Societies.* Aconite Internet Solutions, 2009

Cunha, M. V. de A. – Marin, L. – Sartor, G.: *Peer-to-peer privacy violations and ISP liability: Data protection in the user-generated web.* EUI Working Paper LAW 2011/11, European University Institute, Florence, Department of Law, 2011

Feinberg, J.: *The Moral Limits of Criminal Law Volume 1: Harm to Others.* Oxford University Press, New York, 1984

Löwenstein, S.: Löschen *von Kinderpornos gelingt selten. Frankfurter Allgeimeine Politik.* http://www.faz.net/aktuell/politik/inland/internetseiten-loeschen-von-kinderpornos-gelingt-selten-11008405.html [2011. október 12.]

Maier, B.: *How has the law attempted to tackle the borderless nature of the Internet?* International Journal of Law and Information Technology, vol. 18, no. 2, 2010

Moore, T. – Clayton, R.: *The Impact of Incentives on Notice and Take-down. Seventh Workshop on the Economics of Information Society (WEIS 2008).* June 25-28, 2008. http://weis2008.econinfosec.org/papers/MooreImpact.pdf [2011. október 12.]

Parti K.: *„10 dolog, amit utálok benned", avagy a kormányzati szintű internet-blokkolás kritikája a német törvény kapcsán.* Infokommunikáció és Jog, 2010. június

Senden, L.: *Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?* Electronic Journal of Comparative Law, vol. 9, no. 1, 2005 http://www.ejcl.org/91/art91-3.html [2011. október 12.]

Sieber, U.: *Legal regulation, law enforcement and self-regulation: A new alliance for preventing illegal content on the Internet.* In: **Waltermann, J. – Machill, M. (eds.):** *Protecting Our Children on the Internet.* Bertelsmann Foundation Publishers, Gütersloh, 2000, pp. 319–400.

Sieber, U.: *Sperrverpflichtungen gegen Kinderpornographie im Internet.* Juristen Zeitung, Bd. 64, Nr. 13, 2009

Spindler, G.: *Study on the Liability of Internet Intermediaries.* Country Report – Hungary, 2007.
http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf [2012. február 21.]

Tous, J.: *Government filtering of online content.* e-Newsletter on the Fight Against Cybercrime, vol. 1, no. 2, 2009