Parti Katalin

„10 dolog, amit utálok benned”, avagy a kormányzati szintű internet-blokkolás kritikája a német törvény kapcsán

Bevezetés

Az utóbbi években egyre-másra látnak napvilágot az interneten megjelenő illegális tartalmak központi blokkolására, filterezésére irányuló megoldások. Amellett, hogy a blokkolás eszközei nem túl hatékonyak, még jelentős erőfeszítést is igényelnek és az állampolgári jogok csorbításával is járnak. Az internet kormányzati szintű ellenőrzését általában az online gyermekpornográfia elleni küzdelem égisze alatt vezetik be, de alapja lehet számos más ön- és közveszélyesnek tartott cselekmény is. Azonban minél kisebb kárt okozna a tartalommal való szembesülés a felhasználó oldalán, illetve minél távolabbi az ok-okozati láncolat az elszenvedett kár és az adott tartalommal való szembesülés között, annál kevésbé indokolt a tartalom blokkolása. A megvalósíthatóság technikai, alkotmányos, emberi jogi aggályait a német internet-blokkolási törvénnyel (2009) kapcsolatban ismertetem.

Problémafelvetés

Az internet központi blokkolása mögött a legtöbbször az online gyermekpornográfia elleni küzdelem áll. A gyermekek szexuális kizsákmányolásáról szóló felvételek online megjelenése az ábrázolt személyek emberi méltóságát sérti, a velük való szembesülés az áldozatok traumatizálódásához – stigmatizálódáshoz, halmozott viktimizálódásához – vezethet. Ösztönzi az extrém pornográf tartalmak iránti keresletet, továbbá elfogadottá teszi a gyermekek szexuális kizsákmányolását a pornográfia-fogyasztó közönséggel. Az ábrázolt korosztállyal pedig elhiteti, hogy bizonyos magatartások magától értetődőek, az élet, a szexualitás természetes velejárói. E megfontolások miatt a gyermekeket ábrázoló pornográf felvételek birtoklása és továbbadása az Európai Unió tagállamaiban büntetendő magatartások.[1]

Minél kisebb kárt okozna a tartalommal való szembesülés a felhasználó oldalán, illetve minél távolabbi az ok-okozati láncolat az elszenvedett kár és az adott tartalommal való szembesülés között, annál kevésbé indokolt a tartalom blokkolása.

Németországban 2009. május 5-én látott napvilágot a kommunikációs hálózatokon továbbított gyermekpornográf felvételek internet-szolgáltatók általi szűrésére[2] vonatkozó törvényjavaslat.[3] A javaslat szerint a Német Bűnügyi Hivatalnak (*Bundeskriminalamt*, a továbbiakban BKA) listát kell vezetnie az olyan FQDN-ekről,[4] IP-címekről, és multimédiás anyagok elérési útvonalairól, amelyek a német büntető törvénykönyv (StGB § 184b) értelmében gyermekpornográfiát tartalmaznak, vagy amelyek ilyen tartalmakra mutatnak, hivatkoznak. A törvény értelmében a BKA a törvény hatálya alá tartozó nagyobb internet-szolgáltatóknak minden munkanap aktualizált blokkolási listát bocsát rendelkezésére. Az üzemszerűen legalább 10.000 felhasználónak szolgáltatást nyújtó hozzáférés-szolgáltatók (access provider) 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 domainek 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 2009. június 18-i ülésén elfogadta. A törvény 2010 februárjától hatályos, azonban nem végrehajtható, mivel az új politikai irányvonal liberálisabb elképzelések mentén új törvényjavaslatot kíván kidolgozni. A törvényt ért támadásoknak az alapja az, hogy hatékonysága nem kielégítő, miközben aránytalanul beavatkozik az alapvető állampolgári jogok gyakorlásába, továbbá nem kíméli az internet-szolgáltatók jogosultságait sem.

A blokkolás fajtái – csoportosítás

A továbbiakban a blokkolás különböző technikai megoldásait mutatom be, és vázolom a velük kapcsolatban felmerült aggályokat.

Az internetes illegális és káros tartalmak szűrésére már jó 20 éve vannak kísérletek. Elsőként a kéretlen elektronikus reklám, a spam kiszűrésére születtek megoldások, hogy a levélszemét nehogy lelassítsa az internet-kapcsolatot. Ezeket a megoldásokat a felhasználók önállóan, valamint a szolgáltatók alkalmazták, felhasználóik védelmében. A nem kívánt tartalom blokkolásának igénye azonban idővel ennél magasabb szinteken is megjelent. A blokkolás a következő szinteken valósulhat meg:

a) felhasználói szinten (tűzfal, kéretlen levél-szűrő az internetelérés sebességének biztosítására, a vírusok, férgek kiszűrésére);

b) szolgáltatói szinten (amikor a host, azaz a szervergazda telepíti a tűzfalat vagy a levélszemét-szűrőt a szerverre, így a fent említett szűrő a felhasználónál eggyel magasabb szintre kerül. Ilyen, szolgáltatói szintű védelem a keresőmotorok biztonságos böngészést lehetővé tevő alkalmazása, a *safe search* is);

c) intézményi szinten (amikor pl. a munkáltató infrastruktúrája védelme érdekében veszi igénybe ezeket a szűrőket, de ilyen az is, amikor valamely iskola vagy könyvtár telepít káros tartalmak elleni szűrőszoftvert nevelési célzattal);

d) kormányszinten (amikor valamely kormány központi szinten kívánja kiszűrni az illegális és/vagy a politikailag káros tartalmakat, amelyhez együttműködésre kötelezi az internet hozzáférés-szolgáltatókat, továbbá a keresőmotor-szolgáltatókat).

Szűrés alapvetően két szinten valósulhat meg, a felhasználó szintjén (*personal* vagy *individual filtering*), vagy intézményi (szolgáltatói, szervezeti, kormányzati) szinten *(network blocking)*.

Mint látható, nemcsak a védekezési szintek különbözőek, de a védelmi megfontolások, célok is. Ezzel együtt az igénybevett infrastruktúra, illetve a technikai felszerelés is változatos. Összefoglalva a fentieket, a szűrés alapvetően két szinten valósulhat meg:

a) a felhasználó szintjén (*personal* vagy *individual filtering*), vagy

b) intézményi (szolgáltatói, szervezeti, kormányzati) szinten (*network blocking*).

Vannak olyan országok, amelyek a kétfajta szűrést együttesen alkalmazzák (hibrid-szűrés).

A szűrés szintje meghatározza, kinek a kezében van a döntés arról, hogy milyen tartalmat kell nem kívánatosnak tekinteni. 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.

A szerző az Országos Kriminológiai Intézet tudományos munkatársa.

A kormányzati, azaz a legmagasabb szintű filterezési technikák alapvetően két csoportra oszthatók.

a) Az egyikbe azok az országok tartoznak, amelyek az internet-szolgáltatókat (*access provider*) kötelezik a feltöltött tartalmak szűrésére, meghatározott szempontok szerint. E szempontok alapján a kormányok általában „blokkolási listákat" hoznak létre.

b) A másik csoportba azok az országok tartoznak, amelyek a filterező infrastruktúrát az országba beérkező internet-gerinchálózatba építik be, ezzel megakadályozva, hogy kintről bármilyen illegális tartalom bejusson az országba. (Tous, 2009)[5] Ezt a megoldást azok az országok alkalmazzák, ahol a teljes telekommunikáció szabályozása, kiépítése és üzemeltetése állami monopólium és így kezdettől fogva természetes az újabb médium cenzúrázása is. (Callanan et al., 2009: 11-20)[6]

Technikai kistéka

IP-alapú szűrés

Az IP-alapú szűrés azt jelenti, hogy a kiválasztott IP-címek elérését blokkolják. A legegyszerűbb módja a nem kívánt tartalmak szűrésének, nem igényel különösebb anyagi ráfordítást. Mivel ilyen egyszerű, általában ezt a módszert alkalmazzák először. (Callanan et al., 2009) A baj ezzel, hogy nem képes finom szűrésre, például nem képes valamely weboldal tartalmát részlegesen letiltani. Ugyanígy, ha több weboldalt működtet egy IP, akkor a tiltás minden, hozzá tartozó weboldalt elérhetetlenné tesz. Ugyanakkor kevésbé effektív az olyan weboldalakkal szemben, amelyek több különböző IP-címet használnak a tartalom továbbítására, vagy amelyek találomra választanak IP-címet a tartalom továbbításához. Ezt a technikát, egyszerűsége és tökéletlensége ellenére rendszeresen alkalmazzák cégek, internet-szolgáltatók vírusok, kártékony szoftverek és spam-ek ellen, illetve kormányok az illegális weboldalak elérésének megakadályozására. Persze a technológia kijátszható, mégpedig un. *web proxy* segítségével, azaz ha a szolgáltatók külföldi szerveren keresztül érik el a kívánt weboldalt és juttatják el azt a felhasználókhoz. Erre a célra minden olyan proxy felhasználható, amelynek IP-címét nem blokkolták.[7]

DNS-alapú szűrés

A DNS-alapú szűrés az IP-alapú továbbfejlesztett változata, a domain név szerverre (DNS) telepített szűrési technika. A DNS-t úgy állítják be, hogy bizonyos domaineket ne „ismerjen fel", azaz ne fejthessen vissza nominálissá. Amennyiben pedig nincs meg, hogy a keresett domaint melyik host tárolja, úgy a felhasználó nem is tudja lehívni az adott domaint. A DNS-alapú szűrés finomabb hangolást tesz lehetővé az IP-alapúnál, ami azokban az esetekben elvárt, amikor egy IP-címhez több domain tartozik, de csak egyet kell letiltatni.

A DNS-alapú szűrés is megkerülhető: a keresett domain IP-címe lekérdezhető az interneten.[8] Az így megszerzett IP-címet ezek után a domainekhez tartozó IP-címek listájába kell menteni a számítógépen. Ha a gép itt megtalálja valamely domain IP-címét, akkor a keresett weboldalt a domain helyett a megadott IP-cím segítségével hívja be.[9]

Domain-alapú szűrés

A domain-alapú is viszonylag szenzitív szűrést tesz lehetővé. Mind a DNS-alapú, mind a domain-szűrés gyengesége, hogy csak teljes domainek blokkolására alkalmasak, és nem képesek az azonos domain alá vett tartalmak megkülönböztetésére. A DNS-szűréssel szemben a domain-alapúnál nem magát a DNS-t állítják be úgy, hogy ne ismerjen fel bizonyos domaineket, hanem a DNS által *már felismert* domaineket a szolgáltató egyéni beállításai miatt nem képes elérni a felhasználó. Az új *német* törvény ezt a technológiát hívta volna segítségül a blokkoláshoz, azaz az internet-szolgáltatóknak (*access provider*) hozzáférhetetlenné kellett volna tenniük a blokkolási feketelistában szereplő domain neveket. Más országok, mint *Ausztrália*, az *Egyesült Királyság* vagy *Norvégia* szintén ezt a megoldást alkalmazzák.[10] Ha a felhasználó lehív egy tiltott domainhez tartozó IP-címet, akkor a szolgáltató szervere egy statikus weboldalt küld a felhasználónak azzal az üzenettel, hogy a lehívni kívánt oldalon illegális tartalom található. Ám ez a technika is megkerülhető, mégpedig a legegyszerűbben proxy segítségével.[11] Ha pedig a szűrést úgy hangolják, hogy a proxyval való kommunikáció tartalmában is szűrje az adott domaineket, akkor titkosított adatcsatorna (SSl, azaz *Secure Socket Layer*,[12] vagy VPN, azaz *Virtual Private Network*, virtuális magánhálózat)[13] technológia segítségével mindenképpen megkerülhető.

URL-alapú szűrés

Az URL-alapú szűrés az IP-, a DNS- és a domain-alapúnál is fejlettebb technológia, hiszen az előzőeknél finomabb szűrésre alkalmas. Technikailag ez úgy néz ki, hogy egy web proxyt iktatnak közbe az internet *access provider* és a felhasználók közé, amely semmiféle olyan tartalmat nem enged át, amely a letiltott URL-ekhez tartozik. Mivel ez megoldható egyetlen web proxyval is, ezért könnyű szabályokat alkotni (a szabály vonatkozhat egy adott domainre, weboldalra vagy akár paraméterre),[14] amelyek minden felhasználót kötnek, aki az adott web proxyn keresztül éri el az internetet. Például az URL-alapú szűrésnél lehetséges a Google vagy más keresőmotor által kiadott találatok szűrése feketelistás kulcsszavak megadása alapján. Számos kereskedelmi alkalmazás épít e módszerre: céges profilra lehet alakítani vagy kormányzati szűrésre is alkalmazzák. Hátránya, hogy nagyon nagy mennyiségű információt kell szűrni, amely lelassíthatja a felhasználók internet-használatát (*bottleneck effect*). Az URL-alapú blokkolás egyszerűen megkerülhető open proxy szerverek[15] használatával, vagy bármiféle olyan szerver közbeiktatásával, amely alkalmas a weboldalak tárolására (pl. a Google *cache* – Google gyorsítótár, vagy a Google *translate* – a Google fordítófunkciója).

Kulcsszavas blokkolás

Az előbb bemutatott blokkolási módszerek masszív feketelistás gyűjtéseken alapulnak, amelyet emberek állítanak össze és folyamatosan frissítenek. Éppen ezért nemcsak, hogy rengeteg erőfeszítés van mögöttük, de képtelenség ilyen módon kiszűrni valamennyi illegális tartalmat, tekintve, hogy milyen gyorsan és egyszerűen lehet új tartalmakat feltölteni az internetre. Az illegális tartalmak legpontosabb szűrésére a kulcsszavas a legalkalmasabb, bár ez hatalmas erőfeszítést követel. A kulcsszavas szűrést mélyzseb-szűrésnek (*deep packet inspection*) is nevezzük, mert nem az elküldött üzenet fejléce (*header*) alapján szűr, amelyben csak a felhasználó által lehívandó IP-címek vannak feltüntetve, hanem beletekint magának az üzenetnek a tartalmába (*content*), és a megadott kulcsszavakat tartalmazó URL-eket tartja vissza. Ezzel a módszerrel azonban valószínűleg több adatot blokkolunk mint kellene, pl. azokat az ismeretterjesztő vagy tudományos (reproduktív biológiai) tartalmakat is, amelyek pornográfiára utaló szavakat tartalmazhatnak. Éppen ezért a kulcsszavas szűrés feketelistáit fehérlistákkal kell kiegészíteni, amelyek arra jók, hogy biztosítsák a legális tartalmak továbbélését. Hátránya amellett, hogy nagyon nagy emberi erőbefektetést és szervezést igényel, ezzel a módszerrel is lehetetlen minden illegális tartalmat kiszűrni. *Kína* ezt a megoldást is hadrendbe állította a netcenzúrához, más technikákkal vegyítve. Hogy gyorsabb legyen, automatikusan generált kulcsszavak alapján szűrik az offenzív tartalmakat. Természetesen ennek a módszernek a megkerülésére is vannak megoldások: a domain-alapú szűréshez hasonlóan, olyan kapcsolatot kell létesíteni (SSL vagy VPN) a végfelhasználó és a távoli szerver között, amely titkosítja a kettő között áramló tartalmat, ezáltal biztosítja érintetlenségét, hiszen a közbeékelt kulcsszókereső szerverek így nem képesek azonosítani a megadott kulcsszavakat.

Keresőmotoros-kulcsszavas blokkolás

A kulcsszavas és a keresőmotoros-kulcsszavas szűrés között csak a megvalósítás módjában van különbség, hiszen míg az előzőnél az *access provider* feladata a szűrés, addig az utóbbinál ez a keresőmotor tulajdonosának feladata. A keresőmotoros-kulcsszavas szűrésnél a kormány a keresőmotor-tulajdonossal köt szerződést arra, hogy a keresőmotor ne adjon ki olyan tartalmakat, amelyekben a megadott kulcsszavak szerepelnek. Megint csak a Kínában alkalmazott megoldásra lehet itt utalni: a kínai kormány többek között a Google-lel kötött szerződést arra, hogy bizonyos, károsnak vélt (pl. politikai) tartalmakat ne dobjon ki találatként. A Google azonban, rendszerének feltehetően kormányzati feltörése miatt megelégelte a politikai rendszer kívánalmainak tiszteletben tartását, és válaszul elérhetővé tett olyan politikai tartalmakat, amilyen például az 1989-es Tiananmen-téri mészárlás dokumentumai, teljes leírással és képekkel.[16]

A keresőmotoros-kulcsszavas szűrés előnye, hogy nem kell szervereket közbeiktatni, hiszen csupán a keresőmotorokat kell úgy beállítani, hogy ne adjanak ki bizonyos tartalmakat. Ennek a módszernek az előnye lehet a szű-

rő fél oldalán, hogy a felhasználókat attól függően lehet tévhitben tartani, hogy milyen üzenetet küld a keresőmotor neki. Így pl lehetséges, hogy a felhasználó nem is szerez tudomást arról, hogy bizonyos tartalmakat nem érhet el, hiszen azok a keresőmotor számára nem is léteznek. Ilyenkor a keresőmotor semmiféle üzenetet nem küld, egyszerűen nem hozza fel a keresett oldalt. Ez ellen leginkább a civil szervezetek tiltakoznak, hiszen a felhasználókat teljes sötétségben tartja magáról a cenzúra tényéről is. Más megoldást választott *Kína*, ahol a felhasználót kifejezetten félrevezetik: blokkolt tartalom esetében egy hibaüzenet jelenik meg a képernyőn *„the connection cannot be made"* vagy *„timeout exceeded"* felirattal.[17] Ez arra jó, nehogy a felhasználók kiskapukat keressenek a szűrő megkerülésére. De vannak olyan országok is, mint pl. *Szaud-Arábia*, amelyek tanító célzattal feltüntetik, hogy a tartalom illegális vagy káros, ezért nem lehet elérni, sőt, lehetőséget adnak arra is, hogy a felhasználó a hatósághoz forduljon a szűrés megszüntetése érdekében.[18] Ha a szűrési feltételeket nem ismertetik teljes körűen a felhasználókkal, ez a cenzúrával való visszaéléshez vezethet, így pl. ezen az alapon érte kritika a német vagy az olasz internet-blokkolási törvényt is, amelyek előírják, hogy a feketelisták titkosak legyenek.[19] A listák titkosságát a kormányok szerint az indokolja, hogy a blokkolandó tartalmak olyan súlyosan sértik a közerkölcsöt, illetve olyan súlyos bűncselekményt valósítanak meg, hogy csupán a tartalmakra mutató linkek elérése is megvalósíthatja a bűncselekményt. A *német* bírósági gyakorlat szerint az ilyen tartalmak közvetett, pl. hiperlink formájában való elérése is büntetendő.[20]

A választott módszert alapvetően a politikai berendezkedés befolyásolja

Totális állam – totális szűrés

A totális szűrést megvalósítani kívánó országok között is talán a legfényesebben ragyog a több blokkolási módszert is alkalmazó kínai aranypajzs, azaz a „nagy tűzfal" (*Golden Firewall*). Itt a telekommunikáció állami monopóliuma mellett az internet-szolgáltatóknak csak formális szerep jut: ők felelnek az infrastruktúra működtetéséért, amely feladatot szintén az állam delegálta rájuk. Emellett 2009-ben arra kötelezték a kereskedőket, hogy minden, kereskedelmi forgalomban kapható PC-t a zöld gátnak (*Green Dam*) nevezett szoftverrel együtt adjanak el, amely a gerinchálózaton elhelyezett szűrés otthoni kiegészítője lett volna.[21] A házi számítógépekre kifejlesztett, ám a kínai hatóságok elvárásainak megfelelően, szigorúbb kritériumok alapján szűrő szoftver célja megvédeni az otthon internetező gyermekeket az életkoruknak nem megfelelő tartalmaktól, ám ebbe nemcsak a szexuális, de a vallási és politikai tartalmak is beleesnek. A szoftver bevezetése egyelőre nem történt meg, mivel az soha nem tapasztalt tiltakozást váltott ki az internetezőkből, mondván, a szoftver nem segíti a szülőket, akiknek nincs jogosultságuk a beállítások megváltoztatására, egyéni meglátásaik szerint. A radikális netcenzúra országai Kína mellett még *Irán* és *Észak-Korea* is. Iránban például erősödnek azok a hangok, amelyek a természeti katasztrófákért, a földrengésekért és vulkánkitörésekért a női szexuális szabadosságot okolják, amely jelenség Nyugatról érkezik, és az internet és a műholdas televízió hatására terjed.[22]

A totális szűrést megvalósítani kívánó országok között is talán a legfényesebben ragyog a több blokkolási módszert is alkalmazó kínai aranypajzs, azaz a „nagy tűzfal" (*Golden Firewall*).

A „felnőtt" államok az individuális szűrést támogatják

Az *USA* kormányzati támogatást biztosít az oktatási intézmények és a könyvtárak számára, a szűrőprogramok telepítése érdekében. Ez a szabályozás annyiban liberálisabb, hogy a filter konfigurációja módosítható, így felnőtt látogatók esetén deaktiválható és a szűrési beállítások is változtathatók a helyi adminisztrátor által.[23] Az Egyesült Államokban ugyanakkor otthon mindenki maga döntheti el, mit enged be személyi számítógépére és mi ellen védekezik. Mivel az Egyesült Államokban a kormányszintű, centralizált egységes szabályozás alkotmányellenes (az alkotmány első kiegészítésébe, azaz a szólás- és véleménynyilvánítás szabadságába ütközik), ez lehetővé tette az egyéni felhasználói szintű védelem hatékonyabbá fejlesztését.

Ahol azonban nem ilyen erősek a szólás- és véleménynyilvánítás szabadságához fűződő jog lobby-érdekei, ott az intézményi szintű szűrési megoldásokat hamar felválthatják a hatékonyabbnak hitt kormányzati szintű, azaz központi szűrési technikák. *Ausztráliában* például eredetileg szintén otthoni szűrőprogramokat kínáltak a felhasználóknak, ám egyrészt nagyon kevesen éltek ezzel a lehetőséggel,[24] másrészt pedig a szűrők könnyen megkerülhetők voltak még akár egy gyermek által is – éppen akik védelmére tervezték azokat.[25] Vérszemet kaptak ezzel a kormányszintű szűrés bevezetői, akik minden előfizető számára eleve cenzúrázott, illegális tartalmaktól megtisztított internetkapcsolatot akartak bevezetni opt-out megoldással, azaz a felhasználónak kifejezetten kérnie kellett volna a szolgáltatótól a cenzúrázatlan internet-hozzáférést. A jelenlegi álláspont inkább a liberálisabb, opt-in megoldást részesítené előnyben.[26]

Ahol nem elég erősek a szólás- és véleménynyilvánítás szabadságához fűződő jog lobby-érdekei, ott az intézményi szintű szűrési megoldásokat hamar felválthatják a hatékonyabbnak hitt kormányzati szintű, azaz központi szűrési technikák.

Átmeneti országok – ahol az egyensúly a védelem oldalára billen

A demokratikus államok és az autoriter megközelítés között a legfontosabb az ideológiai különbség: míg az autoriter államok erőforrástól függően, minden illegális és az állampolgárokra nézve káros tartalmakat blokkolnak, addig a demokráciák általában csak a legsúlyosabb bűncselekmények, így leggyakrabban a gyermekpornográfia online terjesztésének akadályozására tesznek kísérletet a tartalom központi blokkolásával. Az utóbbi időben azonban az autoriter és a demokratikus megfontolások lassú közeledésének lehetünk tanúi, mivel az állampolgári biztonság és az állami büntetőjogi igény érvényesítése érdekében a tartalmak egyre szélesebb körét blokkolják a demokratikus berendezkedésű államokban is.

Erre jó példa az önpusztító tartalmak elleni központi védekezés. *Kanadában* például 2009 óta blokkoltatja a kormány az eutanázia-népszerűsítő és étkezési rendellenességekkel foglalkozó weboldalakat és az önveszélyes tartalmak blokkolását sürgető tárgyalások kezdődtek *Ausztráliában* is. (Wykes, 2010: 375)[27]

Az *Egyesült Királyságban* 2008-ban kezdtek arról tárgyalni, hogy minden brit állampolgár e-mail forgalmát és internetes aktivitását monitorozni kellene a terrortámadások elkerülése végett.[28] (hivatkozik rá Wykes, 2010: 375) Ugyanitt a kormány megbízta az internet-szolgáltatókat, hogy távolítsák el az öngyilkosságot előmozdító (elősegítő) weboldalakat és ezzel egyidőben értesítsék a nyomozó hatóságot a veszélyes tartalomról.[29] (hivatkozik rá Wykes, 2010: 380) Ha az internet-szolgáltatók nem vezetik be az öncenzúrát, akkor öngyilkosságban közreműködés bűncselekménye miatt büntetőeljárás indítható ellenük. Kutatások szerint azonban, az internet megjelenésével nemhogy megnőtt volna, de csökkent az öngyilkosságok száma (különösen a média által legbefolyásolhatóbb réteg, a tinédzserek között), hiszen az ilyen weboldalak arra is jók, hogy az előkészülete részleteit online közzétevőt lebeszéljék az öngyilkosságról. Az internet tehát nem növelte a veszélyt, csak láthatóvá tette az önveszélyes cselekmények előkészületeit. Emiatt az internetre inkább a megelőzés eszközeként kellene tekinteni, mintsem a veszélyes, tiltandó médiumként.

Minden módszer végrehajtásának egyedi előnyei és hátrányai vannak mind a megvalósító, mind az érintett hozzáférés-szolgáltató, mind a tartalomszolgáltatók, mind pedig az internet-felhasználók számára.

A bemutatott különböző blokkolási technikák egymással semmiféle hierarchikus vagy fokozatossági viszonyban nem állnak. Minden módszer végrehajtásának egyedi előnyei és hátrányai vannak mind a megvalósító, mind az érintett hozzáférés-szolgáltató, mind a tartalomszolgáltatók, mind pedig az internet-felhasználók számára, amelyet az alábbi táblázat foglal össze. (1. ábra: A táblázat nemcsak a kormányok által használt, webes és keresőmotoros alapú szűrési technikákat tartalmazza, hanem a teljesség kedvéért a céges alapú szűrési variációkat is.)[30]

1. ábra *Az egyes tartalomszűrési megoldások hatására mennyire és hogyan sérülnek az alkotmányos jogok?*[31]

Szűrt médium	Szűrés típusa	Jog típusa			Hatékonyság (ALUL-SZŰRÉS)	Példa országra, ahol az adott szűrést alkalmazzák	Példa a módszer megkerülésére
		A felhasználók információhoz jutási szabadsága (TÚL-BLOKKOLÁS)	A tartalom-szolgáltatók vélemény-nyilvánítási szabadsága	Az internet-szolgáltatók üzleti szabadsága és tulajdonhoz való joga (az internet-szolgáltatóktól mennyi befektetést igényel)			
WEB	DNS	Nagyon valószínű, hogy sérül	Nagyon valószínű, hogy sérül	Nem sérül	Alulszűrés valószínű	Kína	A domain IP-címe lekérdezhető az interneten. Az így megszerzett IP-címet a domainekhez tartozó IP-címek listájába kell menteni a számítógépen. Ha a gép itt megtalálja valamely domain IP-címét, akkor a keresett weboldalt a megadott IP-cím segítségével hívja be.
	Domain	Nagyon valószínű, hogy sérül	Nagyon valószínű, hogy sérül	Közepesen sérül	Alulszűrés valószínű	Németországban hatályos (2009), de nem alkalmazzák, Ausztrália, UK, Norvégia. Ezt a megoldást cégek arra használják, hogy ne lehessen olyan nagy sávszélességet igénylő weboldalakat elérni, amelyek rontanák az internet-elérés sebességét (pl. pornográf weboldal, youtube stb.).	Titkosított adatcsatorna (SSl vagy VPN) vagy open proxy szerver használatával
	URL	Kevésbé valószínű	Kevésbé valószínű	Közepesen sérül	Alulszűrés nagyon valószínű	Kína	SSl vagy VPN, vagy open proxy szerver közbeiktatásával, amely alkalmas a weboldalak tárolására, pl. Google cache, Google translate
	IP	Nagyon valószínű, hogy sérül	Nagyon valószínű, hogy sérül	Nem sérül	Alulszűrés valószínű	Kína	Erre a célra minden olyan web proxy felhasználható, amelynek IP-címét nem blokkolták.
KERESŐ-MOTOR	kulcsszavas	Nagyon valószínű, hogy sérül	Nagyon valószínű, hogy sérül	Nagy mértékben sérül	Alulszűrés nagyon valószínű	Kína, Szaúd-Arábia, Észak-Korea	Olyan – általában kevés felhasználót számláló, kevésbé népszerű – keresőmotort kell használni, amire nem vonatkozik a szűrés.

A német törvény

1. A blokkolás mint „szemfedő"

Az illegális tartalmak elleni küzdelem akkor lehet sikeres, ha a tartalmat a host szervereken *törlik*. Ezt a forródrótok (*hotline*-ok)[32] rendszere mozdítja elő, amely jogellenes tartalmakról fogad bejelentéseket. A forródrótok a szolgáltatóknak notice-and-take-down felszólítást küldenek, amire a szolgáltatónak el kell távolítania szerveréről az illegális tartalmat. Ha azonban ez az eljárás nem vezet eredményre, úgy az eltávolítás – és a büntetőeljárás céljára való megőrzés – céljára jogsegély-egyezményeket lehet csak alkalmazni, amelyek azonban ilyen esetekben lassúak és nehézkesek. A jogérvényesítés e problémái arra vezették a jogalkotókat, hogy az illegális tartalmak – és ezen belül különösen a gyermekpornográfia – letöltését saját államuk területén próbálják megakadályozni. Az elérés megnehezítésének eszköze általá-

ban az illegális tartalmak blokkolása, amely nem egyenlő a törlési, azaz a *notice-and-take-down* eljárással. Az illegális tartalmak a blokkolással továbbra is elérhetők lesznek, a blokkok műszaki megkerülése által.

A német törvény domain-manipulációval képzeli el a gyermekpornográf tartalmak elleni megfelelő védelmet. Ez jogpolitikai szempontból kifogásolható, hiszen azt az illúziót kelti, mintha leszámoltak volna a jelenséggel, holott a blokkolt tartalmak csak a törvény által meghatározott kritériumoknak megfelelő nemzeti szerverekre csatlakozva lettek láthatatlanok, máshonnan szabadon elérhetők. A blokkolás kiválóan alkalmas a gyermekpornográfia elleni küzdelem kipipálására, amelynek azonban koránt sincs vége azzal, hogy az államok a blokkolással „láthatatlanná" teszik az illegális tartalmakat, hiszen azok továbbra is a világhálón maradnak, csupán az adott országban található nagyobb internet-szolgáltatók szerverére csatlakozva lesznek láthatatlanok.

2. A gyermekvédelmi cél megbicsaklik

A törvény célja a gyermekpornográfia elleni küzdelem hatékonyabbá tétele. Egyfelől hogy megóvja az ábrázolt gyermekeket az akár ismételt traumától, másfelől hogy az ábrázolások terjedésének megakadályozásával visszaszorítsa a gyermekpornográf felvételek iránti keresletet, harmadsorban pedig biztosítsa, hogy sem a gyermekkorú, sem pedig a felnőtt internethasználók ne szembesüljenek kéretlenül online gyermekpornográfiával.

A törvény elsődleges, gyermekvédelmi célja ott bicsaklik meg, hogy kizárólag a világhálón fellelhető gyermekpornográf tartalmak elleni küzdelmet tűzi ki célul. Szem elől téveszti, hogy az ilyen tartalmak lelőhelye mára már nem elsősorban a világháló, hanem zárt láncú levelezőrendszerek, hírcsoportok, P2P cserebörzék és chatszobák is. A kereslet-kínálat ilyen irányú, rejtőzködő „elmozdulását" éppen az utóbbi évek sikeres nemzetközi bűnüldözési akciói motiválták. A gyermekpornográf felvételek készítői és terjesztői a világháló nyitott kommunikációjából a biztonságosabb háttérbe húzódtak.[33]

A törvény elsődleges, gyermekvédelmi célja ott bicsaklik meg, hogy kizárólag a világhálón fellelhető gyermekpornográf tartalmak elleni küzdelmet tűzi ki célul. Szem elől téveszti, hogy az ilyen tartalmak lelőhelye mára már nem elsősorban a világháló, hanem zárt láncú levelezőrendszerek, hírcsoportok, P2P cserebörzék és chatszobák is.

3. Alulszűrés és túlblokkolás egyidőben

A feketelistán alapuló blokkolási módszerek – amikor a kijelölt szerv által összeállított listán szereplő weboldalakat kell elérhetetlenné tenni – bizonyos esetekben alul-, másokban túlszűrnek. A blokkolás gyakran káros mellékhatásokkal is jár: az egyszerű letiltási módszerek (mint a német megoldás, a domainek DNS-szintű manipulációja) gyakran nem túl hatékonyak, mivel nem különíthetők el egyértelműen az azonos domain névhez tartozó illegális és legális tartalmak. Ugyanezen okból gyakran túlszűrnek: gyakran legális tartalmakat vagy hivatkozott legális weboldalakat is blokkolnak a felhasználók elől.

Az alulszűrés hatására továbbra is elérhetők az illegális tartalmak, a túlblokkolás viszont sérti a felhasználók információhoz jutási szabadságát. Nem beszélve arról, hogy a szexuális tartalmú weboldalak letiltásával a fiatal korosztályhoz sem jut el a megfelelő oktatási segédanyag.

A német megoldás kuriózuma, hogy csak a nagyobb (a több mint 10.000 felhasználót kiszolgáló) német hozzáférés-szolgáltatókon keresztül elérhető tartalmakra vonatkozik, így aki kisebb vagy külföldi szolgáltatókon keresztül éri el az internetet, az továbbra is hozzáfér az illegális tartalmakhoz is.[34] Ez az „opt-out" – azaz könnyen megkerülhető – megoldás nem sokkal hatékonyabb, mint a felhasználóalapú szűrés, azaz amikor a felhasználó telepít saját gépére szűrőszoftvert és azon saját beállításokat alkalmaz.

4. Sérül a szükségességi-arányossági elv

A blokkolás hatékonysága nem arányos az alkotmányos és emberi jogokba való beavatkozás mértékével – a blokkolással ugyanis az információhoz jutás és a véleménynyilvánítás szabadsága sérül, miközben nem biztosítja a megfelelő védelmet a sértetteknek és a felhasználóknak.

A domain-alapú blokkolás német bevezetésének az egyik hasznos hozadékaként emlegetik, hogy ilyen módon a felhasználók webes böngészései is nyomon követhetők, ami pedig lehetőséget ad a gyermekpornográfia iránt érdeklődők ellen büntetőeljárás indítására. A koncepció lényege az, hogy mivel a letiltott domainek mind gyermekpornográf tartalomra mutatnak, így azok ellen, akik csupán megpróbálják kijátszani a blokkot – pl. más szolgáltatóhoz csatlakoznak –, automatikusan büntetőeljárás indítható lenne. A blokk megkerülése ugyanis igazolná a megszerzés előkészületének (elkövetési magatartás) szándékosságát. (Sieber, 2009: 657)[35] Ezzel az érveléssel három probléma adódik:

1) Mindenkinek joga van megválasztani az általa használni kívánt szolgáltatást, így a szolgáltatót is, és ha ez éppen nem tartozik a nagyobb belföldi szolgáltatók közé, akkor cenzúrázatlan tartalomhoz fog hozzájutni a szolgáltatással. Ha valamely felhasználó nem a nagyobb belföldi szolgáltatókon keresztül éri el az internetet, ez még nem jelenti egyúttal, hogy a célja gyermekpornográf tartalmak letöltése.

2) A szólás- és véleménynyilvánítás szabadsága jegyében mindenkinek joga van elérni olyan tartalmakat is, amelyeket az alkalmazott technikai megoldás a gyermekpornográfiával együtt blokkol, azaz mindenkinek joga van az akaratlanul túlszűrt információ megismeréséhez.

3) Nem lenne meglepő, hogy éppen az alaptalan vádaskodások elkerülése érdekében olyan szolgáltatót vennének igénybe a felhasználók, amelyre nem vonatkoznak a szűrési szabályok, hiszen szeretnék még a látszatát is elkerülni annak, hogy blokkolt domainek véletlen behívási kísérletével magukra vonják a hatóság figyelmét.

Németországban a blokkolásra alkalmazott technika csak a webet szűrné, figyelmen kívül hagyná a gyermekpornográfia olyan megjelenési fórumait, amilyenek például a P2P hálózatok, chatszobák, vagy hírcsoportok. Ugyanakkor nem állnak rendelkezésre kutatások arra nézve, 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.[36]

Az elérni kívánt céllal azért sem arányos az alkalmazott technológia és a rá épített koncepció, mert tökéletlen, mert (valószínűleg) drasztikusabban avatkozik be az állampolgárok alapvető szabadságjogaiba, mint amilyen sérülést a megelőzni kívánt magatartás okozna, továbbá mert a védelmet ezzel elintézettnek tekinti és nem foglalkozik a felhasználói szintű védekezés stratégiájával.

5. Sérül a tisztességes eljáráshoz való jog

A tisztességes eljárás alkotmányos joga sérül azzal, hogy bírói jóváhagyás nélkül lehet összeállítani és frissíteni a blokkolási listát, hiszen nincs olyan független testület, amely felülbírálná a nyomozó hatóság döntését. Amellett, hogy óriási erőfeszítés lenne a BKA-nak egyetlen hatóságként folyamatosan megújítani és alkalmazni a listát, nem is célszerű kihagyni a bíróságot mint független kontrollfunkciót a lista frissítéséből.

A feketelistás domainek automatikus blokkolása egyfelől nem ad lehetőséget a tartalom közzétevőjének arra, hogy levegye a gyermekpornográfnak minősített tartalmat. Másfelől pedig a jogtudatosság sem fejlődik, hiszen a tartalomgazda továbbra sem fogja tudni, mit nem tehet közzé a jövőben.

Hogy a gyermekpornográfia meghatározása mennyire változó, azt mutatja a következő akció is. Egy felhasználó 2009 májusában összesen 348 olyan szolgáltatónak írt, akiknek tartalmai a nyilvánosságra hozott különböző európai blokkolási listákon szerepeltek. Az e-mail elküldését követő 12 órán belül 10 szolgáltató törölt mintegy 60 felvételt, 250 szolgáltató viszont azt válaszolta, hogy az ellenőrzés során csak legális tartalmakat találtak.[37] Ez tehát azt mutatja, hogy valószínűleg rengeteg vitás megítélésű tartalom van, amelyet nem érhetnek el a felhasználók a blokkolás révén. Ugyanakkor a blokkolás az illegális tartalmakat nem törli, amelyek továbbra is elérhetők maradnak. Ezen okok miatt érdemes lenne a blokkolást obligatóriusból szubszidiáriussá alakítani, amelynek keretében először felhívnák a tartalomszolgáltatót az illegális anyag törlésére. A törlési eljárás során a tartalomgazda kifogást emelhetne a törlési felhívás ellen, ami pedig biztosítaná a tisztességes eljáráshoz fűződő jogát.

6. Sérül a tartalomszolgáltató véleménynyilvánítási szabadsága

A bíróság közbeiktatásával a törvény számos más hibája is kiküszöbölhető lenne. Hogyha például nem automatikusan blokkolnák az illegális tartal-

makat, hanem először felhívnák a tartalomgazdát az eltávolítására, a tartalomgazda közigazgatási eljárás keretében előadhatná a tartalom jogszerűségével kapcsolatos kifogásait.

A német feketelistás blokkolási megoldás nem ad lehetőséget arra, hogy a tartalom szolgáltatója maga távolítsa el az illegális tartalmat (tisztességes eljáráshoz való jog), ezzel megakadályozza, hogy az állampolgárok megtudják, mi az illegális és mi a legális tartalom, így esélyük sincs arra, hogy jogkövetően cselekedjenek, továbbá nem teljesül a jogszabályok átláthatóságának követelménye sem.

Az internet szűrése nemcsak az illegális tartalmak feltöltőit akadályozza a terjesztésben, hanem a felhasználók számára is lehetetlenné teszi az illegális tartalmak elérését. Felmerülhet a kérdés, miért van szükség a hozzáférés-szolgáltató szintjén, központilag szabályozott kényszer-blokkolásra, ha felhasználói szinten léteznek már védekezési, szűrési, illetve bejelentési lehetőségek. Az új német kormány ezt a logikát követve a túlszűrés elkerülése végett és az állampolgári szabadság tiszteletben tartása jegyében inkább korosztály-címkézési rendszert vezetne be, amelynek alapján a szülők dönthetnék el, milyen tartalmakhoz férjen hozzá a gyerek.[38]

Fontos megérteni, hogy a tartalomszolgáltatók véleményszabadsága és a felhasználók információszabadsága nem az illegális tartalmak blokkolása miatt sérül, hanem mert a domain-alapú blokkolás legális tartalmakat és olyan funkciók használatát is ellehetetlenítheti, mint a levelezés (vagy pl. az IGroups szolgáltatások). A blokkolási listák folyamatos bővülésével párhuzamosan pedig mind több legális tartalom és internet-funkciók is elveszhet.

7. Nem fejlődik a jogtudatosság

A központi, állami szintű blokkolás feketelistáit általában titokban kell tartani. Ez a helyzet a dán, a finn és a német blokkolási feketelistákkal is. A titkosítás egyebek mellett azon a megfontoláson alapul, hogy így a bűnüldözés nagyobb sikerrel göngyölítheti fel az ügyeket, mivel a listában szereplő oldalak tartalomgazdái, ha nincs tudomásuk a büntetőeljárásról, nem törlik, tehát nem semmisítik meg a bizonyítékot. A bűnüldözés hatékonyságának indoka azonban nem elégséges a tisztességes eljárás követelményével szemben.

Egyfelől, a német törvény alapján a hozzáférés-szolgáltató eleve „stop-üzenetet" küld a tartalom közzétevőjének, mihelyt értesült arról, hogy az adott domain szerepel a feketelistán. A büntetőeljárás megindulásáról tehát a tartalomgazda még azelőtt értesül, hogy gyanúsítottként kihallgatnák. A titkosítást tehát kriminalisztikai érdekek nem indokolhatják.

Másfelől, a német törvény alapján a feketelistát a BKA állítja össze, tehát a blokkolási döntéseket egy rendőrhatóság hozza meg, nem pedig egy személyében független bíró. A német alkotmánybíróság abból indul ki, hogy az érintettek jogainak sértetlenségét a személyes és tárgyi függetlenségük miatt leginkább a bíróság képes biztosítani.[39] A feketelistát tehát egy független bírónak, illetve bírói testületnek kellene elkészítenie, de legalábbis jóváhagynia. (A bírói jóváhagyás kompenzálhatná az elmaradó törlési/eltávolítási felszólítást is.)

Ezzel kapcsolatban felmerülhet az a probléma, hogy egy bíró nem képes napi aktualitással ellenőrizni a feketelista tartalmát, különösen ha egy olyan proliferáló jelenségről van szó, mint amilyen a gyermekpornográfia. Hiszen a gyermekpornográf tartalmak tömegesen vannak jelen az interneten és gyorsan cserélődnek, illetve egészülnek ki újabb tartalmakkal, így már maga az ellenőrzés is jelentős erőfeszítést igényel. E probléma kiküszöbölésére alkalmas lenne a blokkolási módszer notice-and-take-down módszerré alakítása, amelynek során a hozzáférés-szolgáltató felhívná a tartalomszolgáltatót az illegális tartalom eltávolítására, azaz törlésére.

A tartalomszolgáltatók (felhasználók, állampolgárok) egyébként is tisztában kell 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 – nemcsak átláthatóbbá tenné az eljárást, hanem a bíróságot is tehermentesítené: a bíróságnak csak azokat az eseteket kellene vizsgálnia, amelyekben a tartalomszolgáltató kifogást emelt a tartalom eltávolítására irányuló felhívás ellen.

A fent leírt javaslatok nemcsak a jogszabályok átláthatóságát biztosítanák, hanem erősíthetik az állampolgári önkéntességet és altruizmust, amely az internet szabályozásának alapja. Az internetet nem lehetséges „kívülről", egy külső entitás által szabályozni. Hálózata decentralizált, tartalmát a felhasználók alakítják. Éppen ezért csak a felhasználók közössége tehet az internet tartalmának „tisztasága", jogszerűsége érdekében. Ehhez viszont szükséges, hogy a felhasználók értesülhessenek arról, ha az általuk kommunikált tartalom illegális. Ezen az elven működnek az illegális és káros tartalmak bejelentésére szolgáló forródrótok, amelyekre az állampolgárok bejelentéseket tehetnek.

8. Nem tisztázott, mi a szolgáltató kötelezettsége és felelőssége

Nem derül ki, mi a szolgáltató kötelessége, hiszen a törvény a domainek „minimális" blokkolását írja elő a szolgáltatók számára. Hogy ezen felül milyen kötelesség terheli a szolgáltatót a blokkolással kapcsolatban, azt a német törvény nem tárgyalja.

A blokkolás technikai kivitelezésétől függően sérti a blokkolási folyamatban részt vevő internet-szolgáltatók üzleti élethez fűződő szabadságát és tulajdonjogait. Az együttműködésre kötelezett szolgáltató az együttműködést kisebb-nagyobb anyagi és infrastrukturális befektetésekkel képes abszolválni. Másfelől pedig az internet-hozzáférés szolgáltatása és a szabad információáramlás blokkolása egymással szembemenő tevékenységek – az internet-szolgáltató profiljától az utóbbi idegen.

A német multimédiás törvény (TMG § 8a) szerint, ha az internet-szolgáltató előírásszerűen valósította meg a blokkolást, akkor az átengedett illegális tartalmak tekintetében mentesül a felelősség alól. Csakhogy a törvény nem részletezi, milyen lépéseket tegyen a szolgáltató a megfelelően megtett, de eredmény nélkül maradt blokkolást követően. Nem tisztázott, hogy elveszti-e a szolgáltató felelősség alóli mentességét, ha olyan további blokkolási intézkedéseket tesz, amelyek továbbra sem vezetnek eredményre.

Emellett az sem világos, hogy az információszolgáltatók élhetnek-e az állammal szemben kártérítési igénnyel legális tartalom járulékos blokkolása esetén. A törvényhozó abban sem bízhat, hogy az illegális tartalmak gazdái gyermekpornográf anyagaikat majd külön domaineken helyezik el, a legálistól való könnyebb megkülönböztetésük érdekében.

9. Nem tisztázott, ki a „tartalomgazda"

Ugyanígy nem derül ki, kit terhel a felelősség a közzétevő adatainak tárolásáért és átadásáért. A törvény kimondja, hogy a nagyobb német hozzáférés-szolgáltatók kötelesek megőrizni és átadni a közzétevő tartalomgazda adatait a BKA-nak.

A német telekommunikációs törvény (TKG § 8a. 5. bek.) előírja a hozzáférés-szolgáltatóknak, hogy a feketelistában szereplő domaineken illegális tartalmat közzétevő felhasználók adatait rögzítsék és azokat bűnüldözési célra adják át a nyomozó hatóságnak. Így azonban nemcsak a tartalmat közzétevők adatai, de a tartalmat *lekérdezők* IP-címei is megismerhetők a nyomozó hatóság által. Ezzel a szolgáltató egyfelől beavatkozik a felhasználók információkkal való szabad rendelkezési jogába, másfelől a feketelistás tartalmak lehívása a felhasználókra kompromittáló, a nyomozó hatóság számára pedig félrevezető lehet.

A feketelistán szereplő domainek alatt a felhasználók többféle – illegális és legális – tartalmat is közzétehetnek. Éppen ezért, ha valaki akár többször is megkísérelte elérni a feketelistás domaineket, az még nem jelenti automatikusan azt, hogy szándékosan az illegális tartalmakra volt kíváncsi, ám ezt sokszor nem lehet bizonyítani. Ilyen esetekben is megindulhat tehát a nyomozás, amikor a felhasználó által keresett, egyébként legális weboldal olyan illegális linket tartalmaz, amely szerepel a feketelistában. A behívott weboldalakon szereplő tartalom – az illegális linkkel együtt – megtalálható a felhasználó számítógépén, az automatikus letöltések között (a gyorsítótárban), amely szintén hamis nyom lehet.

Németországban ugyanakkor nincs kialakult joggyakorlat a linkek és a hiperlinkek megítélésével kapcsolatban. Hogy a linkek megítélése mennyire radikális lehet, azt a pforzheimi városi és a karlsruhei tartományi bíróság 2009-ben hozott döntései bizonyítják.[40] Ezekkel a döntésekkel házkutatást rendeltek el egy német tartalomszolgáltató ellen, aki honlapján a dán (szintén központi) blokkolás alapjául szolgáló feketelistára mutató linkeket helyezett el. Az már csak hab a tortán, hogy a linkek nem is közvetlenül, hanem számos weboldalon keresztül mutattak a dán feketelistára. Bár ilyen esetben kérdéses, hogy ennek relevanciája lehetne, hiszen általában az illegális tartalomra mutató linkek elnevezéséből sem lehet a valós tartalomra következtetni, így az is kérdéses, hogy az adott weboldal tulajdonosa szándékosan követte-e el a jogsértést.[41] A karlsruhei tartományi bíróság döntése kimondta, hogy bármilyen hosszú is a linkek láncolata, amely az adott illegális tarta-

lomra mutat, a link kihelyezése megalapozza a felelősséget. Indokolása szerint *„a világháló hálózatjellegű felépítése miatt, a conditio sine qua non elv értelmében, minden egyes link a kriminális tartalmak terjesztését szolgálja, akkor is, ha azok egyéb szolgáltatók linkjeinek láncolatán keresztül érhetők el."* A bíróság ezen az alapon azt is kimondhatta volna, hogy a teljes internet illegális, hiszen – hálózati felépítéséből adódóan – pár kattintással minden internet-felhasználó elérhet törvénysértő tartalmakat.

A linkek és a hiperlinkek rendszerét, illetve azokért a tartalmakért való felelősséget, amelyekre a linkek és a hiperlinkek mutatnak, sem az Európa Tanács, sem pedig az Európai Unió nem szabályozza, így azt a tagállamok belső joga dönti el. Németországban a bírói gyakorlat (ez esetben a berlini városi bíróság egy 1997-es döntése) a linkekért és a hiperlinkekért való felelősséget a weboldalak létrehozásáért (tartalomszolgáltatásért) való felelősséggel azonosította. A berlini bíróság ítélete kimondta, hogy az illegális tartalmú weboldalra mutató hiperlink ugyanúgy helyeslően és ösztönzően hat a bűncselekményre, mint maga a weboldal, ezért a weboldal tartalmához hasonlóan, elkövetési tárgy.[42] Ezzel megalapozta a közvetett kapcsolati rendszerben elérhetővé tett tartalomért való felelősséget.[43]

A linkek és a hiperlinkek rendszerét, illetve azokért a tartalmakért való felelősséget, amelyekre a linkek és a hiperlinkek mutatnak, sem az Európa Tanács, sem pedig az Európai Unió nem szabályozza, így azt a tagállamok belső joga dönti el. Németországban a bírói gyakorlat a linkekért és a hiperlinkekért való felelősséget a weboldalak létrehozásáért (tartalomszolgáltatásért) való felelősséggel azonosította.

A jogalkalmazó előtt nagy feladat áll: nemcsak internet természetét kell megértenie, hanem döntéseivel ki kell kristályosítania a különböző technikai megjelenésű tartalmak közzétevőinek felelősségi szabályait is. Ez elengedhetetlen feltétele a jogállamiságnak.

10. Nem fejlődik a bírósági gyakorlat

Azzal, hogy a német törvény egyedül a hatóság (BKA) mérlegelésére bízza annak eldöntését, mi az illegális tartalom, és kihagyja ebből a bíróságot, nem ad esélyt a bírói jogalkalmazás fejlődésére, ugyanakkor viszont olyan kérdések eldöntését bízza a nyomozó hatóságra, amelyben még a bíróságok sem jutottak egyetértésre.

Ilyen kardinális kérdés a gyermekpornográfia fogalmi elemeinek kidolgozása, például hogy mennyire kell realisztikusnak lennie egy fiktív gyermekábrázolásnak, mennyire és milyen módon kell szexuálisnak lennie a felvételnek, milyen kritériumok alapján ítéljék meg a szóbeli, az írásbeli ábrázolásokat, vagy mikor hordoz az ábrázolás irodalmi, művészi, azaz társadalmilag elfogadott értéket. Ez jutott kifejezésre a már idézett esetben is, amikor a szolgáltatók nagy többsége azért nem törölte a tartalmakat, mert azok szerintük legálisak voltak.

Ezeknek a kérdéseknek az eldöntése a jogalkalmazás, és elsősorban a bíróság feladata. A gyermekpornográfia minőségi kritériumaiban való döntés egyfelől a független és pártatlan bíróság jogkörébe tartozik, másfelől pedig a feketelisták folyamatos frissítgetését (bizonyos tartalmak listáról való eltávolítása, mások felírása) a nyomozó hatóság meglehetősen felszínes vizsgálattal végzi el, amelynek során nem is lenne elvárható a beható és minden szempontra kiterjedő vizsgálat. Tehát, ha nem is a lista összeállítására, de legalább a vitás esetek eldöntésére a bíróságot kellene felhatalmazni.

Konklúzió

A „blokkolás" kifejezés azt sugallhatja, hogy az internet könnyen és egyszerűen „megtisztítható" az illegális tartalmaktól. Semmi sem távolibb azonban a valóságtól, mint ez a prekoncepció. Az internet-blokkolás komplex technikai folyamat, amely számos szereplő közrehatását igényli. Minimális technikai ismeretek birtokában egyszerűen megkerülhető, ugyanakkor a szükségességi-arányossági kritérium a blokkolással könnyen sérülhet. Nem mindegy, ki blokkol – a felhasználó, a szolgáltató vagy az állam –, milyen tartalmat blokkol – illegális vagy politikai tartalmat, esetleg mindkettőt –, és hogy milyen ideológiai alapon blokkol – erkölcsi vagy politikai alapon.

A blokkolás technikáját, szintjét és ideológiáját körültekintően kell megválasztani ahhoz, hogy az alapvető jogok sértetlenek maradjanak, de a blokkolás is elérje a célját. Az internet-szűrés technikái különösen alapvető jogokba való beavatkozásuk miatt aggályosak: az internetszolgáltatók szolgáltatási szabadsága, tulajdonuk védelme, a tartalomgazdák véleményszabadsága, a felhasználók információhoz jutási szabadsága, valamint a blokkolási technikától függően a távközlési titok is sérülhet.

Az internet természetéből adódóan szinte mindegyik blokkolási módszer megkerülhető, így nem igazán hatékony. 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.

Végül, az internet-blokkolás bírálóit nem tanácsos elítélni, hiszen legalább annyi érv szól a felhasználói és a szolgáltatói jogok oldalán a felhasználói szintű védekezés mellett, mint a paternalista állami védelem mellett.

Jegyzetek

1 Az erre vonatkozó előírásokról lásd: a Tanács 2004/68/IB kerethatározata (2003. december 22.) a gyermekek szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről. HL L13, 2004. 01. 20.

2 Bár szemantikailag a szűrés a és a blokkolás mást jelent – míg a szűrés (filterezés) a megfigyelésre, a blokkolás a már azonosított tartalom továbbjutásának megakadályozására vonatkozik –, a tanulmányban szinonímaként használom ezeket a fogalmakat.

3 Entwurf eines Gesetzes zur Bekampfung der Kinderpornographie in Kommunikationsnetzen. Drucksache 16/12850, 05. 05. 2009, valamint Gesetzesbeschluss des deutschen Bundestages. Drucksache 604/09, 19. 06. 09 Elérhető online: http://www.bundesrat.de/cln_090/SharedDocs/Drucksachen/2009/0601-700/604-09,templateId=raw,property=publicationFile.pdf/604-09.pdf; [2010. 04. 02.]

4 *Full Qualified Domain Name*, azaz teljes vagy abszolút domain név, amely a domain név helyét abszolút pontossággal meghatározza a tartománynév-hierarchiában.

5 Tous, Jean: Government filtering of online content. in: e-Newsletter on the fight against cybercrime (enac) No. 2, August 2009, pp. 14–20

6 További csoportosításokért lásd: Callanan, Cormac. – Gercke, Marco – de Marco, Estelle – Dries-Ziekenheimer, Hein: Internet blocking. Balancing cybercrime responses in democratic societies. Aconite Internet Solutions, 2009 October, pp. 11–20

7 A Google-ben a „free open proxy" címszavas keresés kiadja azokat a távoli szervereket, amelyek alkalmasak a kizárt szerverek pótlására.

8 Pl. http://www.domain.hu/domain/domainsearch/; [2010. 04. 12.] A lekérdezés természetesen csak olyan weboldalról történhet, amely nincs letiltva.

9 Lásd: http://en.wikipedia.org/wiki/Hosts_file; [2010. 04. 12.]

10 A blokkolási technikákról és az országok besorolásáról lásd a Wikipedia internet-cenzúráról szóló bejegyzését: http://en.wikipedia.org/wiki/Internet_censorship; [2010. 05. 01.]

11 Pl. http://www.opendns.com; [2010. 04. 12.]

12 Az SSL hálózatban elért URL mindig https://...-vel kezdődik.

13 A VPN népszerű a munkahelyi internetezés során a magánszféra biztosítására is: levelezésünk és böngészési szokásaink munkáltató általi kifürkészését lehet ilyen módon kikerülni.

14 Az URL a web-böngészőszávban megjelenő domain név utáni tartalom, amely az oldal részletes tartalmára utal. Ezek a részletek a paraméterek.

15 Az open proxy szerver olyan szerver, amely távoli (proxy) és nyilvános (open), tehát mindenki számára elérhető, titkosítja a felhasználó által lehívandó URL-eket, tehát nem teszi lehetővé a szolgáltatónak, hogy azonosítsa a tiltólistás URL-eket, így azokat nem is képes kiszűrni.

16 Brownlee, John: Google stops censoring some Chinese search results for Tiananmen Square protests, Geek.com 2010 Mar, 15. http://www.geek.com/articles/news/google-stops-censoring-some-chinese-search-results-for-tiananmen-square-protests-20100315/; [2010. 05. 01.]

17 Madariaga, Julen: China's Internet Censorship Explained. Chinayouren 22 January 2009 http://chinayouren.com/en/2009/01/22/1334; [2010. 04. 05.]
18 Internet Filtering in Saudi Arabia in 2004. Opennet http://opennet.net/studies/saudi; [2010. 04. 05.]
19 Wikileaks: Italian secret internet censorship list, 287 site subset, Cyberlaw 21 Jun 2009; http://cyberlaw.org.uk/2009/06/29/wikileaks-italian-secret-internet-censorship-list-287-site-subset-21-jun-2009/; [2010. 04. 05.]
20 A karlsruhe-i tartományi bíróság döntését lásd a 41. sz. lábjegyzetben.
21 China's Green Dam: The Implications of Government Control Encroaching on the Home PC. Opennet http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc; [2010. 05. 01.]
22 Promiscuous Women To Blame For Earthquakes. Guardian Associated Press, 19 April 2010 http://www.guardian.co.uk/world/2010/apr/19/women-blame-earthquakes-iran-cleric; [2010. 05. 01.]
23 United States Cong. Senate, 106th Congress, 2nd Session, „HR 4577: An act making appropriations for the Departments of Labor, Health and Human Services, and Education, and related agencies for the fiscal year ending September 30, 2001, and for other purposes," June 15, 2000, http://w2.eff.org/Censorship/Internet_censorship_bills/2000/hr4577_censorware_20000615_excerpts.html; [2010. 05. 01.] Lásd még: Mariano, Gwendolyn: Net-porn law applies deadline pressure, ZDNet Asia, 29 October 2001, http://www.zdnetasia.com/news/hardware/0,39042972,38028681,00.htm; [2010. 05. 01.]
24 Foo, Fran: Net censorship to cost users, Australian IT, 5 August 2008, http://www.australianit.news.com.au/story/0,,24128728-15306,00.html; [2010.05.01.]
25 Best, Jo: Teen cracks AU$84 million porn filter in 30 minutes, ZDNet Australia, 27 August 2007, http://w2.eff.org/Censorship/Internet_censorship_bills/2000/hr4577_censorware_20000615_excerpts.html; [2010. 05. 01.]
26 Winterford, Brett – Grubb, Ben: Conroy to opt for tiered Internet filtering, IT News, 2 June 2009, http://www.itnews.com.au/News/146629,conroy-to-opt-for-tiered-internet-filtering.aspx; [2010. 05. 01.]
27 Wykes, Maggie: Harm, suicide and homicide in cyberspace: assessing casuality and control. in: Jewkes, Yvonne – Yar, Majid (Eds.): Handbook of Internet Crime, Wyllan Publishing, 2010, pp. 369–390
28 Libin, Kevin: Canada's approach to web censorship – first let the flowers grow, then lop them off, The National Post, 30 October 2008, http://network.nationalpost.com/np/blogs/fullcomment/archive/2008/10/30/kevin-libin-australian-internet.aspx; [2010. 05. 12.]
29 UK Government to clarify the law on suicide websites, Bird and Bird, 3 December 2008 http://mail.twobirds.com/ve/ZZx9058V00t869174R27Z9; [2010. 05. 12.]
30 A blokkolási technikákról lásd részletesen: Sieber, Ulrich – Nolde, Malaika: Sperrverfügungen im Internet. Max-Planck-Institut für ausländisches und internationales Strafrecht, 2008 p. 49., 58., 176.
31 A lista nem teljes. A táblázat elkészítéséhez felhasználtam: Callanan, Cormac. – Gercke, Marco – de Marco, Estelle – Dries-Ziekenheimer, Hein: i. m. p. 20
32 A legnagyobb nemzetközi forródrót-hálózat az 1999-ben létrejött INHOPE (https://www.inhope.org/; [2010. 05. 12.]), amelynek mára 30 tagországban van nemzeti forródrótja. Németország 1999 óta, Magyarország 2005 óta tagja. Németországban jelenleg három, hazánkban egy hotline működik, amely az INHOPE tagja. (Az INHOPE tagok listáját lásd: https://www.inhope.org/en/hotlines/facts.html; [2010. 05. 12.])
33 A pedofil-hálózatok rejtőzködő taktikájáról l. pl. UK police uncover global online paedophile network, Child Exploitation and Online Protection Centre, Media Centre, Monday 08 August 2008 http://www.ceop.gov.uk/mediacentre/pressreleases/2008/ceop_18082008.asp; [2010. 05. 12.] További részletekért lásd még: Krone, Tony: Does Thinking Make it so? Defining Online Child Pornography Possession Offences. in: Trends and Issues in Crime and Criminal Justice. Canberra: Australian High Tech Crime Centre, 2005 No. 299 April 2005 p. 1–6
34 Pl. http://www.opendns.com [2010. 04. 12.]
35 Sieber, Ulrich: Sperrverpflichtungen gegen Kinderpornographie im Internet. in: Juristen Zeitung (JZ) 13/2009 p. 653–662
36 Lásd még: A Google és a Yahoo is az ausztrál internetellenőrzési tervek ellen, Sg.hu: Informatikai és Tudományos Hírmagazin 2010. február 18. http://www.sg.hu/cikkek/72596/a_google_es_a_yahoo_is_az_ausztral_internetellenorzesi_tervek_ellen; [2010. 04. 12.]
37 Lásd: Löschen statt verstecken: Es funktioniert! http://ak-zensur.de/2009/05/loeschen-funktioniert.html; [2010. 06. 08.]
38 Dr. Stadler, Max: Bundesregierung will ein Löschgesetz erarbeiten http://www.max-stadler.de/wcsite.php?wc_c=27491&wc_lkm=2521; [2010. 06. 10.] valamint: Lecseréli Németország a pedofil tartalmak elleni törvényt, Sg.hu: Informatikai és Tudományos Hírmagazin 2010. február 23. http://www.sg.hu/cikkek/72694/lecsereli_nemetorszag_a_pedofil_tartalmak_elleni_torvenyt; [2010. 04. 15.]
39 BVerfGE (a német szövetségi alkotmánybíróság döntései) 103, 141ff. (Rn.33) Elérhető a JZ 2001, 1029 oldalán.
40 A pforzheim városi bíróság 2009. 01. 30-i döntését (Az. 8 Gs 7/09) lásd: http://www.internet-law.de/ag_pforzheim.pdf; [2010. 05. 12.] a karlsruhei tartományi bíróság 2009. 02. 23-ai döntését (Az. Qs 45/09) lásd: http://www-internet-law.de/lg_karlsruhe.pdf; [2010. 05. 12.]
41 Lásd még: http://www.heise.de/news/meldung/135461; [2010. 05. 12.]
42 AG Berlin, 260 DS 857/96, 30. Juni 1997: http://www.netlaw.de/urteile/agb_01.htm; [2010. 05. 12.]
43 További technikai megoldásokkal – pl. keresőmotor útján – közzétett tartalomért való felelősség kérdése sem tisztázott, ám e tanulmány a felelősség kérdésével behatóbban nem foglalkozik.

Alexin Zoltán

Adatvédelmi törvényünk – kisebb hibákkal*

1. Bevezetés

A modern adatvédelem kezdetének az 1983-as évet szokás tekinteni, amikor a német alkotmánybíróság megsemmisítette a népszámlálásról szóló törvény egyes pontjait.[1] E határozat hosszabb időre előre meghatározta az adatvédelem gondolkodásmódját és feltételrendszerét. Az ítélet tartalmazta az információs önrendelkezés fogalmát (informationelle Selbstbestimmung), amely szerint „[az információs önrendelkezés] *az az alapjog, amely biztosítja az egyénnek azt a jogot, hogy alapvetően maga döntsön személyes adatainak kiszolgáltatásáról és felhasználásáról*".[2] A német alkotmánybíróság felismerte, hogy a rohamosan fejlődő információs technológia milyen veszélyeket rejt magában, amikor helytől és időtől függetlenül, gyakorlatilag azonnal elérhetővé tesz viselkedésre, szokásokra, társadalmi érintkezésre, világnézetre, vagyoni helyzetre stb. vonatkozó összekapcsolt adatokat az egyes személyekről.

A rendszerváltás elején az újonnan alakult magyar Alkotmánybíróság is meghozta nevezetes 15/1991. számú határozatát, amely gyakorlatilag a német ítélet gondolatvilágát és megállapításait adaptálta. Ezt követően a magyar Országgyűlés elfogadta Magyarország adatvédelmi törvényét: A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény az akkori viszonyok között megelőzte korát. Magyarország azokban az években még nem volt az Európai Unió tagjelöltje sem,[3] és csak néhány szakember számára voltak ismeretek az Európa Tanács emberi jogi egyezményei. A rendszerváltás éppen csak lezajlott. Ugyanakkor a nyolcvanas évek közepén bevezetett univerzális *személyi szám*, különösen annak a banki és egészségügyi számítástechnikai rendszerekben történő általános alkalmazása sötét fenyegető árnyként borult a szocializmus örökségeként itt maradt, és sok tekintetben változatlan elvek mentén működő államra.

A Magyar Köztársaság Alkotmánybírósága magáévá tette a német alkotmánybíróság hasonló ítéletét és a 15/1991. számú határozatában szinte szóról szóra megismételte annak szövegét. Ezzel egyben le is rakta egy elkövetkező adatvédelmi törvény alapjait. A személyes adatok védelméhez fűződő joggal ellentétesnek ítélte az univerzális személyi számot, amely a magán- és a társadalmi élet minden egyes eseményében egyértelműen azonosította az állampolgárt. Az ítélet tartalmazta azt a felfogást, ami néhány éve a nyu-

A szerző a Szegedi Tudományegyetem Természettudományi és Informatikai Kar adjunktusa, okleveles matematikus, 2007-ben meghívták a The European Privacy Institute projekt tudományos tanácsadó testületébe. 2009 januárjától a Dél-Alföldi Regionális Humán Orvosbiológiai Kutatásetikai Bizottság tagja.