

Összefoglaló
a „Cyberspace 2010” c. nemzetközi konferenciáról
(Brno, 2010. november 26-28.)

A „Cyberspace” konferencia 2010. november 26-28-án nyolcadik alkalommal került megrendezésre, a Brno-i Masaryk Egyetem jogi fakultásán.¹ A konferencia évről-évre az aktuális számítástechnikai és az internettel kapcsolatos büntetőjogi, kriminológiai, pszichológiai, etikai, társadalmi kérdésekkel foglalkozik, melyek közül beszámolómban két témakörben emelek ki előadásokat.

1. Online kockázatok, veszélyek és gyermekvédelem

A konferencia egyik központi témája a gyermekek online védelme volt. A gyermekek online káros és ártalmas tartalmakkal szembeni védelmét az Európai Parlament és a Tanács már 1999 óta központi kérdésnek tekinti. Ekkor fogalmazta meg ugyanis biztonságosabb internet akciótervét először, amelyet később többször is – legutóbb 2013-ig, biztonságosabb internet plusz néven – meghosszabbított. Az EU a telekommunikációs és információs technológiai (IT) eszközök segítségével terjesztett gyermekpornográfia elleni küzdelem felől közelíti meg a kérdést, hiszen a gyermekpornográfia egyik mellékága a gyermekprostitúció, a gyermekszexmunka és a gyermekkereskedelem. Ezek a jelenségek korábban is léteztek, de az IT fellendülésével az 1990-es évek második felében fokozatosan a felszínre kerültek, egyre láthatóbbá váltak, mi több, az IT lökést is adott a szervezett bűnözésnek. Az első akciótervnek az európai forródrót-hálózat kiépítése volt a célja, amelyen a felhasználók mindenféle illegális és káros online tartalmat bejelenthetnek. A másik cél a hozzáférés- és tartalomszolgáltatók által ellenőrzött, önmagát szabályozó rendszer kifejlesztése, amelynek segítségével biztonságosabbá tehető az online környezet az illegális tartalmak kiszűrése által. Az EU 2005-ben „Safer Internet Plus” néven bővítette akciótervét,² amelyben inkább a felhasználókra helyezte a hangsúlyt: a szülőkre, a pedagógusokra, és a gyerekekre koncentrált abban a tekintetben, hogy felvilágosítja őket a veszélyekről, és tudatosítja bennük a teendőket. Az uniónak azonban sokáig nem volt elképzelése arról, hogyan, minek alapján kellene kidolgozni a felvilágosító stratégiákat. Az első említésre méltó kutatás a téren a gyermekeket fenyegető online kockázatok és ártalmak felmérésére a 2009-ben indult EU Kids Online,³ amely 2009-ben csupán kisebb, nemzeti mintán készült kutatások eredményeit dolgozta fel, 2010-ben azonban már egy 25 országra kiterjedő, empirikus vizsgálatot folytatott le, összesen 25.000, 9-16 gyerek és legalább ugyanennyi felnőtt megkérdezésével. A konferencián a kutatás koordinátorai bemutatták az elsődleges eredményeket.

Ellen J. Helsper (London School of Economics, az EU Kids Online kutatás tanácsadó testületének tagja) azt vizsgálta, milyen társadalmi és individuális meghatározói vannak a rendszeres internetezésnek. Kutatása szerint az internet-használatot a nem, az egyéni szocio-ökonómiai státusz, az adott ország egy főre eső jövedelme (GDP), valamint a képzettség befolyásolja. Érdekes módon, a rendszeres internet-használat leginkább nem a

¹ <http://cyberspace.muni.cz/english/index.php>

² A programról részletesen lásd az Európai Információs Társadalom portálját: http://ec.europa.eu/information_society/activities/sip/policy/programme/current_prog/index_en.htm

³ A kutatásról részletesen lásd: <http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx>

legtanultabbak, hanem a középiskolát végzettek gyerekeire jellemző. Ez a megközelítés is az összetevője lehet a biztonságos internetezésről szóló felvilágosító programoknak, amelyeket a kutatás eredményei alapján a 2011-2013-as időszakban, a Safer Internet Plus keretében kiegészítenek, frissítenek.

Ingrid Paus-Hasebrink (Audio-visual Communication at the Department of Communication, Faculty of Culture and Social Science at the University of Salzburg) a salzburgi egyetem média-tanszékének előkészítő fázisában lévő kutatásáról számolt be. A kutatás fő kérdései: hogyan használják a netet a gyerekek? Mit csinálnak a gyerekek a neten? Mi viszi rá őket, hogy azt csinálják, amit csinálnak? A meglévő kutatások csak az individuális modelleket, az egyéni szituációs viselkedési mintákat veszik alapul, és nem veszik számba a nemzeti, a régiós sajátosságokat. A salzburgi egyetem kutatása nemcsak ezeket a hiányosságokat kívánja kiküszöbölni, de az internet mellett vizsgálná a többi médium használatának jellegzetességeit és a különböző médiumok hatását (média-repertoár) is a gyermekek viselkedési mintáinak kialakulására. Ugyanakkor szem előtt kell tartani, hogy az internet-használat nem független a többi média használatától, továbbá az internet nemcsak egy új médium, hiszen egyesíti, magában hordozza a többi médium jellemzőit. Ezért a korábbi média-repertoár-kutatások módszertani átalakítására van szükség. A készülő kutatás keretében nemcsak a családokat, hanem az intézményeket (óvoda, iskola) is vizsgálják, a nevelési elvek összehangolása érdekében. Azt vizsgálják, vajon a szülők stratégiája jó-e arra, hogy segítse a gyerekeket a biztonságos média-használatban, vagy éppen hogy akadályozza őket ebben.

Paus-Hasebrink, az EU Kids Online projekt kutatójaként bemutatta az EU Kids jelentésében található életkor- és nemi megoszlás szerinti internet-használati gyakoriságot is. A felnőttekhez hasonlóan, a gyerekek is gyakrabban használják az internetet passzívan: keresnek rá más által kreált információkra, néznek videoklippeket stb., és csak kevesen létesítenek avatárt, online alteregót és kevesen írnak pl. blogot. A hasonló trend ellenére a gyerekek (a vizsgált korosztályon belül is főleg a 11-16 évesek) nagyobb hányada használja aktív tevékenységre a netet, mint a felnőttek. Cluster-analízis keretében a következő csoportokat sikerült elkülönítenie:

Cluster 1: Játzók és kommunikálók csoportja (16,3%)

Cluster 2: netet munkához (házi feladathoz) használók csoportja (11,8%)

Cluster 3: visszahúzódozó, nem kommunikatív csoport (28,5%)

Cluster 4: kreatív, játékos, kipróbáló csoport (29,0%)

Cluster 5: visszafogott kommunikációt folytatók csoportja (14,5%)

Elemzése szerint csak a nem kommunikatív gyerekek töltenek szignifikánsan kevesebb időt online, a többi csoportnak a neten töltött idejét nem befolyásolja az attitűd (hogy kommunikatív célokra használja-e a netet) és hogy milyen különböző tevékenységeket végez online.

Moni Barbovschi (Faculty of Sociology and Social Work, UBB, Cluj, Romania), az EU Kids Online román referense szerint a felnőttek és a gyerekek kockázat- és veszélyfogalma online nem egyezik meg. (Az EU Kids kutatás munkacíme is ez: kockázatok és ártalmak online) Sokszor a felnőttek által kockázatosnak ítélt dolgot a gyerekek benefitnek tekintik, így pl. a közösségi oldalakon való regisztrációt és a személyes adatok kitételét.

Barbovschi azt vizsgálta, hogy a kisgyermekkorban elszenvedett traumák (érzelmi, fizikai, szomatikus, családi és kortárs-problémák) hogyan függenek össze azzal a jelenséggel, hogy online környezetben másnak adja ki magát a gyermek. A kisebb gyerekeknél (9-10 évesek) nagyobb összefüggést talált, mint a 11-16 éveseknél. Emellett a más identitás

felvétele a polgárpukkasztó, szenzációkeltő magatartással is egyenes arányban változik. Megfigyelte továbbá, hogy minél szívesebben vesz részt a gyermek identitás-játékokban, annál több dolgot próbált ki már online, annál többféle online tevékenységet végez. Ez a kipróbáló-kalandkereső attitűddel függhet össze. Azt, hogy melyik összetevő milyen mértékben hat az identitás-játékokban résztvevő gyerekek attitűdjének kialakításában, a jövőben regressziós analízissel vizsgálja a kutató.

A kutatás kritikájaként merült fel, hogy nem lehet tudni, mikor mond igazat a megkérdezett gyermek, hiszen lehetséges, hogy akkor is más személyiséget játszik, amikor a kérdőívre válaszol. Ennek a valószínűsége azonban nemcsak az identitás-váltást vizsgáló kutatásoknál, hanem minden kutatásnál megvan.

A konferencián jómagam beszámoltam az OKRI 2009-2010-es, gyermekek online szexuális bántalmazását vizsgáló kutatásának eredményeiről.⁴ Kutatásunkban a budapesti, 16 éves iskolás gyermekek internetezési szokásait vizsgáltuk, összehasonlítva azt külföldi kutatások adataival, valamint az EU Kids Online kutatás eredményeivel. (Virág & Parti, 2010) Összehasonlításunkból kitűnik, hogy a kelet-európai – az EU-hoz újonnan csatlakozott – országokban élő gyerekek nagyobb kockázatokat szenvednek el a nethasználat során, az alábbi tényezők miatt:

- a felnőtt és a kiskorú lakosság között nagyobb a digitális szakadék, mint Nyugat-Európában;
- a szülők kevésbé veszélytudatos nethasználók, emiatt nem, vagy kevésbé készítik fel gyerekeiket a nethasználat kockázataira;
- a nethasználat drasztikus megugrása, mindennapivá válása még mindig csak az kis- és középiskolás korú lakosság körében tapasztalható és túl gyorsan történt ahhoz, hogy felvilágosító programokat vagy kampányokat lehetett volna kidolgozni. (pl. Bulgária, Románia, Észtország, Görögország, Lengyelország, Portugália, Magyarország, I. EU Kids Online, 2009: 23);
- Kelet-Európában később kezdődött meg (vagy jelenleg is teljesen hiányzik) a biztonságos nethasználatra oktatás, a gyerekek jórészt csak technikai segítséget kapnak az iskolában, de a szociális szakképzettséggel való ellátásuk nem üti meg a mércét.

Ugyanakkor a kelet-európai gyerekeket szüleik lemaradása nagyobb önállóságra készíteti a nethasználattal kapcsolatos problémák megoldása során – legyen az technikai probléma vagy illegális, illetve káros tartalommal való szembesülés.

2. Cyber law theory

A másik fontos panel a cybertér szabályozásához kapcsolódott.

Qian Tao (China/Scuola Superiore Sant Anna, Pisa, Italy) ugyancsak a közösségi oldalak magánéletet sértő tartalmának megítélését vizsgálta, de összehasonlította a kínai és az európai gyakorlatot is. A magánélet sérthetlenségére a kínai alkotmány és Ptk. nem tartalmaz szabályokat, de a népköztársaság legfelsőbb bírósága három ügyben kimondta a létezését, amelyek precedensértékűek. Emellett az internet-szolgáltatókat kötik az értesítési-levélteli szabályok, különösen az időbeli eltávolítás (takedown in time) szabálya: amint tudomást szerez (értesítést kap) a jogsértésről, a szolgáltatónak el kell távolítania a tartalmakat.

Három esetről számol be.

⁴ A kutatást a Szociális és Munkaügyi Minisztérium, valamint a Mérei Ferenc Fővárosi Pedagógiai és Pályaválasztási Tanácsadó Intézet támogatásával készítette az ESZTER Alapítvány és az OKRI.

1. Zhang Xinlin v. Tianya.cn (2008)

Az adott ügyben az internet-szolgáltató (Electronic Messaging Service Provider) azzal érvelt, hogy az állam által bevezetett filterező szoftvereknek csak az antikommunista tartalmak eltávolítására van kapacitása, de a személyes adatok eltávolítására nincs. A bíróság azonban megállapította, hogy az ilyen szolgáltatóknak igenis monitorozniuk kellene mások tartalmait, így hamarabb eltávolítható lenne a sértő tartalom. Az előadó megfogalmazta az ítélet kritikáját, amely szerint elsősorban a felhasználónak kellene védenie a saját tartalmait/személyi adatait, nem pedig a szolgáltatónak, akinek egyébként nincs oldalszerkesztési joga. Ugyanakkor a monitoring-kötelezettség bevezetése a szólásszabadság sérelméhez vezethet.

2. Wand Fei v. Tianya.cn (2009)

A hivatkozott ügyben a felperes azt mondta, hogy a szolgáltatónak monitorozási tevékenysége közben tudnia kellett volna, hogy mely üzenetek sértőek a felhasználóra nézve. A bíróság szerint azonban a szolgáltató teljesítette monitorozási kötelezettségét. Kérdés marad, hogy mennyi az az idő, ami még elfogadhatónak számít („in time”) a levétel? (nincs joggyakorlat) Plusz, az értesítési-levélteli eljárás határidejét egyébként tartalmaznia kellene a felhasználóval kötött szolgáltatói szerződésben (user agreementben/terms of usage), amely mind a mai napig hiányzik.

3. Yin Hong v. Baidu (2010)

Az alperes kitette weboldalára a felperes pornográf jellegű felvételeit. Ez óriási visszhangot keltett, hiszen a pornográfia megítélése Kínában az európainál sokkal szigorúbb. A per során kérdésként merült fel, hogy kinek kell kérnie az ilyen sértő tartalom eltávolítását? Elegendő-e, ha valaki személyazonossága megjelölése nélkül kéri az eltávolítást? A bíróság 2010 júniusában felelősnek találta a felvételek kitevőjét.

Az említett esetek ahhoz vezettek, hogy az eddig elhanyagolható mértékben gyakorolt és jórészt csupán az értesítési-levélteli eljárásra korlátozódó, ún. passzív monitoring mérsékelt monitoringgá alakult Kínában. Az előadó levezette, hogy 2006 és 2010 között milyen változások mentek végbe a szabályozási politikában, de megjegyezte, hogy egyiknek sem volt summázata a szólásszabadság védelme, szem előtt tartása. Annak ellenére, hogy a szólásszabadság védelme benne van a kínai alkotmányban, az európai kultúrkörtől eltérő értelmezést nyer. E jog csak a közintézményeket illeti meg, a természetes személyeket csak akkor, ha a politikai életben tevékenykednek vagy egyébként befolyásosak.

Az előadás amiatt is aktuális volt, mert az utóbbi időben szerte Európában kísérletek születtek az online illegális tartalmak kormányzati, illetve szolgáltatói szintű szűrésére. Az Európai Unió Tanácsa⁵ kifejezett célként említi az ártalmas (illegális) tartalmak blokkolását a tagállamok számára. (Art. 21) Ezek a rendelkezések számos vitát váltanak ki mind tagállami, mind uniós szinten. Az Európai Tanács törekvései például szembe mennek az elektronikus kereskedelemről szóló Irányelv⁶ rendelkezéseivel, amely szerint a szolgáltatók nem kötelezhetők monitoringra. Ehhez képest a tagállami szinten az utóbbi időben hatályba lépett jogszabályok a monitorozási kötelezettség előírásával az Irányelv határát feszegetik.

⁵ Council of the European Union 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, 6 September 2010

⁶ 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") Hivatalos Lap L 178 , 17/07/2000 o. 0001 - 0016

Alzbeta Krausová (Masaryk University) *Human and Superhuman* c. előadásában felvetette a neurobiológiai kutatások és a jog összefonódásának jelentőségét az információs korban. A legújabb neurobiológiai fejlesztések már olyan művétagok- és szervek fejlesztésével foglalkoznak, amelyek a páciens agyával félig vagy teljesen beépített mikrochipek segítségével kommunikálnak, így azokat a páciens pusztán az akaratával működteti vagy éppen közvetlenül a központi idegrendszer irányítja.⁷ Ugyanakkor e fejlesztések segítségével az emberek képesek egymással gondolati síkon kommunikálni. Ezeket a fejlesztéseket egyfelől bioetikai kérdések követik: ha minden ember a természetnél fogva egyenlőnek születik, akkor hogyan küszöböljük ki azt a csorbát, amelyet az ilyen fejlesztések egyes emberek számára biztosítanak, a szegényebbek számára viszont nem. További kérdés, hogy hogyan használja ezeket a technológiákat a hadiipar és a kereskedelem? Vajon ezek a technológiák jobban veszélyeztetik-e a társadalom alapját, az egyenlőséget, mint az egyébként már meglévő egyenlőtlenség-opciók (kisebbség-többség, gazdagság-szegénység, stb.)? Először is analizálni kell, mit tekintünk egyenjogúságnak, egyformaságnak. Az arisztotelészi, a rawls-i egyenlőség-definíció amely szerint mindenkit egyenlőnek kell tekinteni, aki egyforma, kiegészítésre szorul (miben egyforma?). (Heller, 1975; Rawls, 1997 [1971]) Csak az engedheti meg ezeket a fejlesztéseket, aki rendelkezik elegendő pénzzel, de ennek ellenére még áll a társadalmi egységesség/egyenlőség szabálya, amely szerint senkit nem szabad kizárni. Így az egyenlőség a technikai fejlődéssel átalakul az elérhetőség szabályává.

Ezek a technológiák visszaélésekre is lehetőséget adnak, mégpedig a testünk feletti kontroll átvételére. A kontroll lehet: állami (törvények, javak újraelosztása), fizikai (valakinek a közvetlen hatalma az egyén felett) és mentális (valaki az egyénbe ültet gondolatokat). Mindegy, mennyire lesz fejlett a technológia, az emberekbe be kell építeni az egyenlőség alapelvét. A másik oldal pedig, hogy itt a neurobiológusoknak is nagy a felelőssége: nekik kell megállítaniuk valahol a technikai fejlesztőt, a túlkapások elkerülése végett.

Tomas Scerba (Masaryk University) az elektronikus szerződéskötés c. előadásában arról az alapproblémáról beszélt, hogyan tesszük hitelessé és igazolhatóvá online vásárlásainkat és tranzakcióinkat. (l. még: Héder & Rátai, 2010) Az utóbbi 15 évben, az internet elterjedésével megsokasodtak az írásbeli szerződések. A webes alapú írásbeli szerződések azonban mind formátumukban, mind biztonsági fokukban, mind felhasználhatóságukban különböznek a hagyományos, papíralapú szerződésektől. A hagyományos, papíralapú szerződés jól olvasható, annak birtokosa meggyőződhet minden, a szerződés által hivatkozott dokumentum meglétéről (hiszen azok csatolva vannak a szerződéshez), valamint arról is, hogy a szerződés hitelesen tanúsítja megkötésének körülményeit és a benne foglaltakat. A webes alapú szerződéskötéshez mindezt külön biztosítani kell, mi több, a szerződéskötésnek mind technikai, mind pedig jogi szempontból támadhatatlannak kell lennie. A különböző típusú webes szerződéskötési alkalmazások⁸

⁷ Ilyenek pl. a neten rendelhető ún. „research boksok”, amelyek adatokat gyűjtenek a testről, amit utána be lehet küldeni az orvosnak elemzésre. Az Intendix olyan gépelő program, amelynek nem szükséges diktálni, mert a gondolatokat írja le. Az Egyesült Államok hadseregének fejlesztése a katonák számára egy speciális sisak, amelynek segítségével mérik az agyi funkcióikat és szükség esetén éberben tartják őket – ugyancsak a sisak segítségével (*ultrasonic technology*). A *computer mediated telepathy* (CMT) olyan technológia, amellyel elhalt vagy megsebesült agyterületeket helyettesítenek. Lásd a részletekért Kevin Warwick, professzor, az „első kiborg” weboldalát: <http://www.kevinwarwick.com/icyborg.htm>

⁸ *Shrink-wrap agreement* (pl. cd-t veszek meg dobozban a boltban); *click-wrap agreement* (laptopot akarok venni, és ráklikkelek a „szerződési feltételek elfogadása” gombra); *click-through agreement* (a vásárlónak be is kell írnia már néhány szót, ami már az akarat nagyobb kifejezésének minősül); *browse-wrap agreement* (ha 2-3

segítségével a szerződés nemcsak hogy olvasható (kompatibilis) a webes felületen, de integrálja azokról a jogviszonyokról készült információkat is, amelyekre a szerződés hivatkozik, és mindezt hitelesített formában teszi (időbélyegző és elektronikus aláírás opcionális használatával), ami ahhoz szükséges, hogy a tanúsított jogviszony bíróság előtt is igazolható legyen.

§§§

Hivatkozott irodalom

EU Kids Online, 2009: Livingstone, S. & Haddon, L. (2009) *Eu Kids Online: Final Report*. LSE, London: EU Kids Online. (EC Safer Internet Plus Programme Deliverable D6.5) Available: <http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx> [23.08.2010]

EU Kids Online, 2010: Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (Eds.) (2010) Risk and Safety on the Internet. The Perspective of European Children. Initial Findings from the EU Kids Online Survey of 9-16 Year Olds and Their Parents. www.eukidsonline.net Available: [http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EUKidsII%20\(2009-11\)/EU%20Kids%20Online%20II%20Reports.aspx](http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EUKidsII%20(2009-11)/EU%20Kids%20Online%20II%20Reports.aspx) [13.12.2010]

Heller Á. (1975) Arisztotelész korai etikái In.: Arisztotelész: Eudemoszi Etika - Nagy Etika, Gondolat

Héder M. & Rátai B. (2010) Szerződések szemantikai értelmezése webes felületen In: *Studia Iuridica*, Pécsi Tudományegyetem, ÁJK, 2010 pp. 211-230

Rawls, J. (1997) [1971] Az igazságosság elmélete, Osiris

Virág Gy. & Parti K. (2010) Szemérmetlen tájékozottság. A kelet-európai gyerekek nethasználatának specifikumai. In: Fótiné Német M. (szerk.) *Kölcsönhatások. Az iskolai agresszió megelőzésének és kezelésének többszemponú megközelítése*. MFPI, Budapest, 2010 pp. 118-134

Budapest, 2010. december 20.

Dr. Parti Katalin s.k.
tud. fmts.
Bűnözéskutatási Osztály

percnél tovább marad a felhasználó az adott weboldalon, akkor ezzel önmagában „megrendeli” a szolgáltatást, amit kínál a weboldal).