Összefoglaló

az „Internetes és számítástechnikai bűnözés – megelőzés és megfigyelés” c. workshopról (Barcelona, 2010. november 5.)

A „Internetes és számítástechnikai bűnözés – megelőzés és megfigyelés” (*Cybercrime and computer crime – prevention and surveillance*) c. workshop A jog, a biztonság és a magánélet információs technológiai kérdései c. 5. nemzetközi konferencia *(The 5th International Conference on Legal, Security and Privacy Issues in IT)* keretében került megrendezésre, a Katalóniai Nemzetközi Egyetemen, Barcelonában.

A Katalóniai Nemzetközi Egyetem 1997 óta működik, Barcelonában és Sant Cugatban rendelkezik kampusszal. Míg a barcelonai kampusz a társadalomtudományoknak és az információs technológiának ad otthont, addig a Sant cugati az orvostudománynak. Nemcsak alapképzést, de posztgraduális, mester- és doktori képzést is kínál. Az egyetem hallgatói 69 különböző országból kerülnek ki. Az egyetem vezérelve az interdiszciplináris megközelítés, amely a személyre szabott tréningekben és a szakmai konzultációkon is megjelenik.

A mostani workshop azért volt különösen fontos, mert a jogalkalmazók (nyomozó hatóság, ügyészség, bíróság), valamint a jogalkotók, a kriminálpolitika formálói (igazságügyi tárca) és az informatikai szakértők is képviseltették magukat, így a különböző szakterületek megismerhették egymás álláspontját. Az eseményen ugyanakkor nemcsak spanyol és katalán, hanem holland, norvég, belga, USA-beli és magyar előadók is részt vettek, ismertetve az országukban hatályos jogszabályokat, jó gyakorlatokat és kutatási eredményeket.

Az egynapos program öt kisebb szekciót foglalt magában, az adatvédelem és -biztonság, a büntetőpolitika, a felderítés és a nyomozás, a gyermekek online szexuális abúzusa, valamint a magánélet és a prevenció témájában. A szekciókban 3-4 előadás hangzott el, amelyekből a továbbiakban néhányat ismertetek.

A biztonságtechnikai szakértők még ma is az emberi tényezőt találják a leggyengébb láncszemnek a védelmi rendszerben. (**Antoni Bosch**, Institute of Audit & IT-Governance; **Antonio Troncoso Reigada**, Agencia de Protección de Datos de la Comunidad de Madrid) Nincs értelme költeni a legmegbízhatóbb biztonsági rendszerekre, hogyha elmulasztjuk a dolgozók alapvető biztonsági felkészítését. Ehelyett olyan értékű biztonsági rendszert kell megvásárolni, amely arányos a védeni kívánt értékkel. A védendő értéket az adatok titkossága, biztonsági hierarchiában való elhelyezkedése határozza meg. Kisvállalkozásoknak nem célszerű a legprofibb biztonsági rendszert beépíteniük, hacsak a kezelt adatok nem oly mértékben szenzitívek, hogy azok védelme megér az átlagosnál magasabb szintű védelmet. (l. még: Moitra, 2010) Ilyenek például a kisméretű egészségügyi vagy pszichiátriai szolgáltatást nyújtó intézmények, amelyek rendkívül szenzitív beteg-adatokat kezelnek. Ha ezek az adatok valamilyen okból – ami leggyakrabban az emberi mulasztás – kikerülnek az arra jogosult intézmény birtokából (ahogy az előadásokban idézett spanyol és olasz esetekben történt 2009-2010-ben), sok embernek okoznak nagy kárt. Ilyen módon nemcsak adatvédelmi, de egészségügyi, illetve emberi jogok is sérülnek. Az emberi tényező mulasztása következtében ezek az adatok kikerülhetnek a kezelésre jogosult birtokából például egyszerű géplopás vagy a jelszó nyilvánosságra hozása következtében. Az előadók felhívták a figyelmet a másik fontos alapelvre, mégpedig a felhasználói/adatkezelői jogosultságok szigorú szabályozására. A jogosultságok megosztását – ti. hogy az adatbázis mely szegmensébe, szintjére kinek van hozzáférési jogosultsága – mindig tiszteletben kell tartani.

A számítástechnikai és az internetes bűnözés új tényállásai a spanyol Btk-ban a károkozás informatikai rendszerben, valamint a hacking. Utóbbi Magyarországon is önálló tényállás, illetőleg az anyagi haszonszerzési vagy károkozási célzattal való elkövetés minősítő körülmény (300/C. § Számítástechnikai rendszer és adatok elleni bűncselekmény). Ehhez hasonlóan, az új spanyol tényállás szerint a rendszerbe engedély nélküli behatolás vagy ott engedély hiányában való benn maradás szándéktól függetlenül is bűncselekményt valósít meg.

A spanyol joggyakorlat a gyermekpornográf felvételek megítélésében hasonló szabályozást követ a magyarhoz, minthogy nem az ábrázolt személy látszólagos, hanem valóságos életkora releváns a felvétel megítélésénél. A számítógéppel manipulált felvételek és a gyermeket ábrázoló realisztikus felvételek a büntető joggyakorlat számára csakúgy irrelevánsak, mint hazánkban. Az előadók elmondták, hogy a privát használatú szoftverek már annyira fejlettek, hogy számos esetben csak az informatikai szakértő képes megállapítani, ha az adott felvétel nem valódi személyt ábrázol, csupán pszeudo-felvétel. A spanyol rendőrség ezzel a problémával nincs egyedül (Parti, 2009), ám a magyar gyakorlattal ellentétben ők nem a technikai eszközök hiánya miatt adják át a lefoglalt adathordozókat az informatikai szakértőnek, hanem a komputer-manipulált felvételek kiszűrése érdekében. Az CFLabs munkatársai elmondták, hogy a rendőrség technikai eszközökkel való ellátása és képzése folyamatos. (**Fredesvinda Insa** & **Matías Bevilacqua**, CFLabs) További dilemma, hogy szükséges-e vizsgálni és ha igen, milyen mértékig a felvételek környezetét. Ha például egy büszke szülő saját családi weboldalára tölt fel képeket gyermekéről, az büntetőjogi szempontból irreleváns, míg ha ugyanezeket a felvételeket egy pedofil szerzi meg és saját tematikus könyvtárában őrzi vagy online galériájában közzéteszi, ezt a bűnüldözés nem hagyhatja figyelmen kívül. Az előadók kiemelték a gyermekpornográf bűnszervezetek file-cserélő hálózatokká alakulásának problematikáját. A gyermekpornográf felvételek terjesztői kihasználják a web 2.0 adta előnyöket és a világhálóról a biztos háttérbe húzódnak. Míg a webes tartalmak monitorozással viszonylag könnyen felderíthetők, addig a P2P hálózatok, ahol a tartalom nem a weben, hanem az egymáshoz kapcsolódó felhasználók személyi számítógépein található, nehezen lokalizálhatók. Éppen ezért sem a hagyományos webes alapú tartalmakkal szemben kifejlesztett védekezési módok (pl. felhasználói szinten a szűrőszoftver, kormányzati szinten a tartalomblokkolás), sem az ellenük való nemzetközi fellépések nem sikeresek. (**Antonio Parrilla**, Guarda Civil)

Az online környezetben a sértettek jobban hozzájárulnak viktimizálódásukhoz, mint a földrajzi világban. Ez nem csupán a biztonsági rendszerek személyi oldalának sérülékenységében mutatkozik meg, hanem ékes példái a gyermekekkel szembeni online visszaélések is. A gyermekekkel szembeni online visszaélések területén a legnagyobb veszélyt a személyes adatok közzététele jelenti. Ahogy az előadó fogalmazott: a közösségi portálokon az intimitás helyett az extimitás érvényesül, minél több személyes adatok tesznek ki magukról a gyerekek, annál beágyazottabbak a közösségbe, annál inkább elfogadják őket társaik. (**Jordi Bacaria**, International University of Catalonia) Ebben a tekintetben nem beszélhetünk online kriminológiáról, hiszen a fiatalok esetében ugyanolyan kötőerővel hat a csoporthoz tartozás és a csoportnormákhoz igazodás, mint a földrajzi világban. (Durkheim, 1912; Merton, 1938) Amilyen nagy szerepet vállalhat a közösség a normaszegéstől való visszatartásban (Hirschi, 1969), olyannyira bűnre is csábíthat, abban az esetben, hogyha a közösségi norma az elfogadott társadalmi értékrend tagadása. (Asch, 1956) Emellett a virtuális terek ugyanúgy bűn-generátorként és bűn-vonzóként hathatnak, mint a földrajziak. (Wilson & Kelling, 1982)

A szekciók előadói az online közösségi oldalakat a felejtés végével aposztrofálták: az oda feltöltött adatok, felvételek többé nem törölhetők a világhálóról („the end of forgetting"). (**José Agustina**, International University of Catalonia) Erre rímel az Európai Bizottság új stratégiája az EU adatvédelmi szabályainak szigorításáról, amelyet éppen a konferencia előtti napon hoztak nyilvánosságra.[1] A Bizottság a stratégia keretében a 1995. évi 95/46/EK adatvédelmi irányelvnek megfelelően felülvizsgálja a 2006/24/EK adatvisszatartási irányelv rendelkezéseit. Az adatvisszatartási irányelv előírásai, amelyek a szolgáltatók számára minimum 6 hónapi és maximum 2 évi adatmegőrzési („adatvisszatartási") időt írnak elő vitákat generáltak az EU számos országában, például Spanyolországban is. Az irányelvet számos országban – így Belgiumban, Írországban, Luxemburgban, az Egyesült Királyságban és Norvégiában – nem implementálták a belső jogba. A német és a román alkotmánybíróság pedig alkotmányellenesnek, így alkalmazhatatlannak nyilvánította az irányelvnek a kezelhető adatok körét meghatározó passzusát.[2] A spanyol rendőrség sem tartja szükségesnek az adatvisszatartási irányelv által előírt „készültséget". Érvelésük szerint nem szükséges az irányelvben meghatározott széles körben a forgalmi adatok rögzítése, hiszen a 2004. március 11-i madridi metró-robbantások nyomozásának sikeréhez ugyan hozzájárultak a forgalmi adatok, de ehhez elegendő volt az akkor hatályos jogszabályok szerinti szűkebb adatkör is. A Bizottság a mostani javaslatban célul tűzi ki a magánfelhasználók jogainak erősítését, a büntetőeljárás céljára felhasznált (tárolt és átadott) adatok kezelhetőségének szigorúbb szabályozását, az internet-szolgáltatókat sújtó adminisztrációs terhek csökkentését, valamint az adatvédelmi hatóságok szerepének növelését és fellépésük összehangolását. A Bizottság előterjesztése szerint a magánszemélyek számára biztosítani kell a „felejtés jogát" („right to be forgotten"), azaz megfelelő tájékoztatást kell adni a felhasználóknak adataik rögzítéséről, tárolásáról és felhasználásának miként jéről. A cél az, hogy felhasználók adatai minden esetben csak kifejezett jóváhagyásuk esetén legyenek kezelhetők és továbbíthatók – nem csak offline, de online tranzakcióik során is. A személyes adatok gyűjtését és felhasználását a szükséges minimumra kell korlátozni. Ennek érdekében a Bizottság ösztönzi az ismeretterjesztő kampányokat, valamint a szolgáltató szektor önszabályozási kezdeményezéseit.[3]

Az elektronikus fizetőeszközzel való visszaélések fajtái a hamisított kártyahasználat, az elvesztett vagy ellopott kártya jogtalan használata, valamint a kártyaadatok jogosult általi kiadásának elérése online (phishing). (**Reinhard Steennot**, University of Ghent) E visszaélések megítélésének mindenkori nagy kérdése, hogy ki felel a csalással okozott kárért. Ezt azért nehéz meghatározni, mert az elkövető személye a legtöbbször felderítetlen marad, éppen ezért a kárt a szolgáltató és a szolgáltatás igénybevevője között kell valamiképpen megosztani. A hamisított hitel- vagy bankkártyával elkövetett csalás esetében például mindenképpen a szolgáltató viseli a felhasználó kárát, hiszen ő szavatol azért, hogy a kártyát

[1] Europa Press Releases „RAPID": http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1462&format=HTML&aged=0&language=HU&guiLanguage=hu; (2010. 11. 04.)

[2] Sammel-Verfassungsbeschwerde gegen die Vorratsdatenspeicherung. Stoppt die Vorratsdatenspeicherung! http://www.vorratsdatenspeicherung.de/content/view/51/70/lang,en/; valamint: Romanian Data Retention Law Ruled Unconstitutional. Softpedia. http://news.softpedia.com/news/Romanian-Data-Retention-Law-Ruled-Unconstitutional-123908.shtml; (2010. 11. 09.)

[3] A Bizottság javaslatát 2011. január 15-ig lehet véleményezni! Észrevételek a Bizottság nyilvános konzultációs honlapján tehetők: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm; A nyilvános vita alapján a Bizottság 2011-ben javaslatokat fog benyújtani egy új általános adatvédelmi jogszabályi keretre vonatkozóan, amelyet azután az Európai Parlamentnek és a Tanácsnak kell megtárgyalnia és elfogadnia.

ne lehessen hamisítani. Ez a „Sphärentheory" analógiája, amely szerint mindig az viseli a kockázatot, akinek az adott esetben (szerződés szerint, tranzakcióban, szolgáltatásban stb.) a helyzete leginkább lehetővé teszi, hogy megakadályozza az adott veszteséget. (Ulmer, 1938; Thevenoz, 1990) Ezzel szemben a kártyatulajdonost terheli a felelősség a bankkártyával elkövetett visszaéléssel okozott kárért, hogyha a lopás bejelentése, illetve a kártya letiltása terén mulasztás terheli.[4] De ebben az esetben is csupán 150 Eurós felső határig felel a kártyatulajdonos, kivéve ha súlyos gondatlanság terheli a kártyával kapcsolatos biztonsági intézkedések megtételének elmulasztásában. A gondot az okozza, nincs egységes végrehajtási szabályozás a „súlyos gondatlanság" megítélésére, amelyet így a bíróságnak minden esetben külön mérlegelnie kell. Súlyos-e a gondatlanság például, ha a kártyatulajdonos PIN kódját a kártya mellett a tárcájában tartja? Vagy csupán akkor, ha késlekedett a kártyalopás bejelentésével? (Ilyenkor vizsgálni szükséges, mit jelent a „késlekedés".) Esetleg ha közösség számára nyitva álló helységben őrizetlenül hagyja a kártyát? Vagy ha nem tett eleget az online bankolás alapvető biztonsági követelményeinek (nem cserélte jelszavát, gyenge jelszót adott meg stb.)? Ebből következően nem világos az sem, ki viseli a bizonyítási terhet. Ez azonban nem az elektronikus fizetési szolgáltatások 2007/64/EK direktívájának hiányossága. Az előadó szerint a számítástechnikai bűncselekmények területén tapasztalható punitív joggyakorlati tendencia helyeselni való, hiszen csak így lehet megtanítani a felhasználókat az elektronikus adatokról való felelős gondolkodásra, ugyanakkor szolgáltatói oldalon is előmozdítani a nagyobb adatbiztonságot. (**José Manuel Maza Martin**, Judge of the Supreme Court, Barcelona)

A gyerekek online zaklatásáról szóló szekció előadóinak kivétel nélkül az volt a véleménye, hogy a jelenség kutatását interdiszciplinárissá kell tenni, hiszen önmagában, empirikus kutatások nélkül sem a jogalkotó, sem pedig a jogalkalmazó nem értheti meg a jelenséget. (**Richard de Mulder**, Erasmus University Rotterdam; **Isidro Ordás**, Investigationes Technologicas, Nacional de Policia; **Rubén Mora**, Unidad Central de Delitos Informaticos, Cos de Mossos d'Esquadra) Emellett a jogtudomány semmit nem érhet el az informatikai szakemberek segítsége nélkül – a cselekmények monitorozásában, felderítésében, nyomozásában és szabályozásában sem. A gyermekek online zaklatása különböző megnyilvánulási formái a kortárs online kiközösítés (bullying), a zaklatás, a becserkészés (grooming), valamint a szexuális abúzus. Az Európa Tanács 2007-ben elfogadott Lanzarote egyezménye[5] ösztönzi a tagállamokat az online gyermekabúzus előkészületi cselekményeinek sui generis büntetendővé tételére. (Hasonló ajánlásokat tett az Európai Parlament és a Tanács 2010. szeptember 6-án publikált tervezetében.)[6] Ennek nyomán a gyermekekkel való online kapcsolatfelvétel szexuális visszaélés céljából önálló bűncselekményi tényállásként 2010-ben bekerült a spanyol Btk-ba. Az online kiközösítés (bullying) még mindig kisebb mértékű, mint hagyományos, offline változata, ám sokkal veszélyesebb. Az online kiközösítés elkövetési eszköze lehet a mobiltelefon vagy az online jelenidejű beszélgetőcsatornák (pl. Skype, MSN, Facebook chat, Google chat stb.), amelyek

[4] Az elektronikus fizetőeszközre vonatkozó európai egységes szabályozást l.: Directive 2007/64/EC of the European Parliament and the Council of 13 November 2007 on payment services in the internal market, amending Directives 97/7/EC,2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, *OJ L.* 319, 5 December 2007.

[5] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse CETS No.: 201 (2007.10.25. Lanzarote)

[6] 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 (2010/0064 (COD) Brussels, 6 September 2010)

gyakorlatilag a nap 24 órájában, folyamatos kontaktot biztosítanak az áldozathoz. Az áldozat sehol sem talál menedéket, az állandó megfigyelés érzete miatt sehol nem érezheti magát biztonságban, háborítatlanul. Éppen ezért, habár ritkább, hatása súlyosabb. Az online becserkészés (grooming) gyorsan terjedő eszköze a Poison Ivy. A Poison Ivy olyan trójai program, amelynek segítségével a támadó átveszi az irányítást a gyerek számítógépe (mobiltelefonja, iPad-ja stb.) felett, adatokat gyűjt róla, vagy zsarolással ráveheti további személyes adatok átadására, ezzel komoly lelki sebeket okozva. Az online abúzus különböző megnyilvánulási formáival szemben a legmegbízhatóbb védekezés a célszemélyek felvilágosítása. A katalán belügyminisztériumban az iskolai felvilágosító programok hatásvizsgálata jelenleg folyamatban van. (**Rubén Mora**, Unidad Central de Delitos Informaticos, Cos de Mossos d'Esquadra)

Hivatkozott irodalom

Asch, S. (1956) *Studies of independence and comformity: A minority of one against a unanimous majority,* In: Psychological Monographs, 1956 Vol. 70 No. 9, Whole No. 416

Durkheim, E. (1912) [1965] *The Elementary Forms of Religious Life,* New York: Free Press

Hirschi, T. (1969) *Causes of Delinquency,* University of California Press

Moitra, S.D. (2010) A Risk Analysis Model for Internet Security Management for Organizations, In: Bellini, M., Brunst, P. & Jähnke, J. (Eds.): *Current Issues in IT Security. Proceedings of the interdisciplinary conference 12-14 May, 2009* Berlin: Duncker & Humblot pp. 141-9

Merton, R. (2002) [1938] Social structure and anomy. *American Sociology Review* Vol. 3 No. 3. pp. 672-82

Parti K. (2009) *Gyermekpornográfia az interneten,* Bíbor Kiadó: Miskolc

Thevenoz, L. (1990) *Error and fraud in wholesale Funds Transfers. UCC Article 4A and the Uncitral Harmonization Process,* Zürich: Schulthess

Ulmer, E. (1938) *Das Recht der Wertpapiere,* Stuttgart: Rothhammer

Wilson, J.Q. & Kelling, G.L. (1982) *Broken windows: The police and neighborhood safety,* Elérhető a Manhattan Institute honlapján: http://www.manhattan-institute.org/pdf/_atlantic_monthly-broken_windows.pdf

Budapest, 2010. november 10.

Dr. Parti Katalin
tud. fmts.
Bűnözéskutatási Osztály