Parti Katalin

ÚTI JELENTÉS

INHOPE / INSAFE Central Regional Meeting

Bled, Szlovénia
2010. március 25-26.

Előzmények

A Magyar Tartalomipari Szövetség (MATISZ) mint az INHOPE / INSAFE elnevezésű, biztonságos internetezés elősegítéséért felelős nemzetközi szövetség tagja 2010 februárjában felkért arra, hogy vegyek részt az INHOPE / INSAFE közép-európai regionális találkozóján, amelyre 2010. március 25-26-án kerül sor, a szlovéniai Bledben.

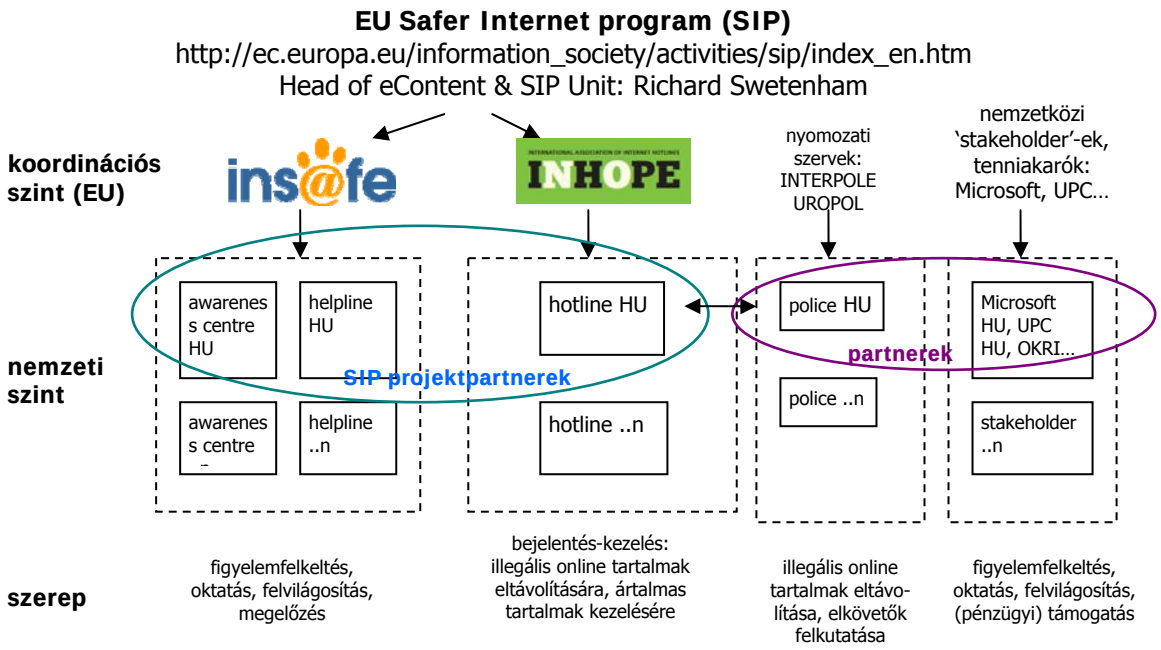
Az internetes illegális és káros tartalmak kezelésével kapcsolatban felmerült kérdésekben az OKRI a MATISZ konzulense 2009 óta. A MATISZ támogatja az Országos Kriminológiai Intézet biztonságos internetezéssel és internetes felderítéssel kapcsolatos szakmai rendezvényeit, amilyen pl. a 2010. február 12-én megtartott „Infolabor – Elektronikus bizonyítékszerzés helye és szerepe a jogérvényesítésben" című, jogalkalmazóknak szóló konferencia is volt. A MATISZ tevékenysége és az említett INHOPE / INSAFE tanácskozás témája szervesen kapcsolódik az Országos Kriminológiai Intézet 2009-ben indított, gyermekek online szexuális abúzusa tárgyában folytatott kutatásához. A találkozón való részvétel különböző nézetek megismerésére és eszmecserére adott lehetőséget a téma kutatóival és az online illegális tartalmak ellen küzdő internetes forródrótok képviselőivel.

Mit jelent az INHOPE és az INSAFE?

Az INHOPE és az INSAFE olyan nemzetközi szervezetek, amelyek az Európai Bizottság a Biztonságosabb Internet Program[1] keretében hozott létre és finanszíroz. Az INHOPE az illegális és káros internetes tartalmak bejelentésére szolgáló online bejelentőhelyek (*hotline*) tevékenységét fogja össze 1999 óta, míg az INSAFE a biztonságosabb internetezést segélyvonalak (*helpline*) és ismeretterjesztő weboldalak (*awareness node*) közös ernyő alá vonásával, koordinálásával biztosítja. A magyar *hotline* üzemeltetője 2005 óta a MATISZ, a *helpline* és az *awareness node* feladatokat pedig a Kék Vonal Gyermekkrízis Alapítvány, a Puskás Tivadar Közalapítvány, valamint a Nemzetközi Gyermekmentő Szolgálat megosztva látja el. Az INHOPE és az INSAFE standard szabályokkal igyekszik egységesíteni és átláthatóbbá tenni az ernyőszervezetek alá tartozó tagszervezetek tevékenységét. (1. ábra)

[1] A programról részletesen lásd: http://ec.europa.eu/information_society/activities/sip/index_en.htm

1. ábra: Az INHOPE és az INSAFE horizontális és vertikális szervezeti ábrája



Forrás: MATISZ, Safer Internet Day, 2010. február 9.

Miért regionális és miért kombinált konferencia?

A Biztonságosabb Internet Program un. kombinált (combined node) projektek megvalósítását támogatja, amelyekben együtt van a *hotline*, a *helpline* és az *awareness raising* szervezet. E program keretében adódott lehetőség 2009-ben Magyarországon a Nemzetközi Gyermekmentő Szolgálat, a MATISZ, a Kék Vonal és a Puskás Tivadar Közalapítvány CERT-Hungary Központ részvételével a magyar biztonságosabb internet kombinált projekt megvalósítására.[2] A kombinált projektek alapja az, hogy a három szervezet eredményesebben képes munkáját végezni, ha összehangolja tevékenységét. Az Európai Bizottság azonban egyfelől világkongresszusokat, másfelől regionális találkozókat szervez a kombinált projektek résztvevői számára. A regionális projektek, amilyen a szóban forgó rendezvény is volt, a régiós sajátságok figyelembe vételével próbálják összehangolni a három szervezet tevékenységét és egyben megosztani a jó gyakorlatokat.

A résztvevők

A konferencián a három említett szervezet mellett szoftvergyártók, mobil- és internet-szolgáltatók, valamint tudományos kutatóintézetek, egyetemek is képviseltették magukat. A mobil- és internet-szolgáltatás manapság integrálja a biztonságos felhasználást szolgáló felszereléseket, valamint a biztonságos tartalmakat is. A kutatóintézetek és egyetemek egyfelől részt vesznek a tartalomszolgáltatók oktatásában,

[2] A magyar biztonságosabb internet kombinált projektről lásd még: http://www.gyermekmento.hu/sajto/

másrészt pedig a felhasználókat fenyegető online illegális és káros tartalmak feltérképezésében játszanak központi szerepet.

A konferencia főbb megállapításai

1. **Az awareness centerek és a helpline-ok beszámolójából,**[3] valamint Janice Richardson (az INSAFE kordinátora) előadásából kiderült, hogy a gyermekek biztonságos internet-használatát nem elég a középiskolában elkezdeni. A kutatások[4] szerint az internet-kapcsolattal rendelkező háztartásokban a gyerekek már igen korán, sokszor még az írás-olvasás elsajátítása előtt, 3-5 éves korban rendszeresen interneteznek. A többi mellett az OKRI kutatása[5] is megerősíti, hogy bár a magyar gyerekek mintegy 5-10 évvel később kezdték rendszeresen használni az internetet, mára felzárkóztak nyugat-európai társaikhoz és 90-95%-uk napi rendszerességgel használja az internetet. A felnőttek és a gyermekek digitális műveltsége között azonban még mindig széles a szakadék. Ez azt eredményezi, hogy a felnőttek nem készítik fel a fiatalokat az internet veszélyeire, mivel nem ismerik azokat. Az oktatásra vonatkozó fenti javaslatot a jelenlévő Richard Swetenham, az Európai Bizottság Biztonságos Internet Programfelelőse is üdvözölte.
2. A fiatalok internet-használati szokásait és kockázatait számos **kutatás** taglalja. Például Julia Davidson (Kingston University) kutatása, amely az online zaklatás (cyber bullying) és az online becserkészés (online grooming) jelenségét vizsgálja.[6] A kutatást, amelyben négy ország (Olaszország, Norvégia, Belgium, Egyesült Királyság) vesz részt a londoni székhelyű Child Exploitation and Online Protection Centre (CEOP) közreműködésével végzik. Az online zaklatás jelensége központi kérdés Nagy-Britanniában, ahol ez az etnikai támadások eszköze, és számos tinédzser öngyilkosságához vezetett. A kutatás szerint a 11-16 éves gyermekek harmadának volt már része ilyen zaklatásban. További kockázati forrás a személyes adatok, mint a saját fényképek, az e-mail cím és az iskola elérhetőségeinek online kiadása.
   Az említett kutatás egyik megállapítása, hogy a hatékony felvilágosításhoz fontos megérteni, hogyan gondolkodnak a gyerekek. Az internet távolító mechanizmusát jól szemlélteti, hogy a gyerekek két hetes rendszeres üzenetváltás után már „barátnak" tekintik az online megismert idegent. Ezek után megszűnik a veszélyérzet, a szükséges óvatosság, amely visszatartaná őket a fizikai kapcsolatteremtéstől.
   A hatékony védelem akadálya az is, hogy az „online" fogalmát a gyerekek a számítógépre szűkítik, pedig a mobiltelefonról, i-phone-ról stb. elérhető internet nem kevesebb rizikófaktort hordoz. A közösségépítő oldalakat (Facebook, MySpace stb.) a legtöbbször már ma is mobil eszközről érik el, ám ezeket az eszközöket nem azonosítják az iskolai felvilágosítás során már rögzült veszélyforrással.

[3] Finn, osztrák, szlovák, szlovén helpline-ok beszámolója.
[4] Livingstone, S. & Haddon, L. (2009). EU Kids Online, Final Report. London School of Economics and Political Science. Elérhető: http://www.lse.ac.uk/collections/EUKidsOnline/Reports/EUKidsOnlineFinalReport.pdf
[5] Fiatalok online szexuális abúzusa kutatás, OKRI & ESZTER Alapítvány, folyamatban.
[6] Young People's Online Experience. Davidson and Martellozzo, 2005; Davidson et al. 2009, 2010; Seto, 2009; Davidson, 2007; Quayle & Jones, 2009; Lee, 2008.

Davidson hangsúlyozta, hogy a fiatalok számára merőben más prevenciós stratégiák szükségesek, mert ez a korosztály – a veszélyérzet hiánya, illetve a kockázatkereső attitűd miatt – nem képes elkerülni a potenciális veszélyeket, legfeljebb azt jegyzi meg, hogyan reagálhat a már kialakult veszélyhelyzetben.
Az elkövetők között nem azok a veszélyesek, akik fizetnek az online tartalmakért, hanem akik nem teszik azonosíthatóvá magukat és esetleg rejtett fájlcserélő hálózatba is kapcsolódnak.
Julia Davidson kutatócsoportja az elkövetői típusok azonosításában együttműködik a CEOP-vel.

3. Az **online grooming** jelenségét, azaz a gyermekkel (18. életévet be nem töltött személy) fizikai szexuális visszaélés elkövetése céljából online kapcsolatteremtést az Európa Tanács és az Európai Bizottság is kiemelt kérdésként kezeli. Elsőként az Európa Tanács gyermekek szexuális kizsákmányolásáról szóló egyezménye (CETS No.: 201, Lanzarote, 2007. október 25.)[7] hívta fel a tagállamokat a magatartás sui generis büntetendővé tételére, majd 2009-ben az Európai Parlament (Roberta Angelilli rapportőr javaslata alapján) fogalmazta meg ugyanezt az elvárást a tagállamokhoz intézett felhívásában.[8] A javaslatokat tett követte: az online becserkészés jelensége mára sui generis büntetendő a következő országok jogában: Albánia, Dánia, Egyesült Királyság, Görögország, Hollandia, San Marino, Macedonia.
4. A **szoftvergyártók** (Anti-Piracy and Digital Crime for Microsoft, EMEA) ugyancsak bekapcsolódnak a biztonságos tartalom előállításába, illetve az online tartalom felhasználó által megadott szempontok szerinti szűrésébe. Ahogyan Laurent Masson előadásából kiderült, a Microsoft együttműködik az elveszett és kizsákmányolt gyermekek nemzetközi központjával (International Centre for Missing and Exploited Children – ICMEC) a jogszabály-javaslatok kidolgozásában. Olyan szoftvert (Child Exploitation Tracking System - CETS) fejlesztettek ki a nyomozó hatóság részére, amelyek lehetővé teszik az ügyek egységes vizsgálatát, a hatékony és gyors kommunikációt a nemzetközi ügyekben. A szoftvert jelenleg 11 ország nyomozó hatósága használja. Ugyancsak a Microsoft által kifejlesztett képfelismerő program a PhotoDNA, amely lehetővé teszi az online megjelenő képfájlok tematikus összegyűjtését, valamint az adatbázisban szereplő képek terjesztésének megakadályozását. Erre a speciális adatbázisra azért van szükség, mert ha látszatra ugyanolyanok is a képek, azok lehet, hogy technikailag nem egyeznek meg, így a letiltás ellenére mégiscsak fenn maradhatnak valamely weboldalon. A képazonosító szoftver *hashing* technológiával működik: ennek segítségével egyeztetik a képeket, hogy minden képet és az abból készített változatokat egyaránt eltávolíthassák az internetről. Az eszközt jelenleg *host* szolgáltatók használják arra, hogy a szerverükről saját maguk távolítsák el a képeket („kigyomlálás"). Fontos, hogy a szolgáltatók legálisan használhassák ezt az eszközt, hiszen ha a hatóságok nem ismerik el, akkor ez monitorozásnak minősül, amit egy szolgáltató sem tehet meg jogszerűen. Az eszköz általános elfogadtatásán még dolgoznak, illetve úgy tűnik, hogy minden országban külön kell kijárniuk a PhotoDNA használatát a *hostoknak*. A Microsoft tervei között

[7] Az egyezmény teljes szövege elérhető: http://conventions.coe.int/treaty/Commun/QueVoulezVous.asp?NT=201&CM=8&DF=06/04/2010&CL=ENG
[8] INI/2008/2144 : 03/02/2009 – EP: non-legislative resolution. Elérhető: http://europarl.europa.eu/oeil/resume.jsp?id=5645632&eventId=1066152&backToCaller=NO&language=en

szerepel, hogy a szolgáltatók után a nyomozó hatóságok és maguk a hotline-ok is használják a képazonosító- és eltávolító eszközt.

Szintén a Microsoft számolt be egy új oktatási központ létrehozásáról, ez a *Cybercrime Centre of Excellence Network for Training*, *Research and Education* (2CENTER).[9] A center a következő kihívásokkal néz szembe:

- hónapról hónapra új technikai fejlesztések jelennek meg az interneten, amellyel nemcsak hogy lépést kell tartaniuk, de egységesen is kell oktatniuk a tréningen résztvevők számára;
- a tréningen résztvevő nyomozó hatóságok és egyéb szervezetek között alacsony szintű a párbeszéd, így a gyakorlatban megvalósíthatatlan az egységes fellépés;
- ha globálissá akarják tenni a tréninget, akkor az EU finanszírozási korlátaival kell szembenézniük, hiszen az EU nem tagállamok számára nem finanszírozza a tréning megtartását és a részvételt sem. Ugyanezzel a problémával néz szembe egyébként az INHOPE és az INSAFE is, az EU-n túli – dél-amerikai és kelet-európai – szervezeti bővítésnél, tudtuk meg az INHOPE tagsági koordinátorától, Adrian Dwyertől.

5. Az **illegális és káros internetes tartalmak egységes kezelése** központi kérdés. Erre jó példát szolgáltatnak a német internet-szolgáltatók erőfeszítései. Frank Ackermann, a német hotline (ECO)[10] szóvivője elmondta, hogy az eredetileg 2009 júniusában a német szövetségi parlament által elfogadott internet-blokkolási törvény mégsem lépett hatályba. A törvény kötelezte volna az internet-szolgáltatókat a szerverükön átfutó azon illegális tartalmak hozzáférhetetlenné tételére, amelyek szerepelnek a német szövetségi nyomozóiroda (Bundeskriminalamt) által összeállított listában. Ez azonban nemcsak a szolgáltatók jogait sérti, de a megelőzni kívánt tartalmak szűrésére is alkalmatlan, mindazonáltal sérti az információhoz jutás szabadságát.
6. Tatjana Music a **szlovén rendőrség fiatalkorúak részlegének vezetője** elmondta, hogy bár a 24/7 forródrót kiépítését Szlovénia is vállalta,[11] de anyagi erőforrás hiányában a rendőrségi hotline a mai napig nem jött létre. A szlovén civil hotline ugyanakkor azért nem lehet tagja az INHOPE-nak, mert ehhez szükség lenne a rendőrséggel kötött együttműködési megállapodásra is, amely viszont munkaerőhiány miatt nem jött létre eddig. Ezzel szemben Nyugat-Európában (pl. Ausztria, Németország), ahol megvannak ezek a hiányzó erőforrások, kiterjedt hotline hálózat működik mind a rendőrségen belül, mind civil szervezetek üzemeltetésében – tudtuk meg a német és az osztrák hotline-ok képviselőitől. Ez a Kelet-Nyugat határvonal a civil hotline-ok és a rendőrség közti kommunikáció gyorsaságában is megmutatkozik. A civil hotline eljárása a következő: először megvizsgálja, hogy a bejelentett tartalom legális vagy illegális-e. Ha illegális, továbbítja azt a partner hotline-hoz (amennyiben a tartalom másik országban található szerveren fut) és a rendőrséghez. A rendőrség beszerzi a bizonyítékot és ezt visszajelentik a hotline-nak. Ez kb. 30-60 percen belül történik meg, ezzel szemben például a magyar rendőrség ugyanerre a sémára 1-3 hónap múlva ad visszajelzést.

[9] Részletesen lásd: http://www.2centre.eu/

[10] Részletesen lásd: http://www.eco.de/

[11] Az Európa Tanács számítástechnikai bűnözésről szóló egyezménye (CETS No.: 185, Budapest, 2001. november 23.) értelmében. Míg a cvil szervezetek által üzemeltetett hotline közvetlenül állampolgári bejelentéseket fogad és ad át a rendőrségnek, addig a számítástechnikai bűnözésről szóló egyezmény értelmében létrehozott rendőrségi hotline-ok a büntetőeljárás során a nemzetközi együttműködést szolgálják. A magyar rendőrségi forródrót üzemeltetője a Nemzetközi Bűnügyi Együttműködési Központ (NEBEK).

7. Táler Orsolya beszámolt a **magyar helpline, a Kék Vonal Gyermekkrízis Alapítvány**[12] tevékenységéről. A Kék Vonal 1993 óta létezik, 2009 óta tagja a Nemzetközi Gyermekmentő által elnyert Safer Internet Projektnek, amelyben a helpline feladatait látja el. Főleg tinédzserek keresik fel őket és a telefonos kapcsolatot veszik igénybe. Többnyire internetes zaklatással, online illegális és káros tartalmakkal szembesülés áldozataival foglalkoznak. Munkatársai önkéntesek, akiket pszichológiai teszt alapján választanak ki és a felkészítést speciális tréning biztosítja. Rendszeres szupervízióval, tesztekkel biztosítják, hogy az önkéntesek ne azért jelentkezzenek, hogy aztán visszaéljenek a gyerek helyzetével. Emellett minden helpline szolgáltatás anonim, a betelefonálónak nem kell megadnia semmiféle személyes adatot.
   A hívások monitorozása fontos lenne, bár ez jelenleg nem megoldott. Ennek nyomán lehetőség volna kiegészíteni, fejleszteni az önkéntesek tananyagát. Fontos lenne továbbá, hogy a tananyagokat az egyes helpline-ok kicseréljék egymással.
   A helpline az **illegális tartalomról szóló bejelentéseket** többféleképpen kezelheti. A magyar helpline a bejelentésről minden adatot átküld a hotline-nak, mert a gyereket nem kérhetik fel arra, hogy maga tegye meg a bejelentést. Éppen ezért a magyar helpline elkéri a gyerek személyes adatait és úgy továbbítja a kérést/bejelentést. Később törlik a gyerek adatait.
   Az osztrák, a német és a szlovák helpline gyakorlata ezzel szemben az, hogy rendesen a gyereknek kell megtennie a hotline-hoz a bejelentést, azt az önkéntes nem teheti meg helyette. Ezzel a gyermeknek nem kell felfednie személyes adatait a helpline felé, másfelől pedig így tudatosítják, hogy mi minősül ténylegesen illegális tartalomnak – amellyel a gyermekek általában nincsenek tisztában. Ugyanakkor, ha a gyermek közvetlenül fordul a hotline-hoz, és nem a helpline teszi meg helyette a bejelentést, úgy visszajelzést kaphat arról, hol tart az ügye (esetleg a hotline eljutatta azt a rendőrséghez, gondoskodott a tartalom eltávolításáról a szolgáltatónál stb.).
8. Az **Ifjúsági Panel (Youth Panel)** a fiatalokat a biztonságos internetezés témája köré szervező nemzetközi program, egyfajta kortárs-segítő mozgalom, amely szintén az Európai Parlament Biztonságosabb Internet Programja keretében indult az EU számos országában. Magyarországon a Kék Vonal szervezi a panel összejöveteleit. Félnapos workshopok keretében elbeszélgetnek a gyerekekről az internet-használat veszélyeiről és felkészítik az idősebbeket arra, hogyan segíthetnek a fiatalabb gyerekeknek. Az Ifjúsági Panelek céljára más országok – pl. Finnország, Ausztria, Németország – ifjúsági táborokat, vetélkedőket, találkozókat szerveznek.
   A konferencia keretében alkalmunk volt egy ilyen Ifjúsági Panel beszélgetés meghallgatására. A panel három tagja, három szlovén tinédzser beszélgetett a felmerült témákról. Javasolták, hogy a helpline legyen a keresőmotorok (pl. Google) egy lehetséges opciója vagy *bannere*, amelyre rákattintva könnyebben meg lehetne tenni az illegális tartalmakról a bejelentést. Ezzel a módszerrel valószínűleg több bejelentés is érkezne. A gyerekek megerősítették, hogy fiataloknak kell tanítaniuk fiatalokat, mert amit felnőtt mond az internetről, az sokszor nem hiteles.

[12] A Kék Vonalról lásd: http://www.kek-vonal.hu/index2.php?m=16

Ehhez hasonló kezdeményezés Magyarországon a MATISZ IT-mentor-képzése,[13] amelynek keretében az iskolákban az ügyesebb gyerekeket tanítják meg arra, hogyan segíthetnek társaiknak a biztonságos internetezésben. A gyerekek egyöntetű véleménye az volt, hogy nem tanulási körülmények között kell a biztonságos böngészést tanítani, hanem inkább játékkal kell összekötni.

dr. Parti Katalin
tud. mts.
Bűnözéskutatási Osztály
OKRI

[13] Az IT-mentor programról részletesen lásd:
http://itme.itmentor.hu/engine.php?startload=front&itme_itmentor_hu=dc107df4850994d0b473cc8fb9738d79