Parti Katalin

Úti jelentés

Beszámoló a *Cybercrime and Electronic Evidence* c. képzésről (Pozsony, 2009. március 23-26.)

A spanyol illetőségű Cybex az Európai Bizottság támogatásával 2009-ben és 2010-ben összesen 14 országban tart képzést jogalkalmazók – rendőrök, ügyészek és bírák –, valamint informatikai igazságügyi szakértők számára. Az Európa 11, és Latin-Amerika három országában megtartandó egyenként négy napos kurzus témája az interneten megjelenő bűncselekmények nyomozása során alkalmazandó elektronikai eszközök bemutatása, az elektronikus bizonyítékok hiteles rögzítése, archiválása és felhasználása a büntetőeljárásban, valamint a nemzetközi együttműködés elméleti és gyakorlati kérdései. 2009. március 22. és 27. között a pozsonyi ügyvédi kamarában megrendezett képzésen vettem részt. Az alábbiakban a kurzus három fő irányvonalából emelek ki néhány témát.

1. Az interneten megjelenő bűncselekmények nyomozása során alkalmazandó elektronikai eszközök bemutatása

Az interneten megjelenő bűncselekmények felderítése és nyomozása kihívást jelent a jogalkalmazók számára. Minden ügyben igazságügyi informatikai szakértőt (a továbbiakban szakértő) kell kirendelni, a jogalkalmazónak pedig értelmeznie kell a szakértői véleményt és azt fel kell tudni használni az eljárás során. Nemcsak megértenie kell, hanem egyszersmind megmagyaráznia a szakértői vélemény jelentését más jogalkalmazóknak – például az ügyésznek vagy a bírónak. A szakértőtől tudni kell kérdezni, hiszen a szakértő látja az ügyek lényegét (l. jéghegy-effektus, amikor az adathordozó vizsgálója látja az ügy 80%-át, a jogalkalmazó, aki csak nyomon követi az elemzést, csak a történések 20%-ának van tudatában). Éppen ezért a Cybex hangsúlyozza az informatikai irányban továbbképzett jogalkalmazók jelentőségét, akik ugyancsak a felszínt látják, de vannak elképzeléseik (a kriminalisztika ezt nevezi verzióknak) arról, hogy egyáltalában mi történhetett, milyen szempontok szerint kell vizsgálni az adathordozót.

A szakértő szerepe annál is hangsúlyosabb, minthogy az elektronika folyamatosan fejlődik, így csak folyamatos tanulással lehet lépést tartani az újonnan megjelenő eszközökkel. Elérkeztünk az informatikai szakértők specializálódásának idejéhez, amikor már nem mindenféle számítástechnikai munkára rendelhető ki egy bizonyos szakértő, hiszen egy kisebb területről rendelkezik megalapozott tudással, tapasztalattal.

2. Az elektronikus bizonyítékok hiteles rögzítése, archiválása és felhasználása a büntetőeljárásban

Az elektronikus bizonyíték büntetőeljárásbeli felhasználhatóságának követelményei a hiteles rögzítés és a hiteles archiválás. Elektronikus adatot úgy lehet megszerezni és egyben a fenti feltételeknek eleget tenni, hogy az adat hordozóját foglalják le. Az eredeti adathordózóval forenzikus munkát nem szabad végezni, csak az arról készített másolaton. A másolatnak hitelesnek kell lennie (hash kulcs jelentősége, sic!) és hűen tükröznie a lefoglaláskori állapotot, hiszen például az adathordozó megnyitása (a számítógép bekapcsolása és az operációs rendszer elindítása) is módosítja – újrarendezi, felülírja a törölt állományt, így azok bizonyítékként már nem használhatók fel. Kérdés, hogy hány darab ilyen hiteles másolatot és kinek kell készítenie az adathordozóról. A Cybex szerint kettőt, az egyiket maga a lefoglaló szerv, a másikat a szakértő készíti a neki átadott adathordozóról. A magyar gyakorlatban ez jelenleg nem így van. Ennek ellenére az ismert joggyakorlat szerint senki nem kérdőjelezte még meg a bizonyíték hitelességét.

A Cybex hangsúlyozza, hogy tilos elektronikus bizonyítékokat kontextus nélkül gyűjteni. Mindig több adatot kell gyűjteni, mint amiről úgy gondoljuk, hogy feltétlenül szükséges. Ennek egyik oka, hogy sok online művelet csak a megelőző és a sorrendben követő művelettel együtt értelmezhető. A másik ok, hogy a szándékos elkövetést kizárhatja az illegális tartalmak letöltését követő mozzanat, mint amilyen a tartalom azonnali törlése. Ugyanebből a logikából eredően óvakodni kell attól, hogy valamely online üzenetet csak a „lényegét tekintve” küldjünk meg a szakértőnek, mert az e-mail tartalma nem bizonyít semmit. Ahhoz, hogy megállapítható legyen, hogy az e-mali eredeti – ténylegesen elküldték, ki küldte, kinek, mikor, a címzett

megkapta-e stb. – a fejlécben szereplő adatok is szükségesek. Éppen ezért nemcsak környezetvédelmi megfontolások miatt tilos valamely elektronikus adatot kinyomtatni, hanem mert önmagában a papír semmit nem bizonyít.

A Cybex emellett azonban minden jogalkalmazót óva int a fölösleges számítástechnikai eszközök (l. externális adathordozók, printer stb.) lefoglalásától. A sok adathordozó egyben több munkát, tárolási gondot és anyagi ráfordítást igényel. Nem beszélve az üzletvitel szabadságáról, amely a szükségtelen lefoglalás következtében sérülhet – például valamely bűncselekménnyel kapcsolatba hozható szerver lefoglalása a tulajdonostól nem indokolt, hogyha az adatok kimenthetők és az eredeti adathordozó pedig megőriztethető a tulajdonossal.

3. A nemzetközi együttműködés elméleti és gyakorlati kérdései

Az interneten megjelenő bűnözés nem ismer határokat, ezért sokszor kell külföldi hatóságot megkeresni valamely, az elkövetőt azonosító adat kiadása érdekében. Azonban az elkövetőt sokszor nehéz megtalálni, majd pedig az elkövető letartóztatása (házkutatás tartása, az adatok internet-szolgáltatótól való bekérése) is nehézségekbe ütközik a nemzetközi színtéren. Ezekben az ügyekben elektronikus adathordozókat kell lefoglalni, ill. az adat tárolóját kell adatrögzítésre és megőrzésre kötelezni. A problémát az eltérő jogi környezet okozza, amelyben az együttműködő felek közti kommunikáció lassú, illetve eltérő jogszabályi környezet mellett nem eredményes. Ennek eklatáns példái a távoli földrészeken található szerverek. A 2001. november 23-án Budapesten aláírt számítástechnikai bűnözésről szóló Európa tanácsi egyezmény, később az Európai Unió tagállamaira vonatkozó, a hírközlési hálózatokban keletkezett adatok tárolásáról szóló 2006/24/EK irányelv hiába kötelezi az internet-szolgáltatókat arra, hogy megkeresésre rögzítsék és meghatározott ideig meg is őrizzék, majd át is adják az ügyféladatokat, hiszen a latin-amerikai és ázsiai országok szerver-gazdái nem is válaszolnak az ilyen megkeresésekre. A másik oldalon pedig éppen amiatt érezheti biztonságban adatforgalmát a bűncselekmény elkövetője, mivel például Brazíliában vagy Indiában még kiforratlan az együttműködés gyakorlata, így a szervergazda nem adja át a keresett adatot, ha egyáltalán megőrzi azokat.

Az Európai Unióban a koordinációt az Eurojust, valamint az Europol látja el. Az Europolnak azonban nincs ártalmas internet-tartalmak (pl. gyermekpornográfia) nyomozására vonatkozó munkafájlja, ami viszont jelentősen megkönnyítené az együttműködést azzal, hogy automatizmusokat generálna a kapcsolattartás terén.

A tanfolyamon részt vevők nyomtatott tansegédletet kaptak, az utolsó napon elméleti és gyakorlati vizsgát tettek.

Budapest, 2009. április 1.

dr. Parti Katalin
tudományos munkatárs
Bűnözéskutatási Osztály
OKRI