DOI: 10.38146/BSZ.2015.9.3

SORBÁN KINGA

Informatikai bűncselekmények és nyomozásuk az Egyesült Királyságban

A számítógép, az internet és az elektronikus kommunikáció egyre növekvő szerepet tölt be mindannyiunk életében, általános, hogy internetet használunk otthon, a munkában, vagy az oktatási intézményekben. Olyannyira beférkőztek a mindennapi életünkbe, hogy már egyáltalán nem kelt feltűnést, ha egy átlagos felhasználó napja nagyjából a következők szerint néz ki: A reggeli kávé mellett a táblagépen elolvassa a híreket, majd elindul dolgozni, út közben a kedvenc zeneszámait hallgatva a telefonról. A munkába érve első dolga bekapcsolni a számítógépet, és gyakorlatilag a munkaidő végéig fel sem áll mellőle, talán csak akkor, amikor a futár meghozza az interneten megrendelt ebédet. A munkaidő végén még gyorsan megnézi a térképen, hogy hol lesz az esti találkozó a barátokkal, mikor jön a busz, és a legjobb útvonalat elmenti az okostelefon térképalkalmazásában (ha esetleg út közben mégis eltévedne, a GPS segítségével odatalál). Otthon még gyorsan megrendel pár ajándékot közeli rokona közelgő születésnapjára (természetesen bankkártya vagy PayPal segítségével gyorsan ki is fizeti).

A kibertérben azonban számos veszély is leselkedik a felhasználókra, a technológia kényelmes és könnyű hozzáférhetősége ugyanis a bűnelkövetők számára is sok új, kiaknázható lehetőséget kínál.

Az Egyesült Királyság az elmúlt tíz évben az egyik vezető szereplője lett a világ digitális (főleg a televízió- és a mobiltelefon-) piacának. A 2009-ben kiadott *Digital Britain Report*ban[1] a brit kormány elkötelezte magát az egyetemes széles sávú szabvány kialakítása mellett, a Home Access (otthoni hozzáférés) program és más hasonló kezdeményezések keretében pedig kiállt amellett, hogy minden brit állampolgárnak legyen internet-hozzáférése. A jelentés kiemelte, a kormány kívánalma, hogy az Egyesült Királyság gazdasága kiaknázza az internet minden hasznát, és a lakosság igénybe vehesse az általa kínált szolgáltatásokat.

1 Digital Britain. Final Report. June 2009.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228844/7650.pdf

A Home Office[2] által 2010-ben megjelentetett *Cyber Crime Strategy*[3] (kiberbűnözési stratégia) szerint, Európában az Egyesült Királyság vezet az internetes piac nagysága tekintetében; 2008-ban az online kiskereskedelmi forgalom negyvennyolcmillió font (kb. tizenkilencmilliárd forint) volt. Ugyanebben az évben az Egyesült Királyságban ötvenhét százalékkal több magánember rendelt magánhasználatra termékeket, illetve szolgáltatásokat az interneten, mint az előző évben. Az említett adatok ellenére a brit internetfelhasználók közül háromból egy nem vásárol online, ennek a fő oka az internettel kapcsolatos bizalmatlanság. A felhasználók a bizalmatlanság okaként említik a félelmüket a személyes biztonságuk miatt, és az interneten árusító vállalatok iránti ellenérzéseiket. A kiberbűncselekmények csökkentik a fogyasztók bizalmát, aminek magas lehet az ára: a hitelkártyacsalásokból eredő veszteség, amikor is a fogyasztó kártyáját úgy használták, hogy ő maga nem volt jelen, 328 millió font volt 2008-ban (ez tizenhárom százalékos növekedés az előző évhez képest), és a gazdaság éves veszteségének becsült összege az online rendelt kiszállítatlan termékek miatt ötvenötmillió font.

Mik az informatikai bűncselekmények?

E tanulmány szempontjából döntő fontosságú a fogalmak tisztázása, hiszen még manapság sincs általánosan elfogadott, egységes fogalmuk a számítógéppel kapcsolatos bűncselekményeknek. Az említett bűncselekményi kör leírására mind a magyar, mind a külföldi szakirodalom különböző fogalmakat használ úgymint: informatikai bűncselekmény, számítógépes bűncselekmény, kiberbűncselekmény, e-crime/e-bűncselekmény, netbűncselekmény. Sok esetben ezek a fogalmak egy tanulmányon belül is egymás szinonimáiként jelennek meg, holott – amellett, hogy mind ugyanarra a jelenségre irányulnak – bizonyos elemeikben eltérnek egymástól, e miatt fontos a következetes használatuk.

– *Számítógépes bűncselekmény (computer crime) vagy kiberbűncselekmény (cybercrime):* a számítógépes bűnözés, valamint a kiberbűncselekmény lényegében szinonim fogalmak, minden olyan bűncselekményt magukban

2 A belügyminisztérium brit megfelelője.

3 Cyber Crime Strategy. Home Office, March 2010. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

foglalnak, amelyekben megjelenik számítógép és/vagy a számítógépes hálózat.

– *Informatikai bűncselekmény (IT crime):* az informatikai bűncselekményeket sok helyen azonosítják az előbbi fogalmakkal, de ez nem teljes mértékben helytálló. Az eltérés oka a számítástechnika *(computing),* valamint az informatika *(information technology)* fogalmának eltérésében keresendő, ugyanis míg az előbbit akként határozhatjuk meg, mint az automatizált adatfeldolgozás eszközeivel és azok különböző területeken való használatával (például a számítógép építése és azok programozása) foglalkozó elméleti és alkalmazott műszaki tudományt, addig az utóbbi azokkal a számítógépekkel és telekommunikációs eszközökkel foglalkozó tudomány, amely az információ keletkezését, továbbítását, feldolgozását és hasznosítását vizsgálja. Az informatika tehát tágabb fogalom, hiszen a számítógépek mellett magában foglalja a televíziót, a rádiót, a telefonokat is.
– *E(lektronikus)-bűncselekmény (e-crime):* az e-bűncselekmény a legtöbb országban lényegében az informatikai bűncselekményekkel szinonim fogalom. Az ok, amiért itt külön tárgyaljuk, az, hogy az Egyesült Királyságban az e-crime fogalmat kettős értelemben használják: sokszor kifejezetten azokat az antiszociális viselkedésformákat értik rajta, amelyeket az elkövetők az interneten vagy a mobiltelefonon tanúsítanak (például cyberbullying, internetes zaklatás)[4]. A Rendőrfőnökök Egyesületének *(Association of Chief Police Officers)* e-crime-stratégiája szerint azonban e-crime a *„hálózatba kötött számítógépek vagy az internet használata bűncselekmények elkövetésére, vagy a bűncselekmény elkövetésének megkönnyítésére”*[5].
– *Internetes bűncselekmény (netcrime):* azok a számítógéppel kapcsolatos bűncselekmények tartoznak ide, amelyeket az internet kihasználásával követtek el.

A tanulmány a továbbiakban az informatikai bűncselekmény fogalmat használja. Ennek a fő oka, hogy a technológia folyamatos fejlődése következtében már nem egyértelmű, mi tartozik a számítógépek körébe, hol van a határ az egyes eszközök között, hiszen tudunk a televíziónkon keresztül internetezni, az okostelefonunkon televíziót nézni és az asztali számítógépünkkel telefonálni. Felépítését és funkcióit tekintve az okostelefon, az okostelevízió és az egyéb „okos” eszközök ugyanúgy nevezhetők számítógépnek, mint te-

4 http://www.ecrime-action.co.uk/what-is-ecrime.html

5 House of Commons Home Affairs Committee E-crime Fifth Report of Session 2013–14, p. 5. http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf

lekommunikációs eszköznek. Éppen ezért mind a számítógépes bűncselekmény, mind az informatikai bűncselekmény fogalmának használata helytálló lehet, az egyértelműség kedvéért azonban a továbbiakban a számítógépes bűncselekmény fogalmat csak a szűk értelemben vett számítógép (PC, laptop) ellen vagy által elkövetett bűncselekmények esetében használjuk.

Milyen deliktumok tartoznak az informatikai bűncselekmények körébe az Egyesült Királyságban?

A brit jogrendszer az informatikai bűncselekmények két fajtáját különbözteti meg: új deliktumok, amelyeket új technológiákkal követnek el, mint az információs rendszer és adatok elleni bűncselekmények, amelyekkel a számítógépes visszaélésekről szóló törvény *(Computer Misuse Act, 1990)* foglalkozik *(cyber-dependent crimes[6]),* valamint régi típusú bűncselekmények, amelyeket új technológiákkal követnek el, mert a hálózatba kötött számítógépek és más eszközök elősegítik a bűncselekmény elkövetését *(cyber-enabled crimes[7])*.

Az Egyesült Királyság jogrendszerének egyik különlegessége, hogy nincs egységes szerkezetbe foglalt büntető törvénykönyve. Az egyes bűncselekmények vagy bűncselekménycsoportok külön törvényekben találhatók meg, amelyek anyagi és eljárásjogi szabályokat egyaránt tartalmaznak, illetve vannak olyan deliktumok, amelyeket teljes mértékben a *common law,* a bírói gyakorlat szabályoz. Utóbbi kategóriát jól példázza az emberölés tényállása, amelynek a büntetendősége nem jelenik meg írott törvényben, csak a kiszabható büntetési tétel. Szerencsére a XX. századtól már egyértelmű a hajlandóság a bűncselekmények kodifikálására, ezért az informatikai bűncselekmények, illetve az e deliktumokkal foglalkozó rendelkezések több törvényben is megjelennek, amelyek közül a következők a legfontosabbak:

– a számítógépes visszaélésekről szóló 1990-es törvény *(Computer Misuse Act),* amelyet a rendőrségről és az igazságszolgáltatásról szóló törvény *(Police and Justice Act)* módosított 2006-ban, valamint a
– a csalásról szóló 2006-os törvény *(Fraud Act)*.

6 Mike McGuire – Samantha Dowling: Cyber crime: A review of the evidence. Research Report 75. Chapter 1: Cyber-dependent crimes. Home Office, October 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf

7 Mike McGuire – Samantha Dowling: Cyber crime: A review of the evidence. Research Report 75. Chapter 2: Cyber-enabled crimes – fraud and theft. Home Office, October 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Az informatikai bűncselekményeket érintik a következő törvények is:

– A büntetőeljárásról szóló törvény *(Proceeds of Crime Act, 2002)*;
– A terrorizmusellenességről, bűnözésről és biztonságról szóló törvény *(Anti-terrorism, Crime and Security Act, 2001)*;
– A hamisításról szóló törvény *(Forgery and Counterfeiting Act, 1981)*;
– A gyermekek védelméről szóló törvény *(The Protection of Children Act, 1978)*;
– A büntető igazságszolgáltatásról szóló törvény *(The Criminal Justice Act, 1988)*;
– A büntető igazságszolgáltatásról és a közrendről szóló törvény *(Criminal Justice and Public Order Act, 1994)*;
– A közrendről szóló törvény *(The Public Order Act, 1986)*;
– Az adatvédelemről szóló törvény *(Data Protection Act, 1998)*;
– A kommunikációról szóló törvény *(Communications Act; 2003*).

A számítógép-függő bűncselekmények

A számítógép-függő (vagy tisztán informatikai) bűncselekmények *(cyber-dependent crimes)* olyan deliktumok, amelyeket csak számítógéppel, számítógépes hálózattal, vagy egyéb infokommunikációs technológia felhasználásával lehet elkövetni. Ezek a cselekmények főképp számítógépek vagy hálózati erőforrások ellen irányulnak, noha a támadás következtében másodlagos hatások is megjelenhetnek. A számítógép-függő bűncselekmények két fő típusba sorolhatók:

a) tiltott behatolás egy számítógépbe vagy számítógépes hálózatba, ilyen például a hackelés; valamint
b) a számítógép működésének, illetve a hálózati kapacitásnak a megzavarása lerontása, utóbbira alkalmasak a különféle malware-ek vagy a DDoS-támadások.

A számítógép-függő bűncselekményeket a *Computer Misuse Act* tartalmazza, ezt indokolt bővebben tárgyalni[8].

A törvényt 1990-ben fogadták el, napjainkig többször módosult, legutóbb 2006-ban módosította a rendőrségről és az igazságszolgáltatásról szóló törvény *(Police and Justice Act).* A brit törvényekre jellemzően vegyesen tartal-

8 A fordítás alapjául a következő tanulmányt használtam: Egyesült Királyság. Törvény a számítógépes visszaélésről [1990] és részletek a törvényjavaslat parlamenti vitájából. In: Informatika–Jog–Közigazgatás. Nemzetközi dokumentumok IV. InfoFilia, Budapest, 1992.

maz anyagi és eljárásjogi szabályokat[9]. A törvény a számítógépes bűncselekmények körében összesen négy tényállást különböztet meg.
Az első a jogosulatlan hozzáférés számítógépen tárolt adatokhoz. E szerint:

(1) Bűncselekményt követ el az a személy, aki
   a) a számítógépet azzal a szándékkal használja, hogy egy számítógépen tárolt bármely programhoz vagy adathoz hozzáférést biztosítson, illetve hogy elősegítse a hozzáférés biztosítását;
   b) az a hozzáférés, amelynek a biztosítására a szándéka irányul, vagy amelynek a biztosítását elősegíti illetéktelen; és
   c) az elkövető a számítógép használatakor tudja, hogy a hozzáférésre nem jogosult.

A törvényjavaslat parlamenti vitája kifejti, hogy ebben az esetben a törvény célja az elrettentés a szándékos illetéktelen hozzáféréstől, vagy annak kísérletétől, ezt a deliktumot gyakran számítógépes betörésnek (hackelés) nevezik. Az előbbi tényállás kulcseleme a szándék, a törvényjavaslat parlamenti vitájában *Michael Colvin,* a javaslat előterjesztője ugyanis azzal érvel, hogy *„helytelen lenne arra törekedni, hogy rajtakapjuk azt a személyt, aki hozzáférést biztosít pusztán azért, mert figyelmetlen, hozzá nem értő, gondatlan, vagy nincs kellően tájékoztatva illetékességének korlátairól”*[10]. A szándék fontosságát a Rendőrfőnökök Egyesületének elektronikus bizonyítékokról szóló útmutatója is kiemeli, amikor úgy fogalmaz, hogy az ilyen bűncselekmények esetében két dolgot kell bizonyítani: azt, hogy a hozzáférés jogosulatlanul történt, valamint azt, hogy a gyanúsítottnak erről tudomása van.

(2) Ahhoz, hogy a bűncselekmény megvalósuljon, az elkövetésre irányuló szándéknak nem kell közvetlenül
   a) konkrét programra vagy adatokra;
   b) konkrét program- vagy adatfajtákra;
   c) az adott számítógépben tárolt programra vagy adatokra irányulnia.

(3) Az a személy, aki a fenti cselekményben bűnös
   a) Angliában és Walesben egyszerűsített eljárás alapján tizenkét hónapot meg nem haladó szabadságvesztés-büntetéssel, a törvényi maximumot meg nem haladó pénzbüntetéssel, vagy mindkettővel;

9 Computer Misuse Act (1990). http://www.legislation.gov.uk/ukpga/1990/18/contents

10 Egyesült Királyság. Törvény a számítógépes visszaélésről [1990] és részletek a törvényjavaslat parlamenti vitájából. In: Informatika–Jog–Közigazgatás. Nemzetközi dokumentumok IV. InfoFilia, Budapest, 1992, 24.10. o.

b) Skóciában egyszerűsített eljárás alapján hat hónapot meg nem haladó szabadságvesztés-büntetéssel, a törvényi maximumot meg nem haladó pénzbüntetéssel, vagy mindkettővel;
c) Bűnvádi eljárásban két évet meg nem haladó szabadságvesztés-büntetéssel, pénzbírsággal vagy mindkettővel

büntetendő.

A második a jogosulatlan hozzáférés további bűncselekmények elkövetésének vagy elősegítésének szándékával.

(1) Bűncselekményt követ el az a személy, aki az 1. §-ba tartozó bűncselekményt azzal a szándékkal követi el, hogy
a) Olyan bűncselekményt kövessen el, amelyre ez a szakasz vonatkozik, vagy
b) bűncselekmény elkövetését (saját maga vagy más személy számára) elősegítse,

amennyiben az elkövetni vagy elősegíteni szándékozott bűncselekmény e paragrafus (2) bekezdése értelmében további bűncselekménynek minősül.

A bűncselekményt ebben az esetben ugyanúgy követik el, mint az első szakaszban, de azzal a céllal, hogy további bűncselekményt kövessenek el, vagy elősegítsék egy további bűncselekmény megvalósulását. A további bűncselekmény ebben az esetben jelenthet például csalást vagy zsarolást. Colvin szerint *„ha arra használom a számítógépet, hogy információhoz jussak valaki zsarolása céljából, bűncselekményt követtem el, még mielőtt a zsaroló levelet elküldtem volna”*[11].

(2) Az (1) bekezdés alapján további bűncselekménynek minősülnek azok a bűncselekmények,
a) amelyekre törvény büntetést állapít meg, vagy
b) amelyek huszonegyedik életévét betöltött, vagy idősebb (Angliában és Walesben a 18 éves) elkövető esetében öt évig terjedő szabadságvesztéssel is sújtható [vagy Angliában és Walesben a városi bíróságokról szóló törvény *(Magistrates' Courts Act, 1980)* 33. szakasza által felállított korlátozásokkal ítélhető el].

11 Uo.

(3) E szakasz vonatkozásában lényegtelen, hogy a további bűncselekmény elkövetése ugyanabban az időpontban történt-e, mint a jogosulatlan hozzáférés, vagy bármikor azután.

(4) E paragrafus értelmében a bűncselekmény elkövetése akkor is megállapítható, ha a körülmények folytán a további bűncselekmény elkövetése nem lehetséges.

A Rendőrfőnökök Egyesületének elektronikus bizonyítékokról szóló ajánlása szerint amennyiben nem sikerül bizonyítani a további bűncselekmény elkövetésére irányuló szándékot, az 1. szakaszban meghatározott deliktum valósul meg.

(5) Az a személy, aki a fenti cselekményben bűnös,

a) Angliában és Walesben egyszerűsített eljárás alapján tizenkét hónapot meg nem haladó szabadságvesztés-büntetéssel, a törvényi maximumot meg nem haladó pénzbüntetéssel, vagy mindkettővel;

b) Skóciában egyszerűsített eljárás alapján hat hónapot meg nem haladó szabadságvesztés-büntetéssel, a törvényi maximumot meg nem haladó pénzbüntetéssel, vagy mindkettővel;

c) Bűnvádi eljárásban öt évet meg nem haladó szabadságvesztés-büntetéssel, pénzbírsággal vagy mindkettővel

büntetendő.

A harmadik paragrafusba azok az illetéktelen cselekmények tartoznak, amelyeket a számítógép működésének akadályozásának szándékával követtek el, valamint azok a gondatlanságból elkövetett cselekmények, amelyek akadályozzák a számítógép működését.

(1) Bűncselekményt követ el az a személy, aki

a) egy számítógéppel kapcsolatban illetéktelen cselekményt hajt végre;

b) az elkövetés időpontjában tudja, hogy a cselekményre nem jogosult; és

c) ezen paragrafus (2) vagy (3) bekezdése alkalmazandó.

(2) Ez a szakasz alkalmazandó, amennyiben az elkövető szándéka a cselekményével

a) akadályozni a számítógép működését;

b) megnehezíteni vagy megakadályozni a számítógépen tárolt programhoz vagy adatokhoz való hozzáférést;

c) veszélyeztetni bármely fenti célra szolgáló program működését vagy az adatok megbízhatóságát;

d) lehetővé tenni bármely a)–c) pontba tartozó cselekmény elkövetését.

(3) Ez a szakasz alkalmazandó akkor is, ha az elkövetőt gondatlanság terheli annak megállapításában, hogy a cselekedete alkalmas-e a (2) bekezdés a)–d) pontjában nevesített hatások kiváltására.
(4) A (2) bekezdésben nevesített szándékosságnak, illetve a (3) bekezdésben nevesített gondatlanságnak nem kell kapcsolódnia
  a) egy meghatározott számítógéphez;
  b) meghatározott programokhoz vagy adatokhoz;
  c) meghatározott program- vagy adatfajtákhoz.
(5) E szakasz szerint
  a) a cselekmény elkövetésének minősül a cselekmény elkövetésének a kiváltása is;
  b) a „cselekmény" kifejezés magában foglalja a cselekmények sorozatát;
  c) a megakadályozásra, megnehezítésre, veszélyeztetésre utaló kifejezések magukban foglalják a helyzet ideiglenes fennállását.
(6) Az a személy, aki a fenti cselekményben bűnös,
  a) Angliában és Walesben egyszerűsített eljárás alapján tizenkét hónapot meg nem haladó szabadságvesztés-büntetéssel, a törvényi maximumot meg nem haladó pénzbüntetéssel, vagy mindkettővel;
  b) Skóciában egyszerűsített eljárás alapján hat hónapot meg nem haladó szabadságvesztés-büntetéssel, a törvényi maximumot meg nem haladó pénzbüntetéssel, vagy mindkettővel;
  c) Bűnvádi eljárásban tíz évet meg nem haladó szabadságvesztés-büntetéssel, pénzbírsággal vagy mindkettővel
  büntetendő.

A törvény parlamenti vitája szerint ennek a szakasznak a célja a „megfoghatatlan tulajdon", például az adatok védelme. Ez a deliktum nem terjed ki a számítógépben vagy a mágneslemezben okozott fizikai kárra, kiterjed viszont olyan cselekvési formákra, mint a törlés, vagy olyan lemezek forgalomba hozatalára, amelyeket vírussal fertőztek meg, azzal a céllal, hogy a számítógépet megrongálják.

3A) Az 1. vagy a 3. szakaszokban meghatározott bűncselekmény elkövetéséhez használt eszköz készítése, kínálata, megszerzése szakasz csak 2006-ban került a törvénybe, a rendőrségről és az igazságszolgáltatásról szóló törvény iktatta be.
(1) Bűncselekményt követ el az a személy, aki az 1. vagy a 3. szakaszokban meghatározott bűncselekmények elkövetéséhez vagy elkövetésének előse-

gítéséhez használt tárgyat készít, átalakít, forgalomba hoz, illetve a forgalomba hozatalát felkínálja.

(2) Bűncselekményt követ el az a személy, aki olyan eszközt hoz forgalomba vagy kínálja fel a forgalomba hozatalát, amelyet valószínűsíthetően az 1. vagy 3. szakaszokban meghatározott bűncselekmények elkövetéséhez, vagy elkövetés elősegítéséhez használnak.

(3) Bűncselekményt követ el az a személy, aki azzal a szándékkal szerez meg valamely eszközt, hogy az 1. vagy 3. szakaszokban meghatározott bűncselekmények elkövetésére, vagy az elkövetésük megkönnyítésére kínálja fel.

(4) E paragrafus alapján „eszköznek" minősül az elektronikus formában tárolt program és adat.

(5) Az a személy, aki a fenti cselekményben bűnös,

a) Angliában és Walesben egyszerűsített eljárás alapján tizenkét hónapot meg nem haladó szabadságvesztés-büntetéssel, a törvényi maximumot meg nem haladó pénzbüntetéssel, vagy mindkettővel;

b) Skóciában egyszerűsített eljárás alapján hat hónapot meg nem haladó szabadságvesztés-büntetéssel, a törvényi maximumot meg nem haladó pénzbüntetéssel, vagy mindkettővel;

c) Bűnvádi eljárásban két évet meg nem haladó szabadságvesztés büntetéssel, pénzbírsággal vagy mindkettővel

büntetendő.

A számítógép által lehetővé tett bűncselekmények

A számítógép által lehetővé tett bűncselekmények *(cyber-enabled crimes)* tradicionális deliktumok, a számítógép-függő bűncselekményekkel ellentétben ezek infokommunikációs technológiák felhasználása nélkül is elkövethetők. A legsűrűbben előforduló számítógép által lehetővé tett bűncselekmények:

– a tiltott pornográf felvétellel való visszaélés;
– a gyűlölet-bűncselekmények;
– a zaklatás;
– a pénzügyi jellegű bűncselekmények, mint az online csalás, személyazonossággal való visszaélés; valamint
– a szellemi tulajdon elleni bűncselekmények.

Mely hatóságok járnak el az informatikai bűncselekmények nyomozásában?

Rendvédelmi szervek az Egyesült Királyságban[12]

A rendvédelmi szervek rendszere az Egyesült Királyságban meglehetősen komplex. A komplexitás egyik oka az Egyesült Királyság decentralizálódott közigazgatási rendszerében keresendő, ugyanis Skócia, Wales és Észak-Írország bizonyos szintű jogalkotási, közigazgatási, illetve pénzügyi autonómiát élvez, ezért van az, hogy a skót rendőrség „szervezetileg és a jogi szabályozásban elkülönül". Észak-Írországban pedig *„a centralizált, militarizált rendőrség mellett a hadseregnek is jelentős szerep jut"*[13].
Négyféle rendvédelmi szervet különböztethetünk meg:

1. Önkormányzati rendőri szervek: 2013. április 1-jétől Angliában, Észak-Írországban, Skóciában és Walesben[14] összesen negyvenöt földrajzi alapon szervezett helyi rendőri egység van, amelyeket egy-egy rendőrkapitány *(chief constable)* vezet. Országos szervezetük 2015. április 1. előtt a Rendőrfőnökök Egyesülete *(Association of Chief Police Officers; ACPO)* volt, amely szakmai önkormányzatként működött, szervezetirányítási jogkör nélkül. 2015. április 1-jétől a Rendőrfőnökök Egyesületét felváltotta a Rendőrfőnökök Tanácsa *(National Police Chiefs' Council)*[15]. Angliában és Walesben (Nagy-Londonon kívül) mindegyik területi egység egy vagy több helyi önkormányzati területet *(county)* fed le. Skóciában a skóciai rendőrség *(Police of Scotland)* felelős a rendfenntartásért, Észak-Írországban pedig az Észak-írországi Rendőri Szolgálat *(Police Service of Northern Ireland). „A helyi rendőrség magában foglalja a közbiztonsági, a közlekedésrendészeti feladatokat, de ezek a szakterületek csak a belső munkamegosztásban különíthetők el."*[16] A helyi szinten működő rendőrségek szakmai felügyeletét 2012 óta a rendőrségi és bűnügyi biztosok *(Police and Crime*

12 A tanulmány e részének elkészítésekor Kozáry Andrea tanulmányra támaszkodtam. Kozáry Andrea: Nemzetközi összehasonlító szervezettan. Rendőrtiszti Főiskola, Budapest, 2008. http://rtk.uni-nke.hu/downloads/tanszekek/tarstud/tema/nemz_osszh_modsztan.pdf

13 Salgó László – Tóth László: Rendészet a jogállamban. Magyar Rendészet, 2004/1.

14 Association of Chief Police Officers – Policing in the UK: A Brief Guide. http://wyp-unison.org.uk/assets/2410 - ACPO - Policing in the UK.pdf

15 http://www.npcc.police.uk/About/AboutNPCC.aspx

16 Finszter Géza: Rendőrségek Európában (Nyugat-európai modellek). In: Balogh Ágnes – Hornyák Szabolcs (szerk.): Tanulmányok Erdősy Emil professzor 80. születésnapja tiszteletére. Studia Iuridica Auctoritate Universitatis Pécs Publicata 136., PTE Állam- és Jogtudományi Kar, Pécs, 2005, 145. o.

Commissioner) látják el. Területi alapon szerveződnek továbbá egyes regionális egységek, a központi autópálya-rendőrség *(Central Motorway Police Group)* és az északnyugati autópálya-rendőrség *(North West Motorway Police Group),* amelyek az autópályákkal kapcsolatos rendvédelmi feladatokat látják el.

2. Speciális rendőri szervek: több olyan rendvédelmi szerv is van, amelyek nincsenek meghatározott földrajzi területhez kötve, hanem országos szinten látnak el rendvédelmi feladatokat. Ilyen speciális egység a vasúti rendészet *(British Transport Police),* amely Angliában, Skóciában és Walesben gondoskodik a vasúti hálózatok védelméről, a civil nukleáris őrség *(Civil Nuclear Constabulary),* amely az erőművek, nukleáris anyagok védelmét látja el, valamint a honvédelmi minisztériumi rendőrség *(Ministry of Defense Police). „Angliában különlegesen nagy fordulatnak számít, hogy a provincializmust feladva az egyes kiemelt súlyú, bonyolult jogi megítélésű és nehezen felderíthető bűncselekmények leleplezésének eredményesebbé tétele érdekében centralizált országos hatáskörű bűnüldöző apparátusokat és információs központokat szerveztek."*[17]
3. Egyéb rendőri szervek: olyan rendőri szervek, amelyek régebbi jogszabályok, vagy a common law alapján jöttek létre, feladataik általában egy meghatározott területhez vagy tevékenységhez kötődnek, ilyenek a kikötőkben van a parkokban működő rendőrségek (például a doveri kikötői rendőrség[18]).
4. Rendőri szervnek nem minősülő rendvédelmi szervek: ebbe a kategóriába sorolható minden olyan szerv, amely nem tartozik a rendőri szervek közé, de rendvédelmi feladatokat lát el, és a dolgozói is gyakran rendőrtisztek. Ilyen rendvédelmi szervek a Nemzeti bűnügyi ügynökség *(National Crime Agency),* a határőrség *(Border Force),* vagy a brit adó- és vámhivatal *(Her Majesty's Revenue and Customs).*

Az informatikai bűncselekmények nyomozásában eljáró hatóságok

Az informatikai bűncselekmények nyomozása számos kérdést vet fel az Egyesült Királyságban is. Ilyen például az, hogy a rendőrtiszteknek milyen mértékben kell részt venniük az igazságügyi szakértői tevékenységben, illetve egyáltalán részt kell-e venniük ilyesmiben. Szintén ilyen kérdés, hogy

17 Finszter Géza: Rendőrségek a XXI. században. Belügyi Szemle, 2000/1., 64–74. o.
18 http://www.doverport.co.uk/about/police/

van-e értelme kiszervezni a technikai jellegű vizsgálatokat magánkézben lévő vállalatokhoz, hogy a közbeszerzési eljárással pénzt spóroljanak, vagy az igazságügyi szakértői tevékenységet a rendvédelmi szervezetrendszeren belül kellene szervezni. Problémákat vet fel az informatikai bűncselekmények sokszínűsége és komplexitása is: teljesen más típusú fellépést igényel egy szervezett bűnözői csoport által végrehajtott hitelkártyacsalás-sorozat és a tiltott pornográf felvételekkel kapcsolatos bűncselekmények nyomozása. Az említett okok következtében a rendvédelem struktúrája folyamatosan változik az adott politikai, stratégiai irányvonalnak megfelelően, és elmondható, hogy az informatikai bűncselekmények nyomozásában részt vevő szervek rendszere korántsem mutat egységes képet. Az előbbi ok miatt indokoltnak tartom röviden áttekinteni az informatikai bűncselekmények nyomozásában részt vevő szervek történetét, mielőtt rátérnék a jelenlegi szervezetrendszer ismertetésére.

Az első jelentős nemzeti szinten működő szerv, amelyet 2001-ben kifejezetten az informatikai bűncselekmények megfékezésére hoztak létre Angliában, Walesben és Észak-Írországban, a Nemzeti csúcstechnológiás bűnözés elleni egység *(National Hi-Tech Crime Unit; NHTCU)* volt. A központi szerv munkáját negyvenhárom helyi szinten működő egység, az úgynevezett csúcstechnológiás bűnözés elleni egységek *(Hi-tech Crime Unit)* segítették.

Az NHTCU 2006-ban beolvadt a Súlyos szervezett bűnözés elleni ügynökségbe *(Serious Organised Crime Agency; SOCA),* ezzel azonban rés keletkezett az informatikai bűncselekmények elleni harc nemzeti szintjén. Ennek következtében csökkent az informatikai bűncselekmények megelőzésére való koncentráció, az erőforrások koordinációja, és az olyan nagy volumenű informatikai bűncselekmények nyomozására való alkalmasság, amelyek nem tartoztak a SOCA hatáskörébe. A SOCA e-crime egységének a megbízatása arra terjedt ki, hogy mérsékelje az online szervezett bűnözés okozta károkat, kezelje a technológia által lehetővé tett szervezett bűnözésből eredő veszélyeket, illetve csökkentse az internethasználat és információs hálózatok szerepét a bűncselekmények elkövetésében. További feladata volt, hogy arra használja az internetet, hogy információt szerezzen a komoly szervezett bűnözésről.

2008 áprilisában az informatikai bűncselekmények fontosságának növekedése miatt az Rendőrfőnökök Egyesülete megalkotta az e-crime portfóliót a Fővárosi Rendőri Szolgálat *(Metropolitan Police Service; MPS)* vezetése alatt. Ugyanezen év szeptemberében a Home Office bejelentette, hogy három éven keresztül három és fél millió font támogatást ad a Központi e-crime

egység *(Police Central e-crime Unit; PCeU)* felállítására a Fővárosi Rendőri Szolgálaton belül, hogy vezető szereplője legyen az informatikai bűncselekmények elleni harcnak. Az Fővárosi Rendőri Szolgálat beolvasztotta a már létező számítógépes bűnözés elleni egységét *(Computer Crime Unit)* a Központi e-crime egységbe, és további 3,9 millió font támogatást adott. A Központi e-crime egység fő feladata az informatikai bűncselekményekkel kapcsolatos képzési, eljárási, reagálási rend kialakítása, valamint a szervközi koordináció ellátása volt.

Az informatikai bűncselekmények nyomozásához kapcsolódó feladatot látott el korábban a gyermekek kizsákmányolása elleni, illetve a gyermekek online védelmét biztosító központ *(Child Exploitation and Online Protection Centre; CEOP),* amely 2006 áprilisában jött létre, azzal a céllal, hogy a megfelelő erőforrások birtokában hatékonyan kezelje a gyermekeket az online környezetben érintő szexuális bűnözők általi fenyegetést. Ez a szerv volt az Egyesült Királyság egyetlen kapcsolattartója a nemzetközi bűnüldöző szervekkel, ezen felül a gyermekek, a felnőttek és az ipari szereplők bejelentő központjaként működött, hogy jelenthessék a fiatalokat online fenyegető veszélyeket. A begyűjtött információt arra használják, hogy megállítsák az elkövetőket, és kármérséklő intézkedéseket vezessenek be, ezek magukban foglalják a gyermekek számára készülő oktatási anyagokat, a fiatalok és szüleik utógondozását, valamint azoknak a szakembereknek a képzését, akik az áldozatokkal dolgoznak.

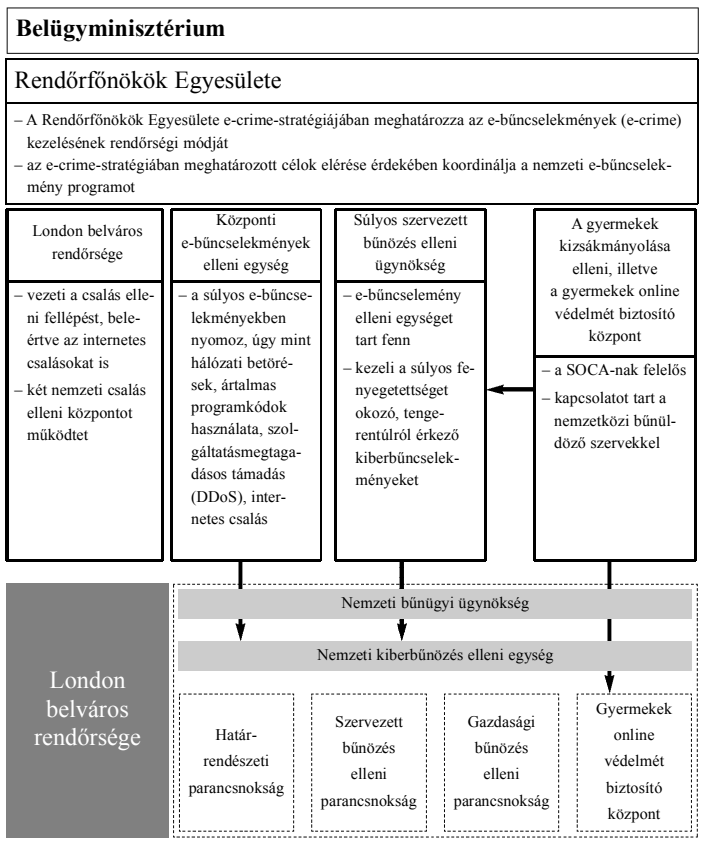
Az informatikai bűncselekmények nyomozása jelenleg megoszlik a helyi rendőri szervek, valamint a Nemzeti bűnügyi ügynökség *(National Crime Agency)* között.

A Nemzeti bűnügyi ügynökség 2013. október 7-én jött létre, országos szinten működő rendvédelmi szerv, amely a CEOP, a SOCA, valamint a PCeU összevonásával keletkezett. A feladatai közé tartozik a szervezett bűnözés, az ember-, fegyver- és drogcsempészet, az informatikai bűnözés, valamint a határon átnyúló gazdasági bűncselekmények nyomozása.

Jelenleg a Nemzeti bűnügyi ügynökségen belül a Nemzeti kiberbűnözés elleni egység *(National Cyber Crime Unit; NCCU)* foglalkozik az informatikai bűncselekményekkel. Ez a szervezeti egység a PCeU és a SOCA informatikai bűnözés elleni csoportjainak összevonásával keletkezett, a létrehozásának célja az volt, hogy egy olyan szakértői egység alakuljon, amely technikusokból, taktikai felderítő, valamint nyomozó csoportokból áll. A Nemzeti kiberbűnözés elleni egység vezeti azokat a nyomozásokat, amelyekben az informatikai elem dominál, és támogatja azokat a szerveket, amelyeknek a munkájuk

1. számú ábra

Az informatikai bűncselekmények nyomozását érintő szervezeti átalakulások[19]



19 Forrás: House of Commons Home Affairs Committee E-crime Fifth Report of Session 2013–14, p. 19. http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf

során digitális bizonyítékokkal kell foglalkozniuk. A szervezeti átalakulásokat a *1. számú ábra* illusztrálja.

A helyi szinten több rendőri szerv is szerepet kapott az informatikai bűncselekmények nyomozásában. Minden helyi rendőrségnél működik egy úgynevezett helyi csúcstechnológiás bűnözés elleni egység *(local hi-tech crime unit),* így van bizonyos kapacitásuk a merevlemezek és a hálózatok elemzésére, noha az utóbbi azokra a hálózatokra korlátozódik, amelyek az internethez hasonló TCP/IP protokollokat használnak. A kisebb rendőri szervekre jellemző, hogy regionális hálózatokat (hub) hoznak létre. Néhány egységnél a szakértők mind rendőrtisztek, máshol civileket alkalmaznak. Számos szakértő rendőrtiszt van, akik számottevő szaktudással bírnak, néhányuknak diplomája is van igazságügyi informatikából. Azonban vannak tisztek a helyi csúcstechnológiás bűnözés elleni egységeknél, akik csak rövid ideje dolgoznak ezen a területen, és csekély mértékű szakértői képzésben részesültek. A helyi szinten működő rendőrségek között kiemelt szerepet tölt be a Fővárosi Rendőrség *(Metropolitan Police),* valamint a London belváros rendőrsége *(City of London Police). „A Metropolitan Police – illetékessége ma Nagy-London egész területére kiterjed, kivéve a London City nevű városközpontot."*[20] A Fővárosi Rendőrségnek több olyan – részben elkülönülten működő – speciális egysége van, amelyek digitális bizonyítékokkal foglalkoznak, ezek: S015; Terrorizmus elleni parancsnokság *(Counter Terrorism Command);* valamint a Fővárosi Rendőrség gyermekvédelmi egysége.

Ezeken felül működtet egy civilekből álló, számítógépes rendszerek vizsgálatára szakosodott labort, amely számítógépeket, táblagépeket és mobiltelefonokat vizsgál.

Részben informatikai bűncselekményekkel foglalkozik London belváros rendőrsége, amelynek van egy külön egysége a csekk- és hitelkártyacsalások nyomozására *(Dedicated Cheque and Plastic Crime Unit*[21]*).* A szerzői jogi bűncselekmények nyomozására szintén külön egység működik London belváros rendőrségének berkein belül, a *Police Intellectual Property Crime Unit*[22].

20 Kozáry Andrea: i. m. 39. o.

21 http://www.financialfraudaction.org.uk/Police-The-dcpcu.asp

22 https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/default.aspx

A nyomozásokhoz szükséges szakértői háttér megteremtése

„Az Egyesült Királyságban a kriminalisztika mint tudományos fogalom nem terjedt el, a bűnügyi tudományok (forensic science) fogalmát részben a kontinentális kriminálтechnikával azonosították. Szakirodalmi források a »forenzikus» (bírósági, bűnügyi) jelzővel, azonos tartalommal használták a »scientific« (tudományos) jelölést."[23] Az igazságügyi szakértő *(forensic scientist)* megállapításait (amit a tudomány aktuális állásának megfelelő módszerek, eljárások alkalmazása táplál) vélemény formájában terjeszti elő. Hasznosulását, formáját tekintve tehát a bűnügyi tudomány „véleménytudomány", amelynek az érdemi sikerét az elfogadása adja. Egy „jó" igazságügyi szakértői vélemény tehát az általános és speciális kriminalisztikai ismeretekre támaszkodva, az adott ügyre vonatkoztatott megállapításokat tesz (kitérve annak esetleges egyedi jellegzetességeire), és felhasználva a megismeréselméletek következtetéseit, az aktuális jogkérdésekben releváns, megfogalmazásában logikus, világos, tárgyilagos és igaz következtetéseket tartalmaz, amelyek retorikájukban is alkalmasak a közöltek alátámasztására.[24]

Fontos megemlíteni, hogy az angol „forensic expert" kifejezés nem felel meg teljes mértékben a magyar fordításként használt „igazságügyi szakértő" elnevezésnek, hiszen tágabb személyi körre utal. Az Egyesült Királyságban ugyanis a „forensic expert" kifejezést használják a bűnügyi technikusokra, más néven a helyszínelőkre *(Scenes of Crime Officer),* akiknek a feladata a bűncselekmény helyszínén lévő bizonyítékok azonosítása és szakszerű összegyűjtése.

Az igazságügyi tudományok szerves részei a brit büntető igazságszolgáltatási rendszernek, és gyakran kulcsszerepet játszanak a büntetőeljárás során a bizonyítékok szolgáltatásában. 2005-ben az alsóház *(House of Commons)* tudomány és technológia bizottsága *(Science and Technology Commitee) Forensic Science on trial* (Bűnügyi tudomány a tárgyaláson) címmel jelentést adott ki a bűnügyi tudományokról[25]. A jelentés meghatározza az igazságügyi tudomány fogalmát, valamint felsorolja azokat a szervezeteket, amelyek a

23 Katona Géza: A kriminalisztika és a bűnügyi tudományok. BM Kiadó, Budapest, 2002, 39. o.

24 Angyal Miklós: Ismeretlen személyazonosságú holttestek kriminalisztikai és szakértői azonosítása. Doktori értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2014, 12. o., http://ajk.pte.hu/files/file/doktori-iskola/angyal-miklos/angyal-miklos-muhelyvita-ertekezes.pdf

25 House of Commons Science and Technology Committee: Forensic Science on trial. The Stationery Office Limited, London, 2005.
http://www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96i.pdf

nyomozástól az ítélethozatalig az igazságügyi szakértői tevékenységben részt vesznek. A jelentés igen tág módon definiálja az igazságügyi tudományokat: igazságügyi tudomány minden olyan tudomány, amely a jog szolgálatában áll. Ez magában foglalja az egyes tudományterületek teljes spektrumát az alapkutatástól egészen az alkalmazott technológiákig, így a kifejezés nemcsak azokra a szolgáltatásokra vonatkozik, amelyeket az igazságügyi szakértői szervezetek nyújtanak (például toxikológia, DNS-vizsgálat, lőfegyver, kábítószer, dokumentumok vizsgálata), hanem azokra a kutatásokra is, amelyek elősegítik az új igazságügyi technológiák kifejlesztését, tesztelését, bevezetését.

A szakértői háttérről a köz- és a magánszféra vegyesen gondoskodik: egyrészről a forenzikus szolgáltatásokat nyújtó vállalatok, másrészről pedig a brit rendőrség. A szakértők munkájának átlátásához ad segítséget a brit büntetőeljárást bemutató *2. számú ábra.*

Röviden összefoglalva tehát az igazságügyi szakértők alapvetően két ponton kapcsolódhatnak be az eljárásba: a helyszínen a bizonyítékok összegyűjtésekor, valamint a bizonyítékok elemzésekor. Az előbbi tevékenységet klasszikusan a rendőrség munkatársai, a helyszínelők végzik, utóbbit azonban többnyire – ám nem kizárólagosan – vállalatok alkalmazottaiként dolgozó szakértők végzik.

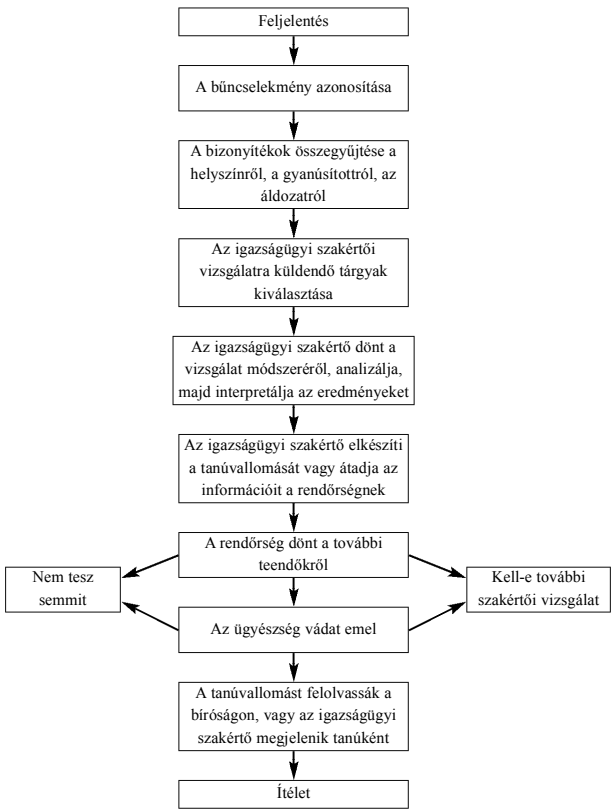
Az igazságügyi szolgáltatásokat Angliában és Walesben különböző cégek nyújtják piaci alapon. 2012 márciusáig a legnagyobb szolgáltató az állami tulajdonban álló *Forensic Science Service* (FSS) volt, ez biztosította az igazságügyi szolgáltatásokat a negyvenhárom helyi rendőrség, a koronaügyészség, valamint a brit adó- és vámhivatal részére. Hatvanszázalékos piaci dominanciája ellenére a cég nehezen tudott alkalmazkodni a folyamatosan változó környezethez, az évek során pedig folyamatosan csökkent a piaci részesedése, ezért a megszüntetéséről határoztak. Skóciának és Észak-Írországnak saját, közpénzből finanszírozott igazságügyi szolgáltatói vannak: a Skót Rendőrségi Szolgáltató Hatóság *(Scottish Police Services Authority)* alá tartozó Igazságügyi Szolgáltatások *(Forensic Services),* valamint az észak-írországi igazságügyi tudományokkal foglalkozó ügynökség *(Forensic Science Northern Ireland*[26]*).*

Szót kell még ejtenünk a rendőrségről, hiszen a rendőri szervezetrendszeren belül is több igazságügyi szakértő dolgozik: mind a negyvenhárom angliai és walesi helyi rendőrség alkalmaz tudományos tanácsadó munkatársakat *(Scientific Support Staff).* Az egyes munkakörök megnevezései egységenként

26 http://www.dojni.gov.uk/index/fsni/fsni-about.htm

2. számú ábra

Az igazságügyi szakértő a brit büntetőeljárásban[27]



27 Az eredeti ábra címe: The use of forensic science by the criminal justice system Forrás: House of Commons. Science... i. m. 11. o. http://www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96i.pdf

eltérők lehetnek, de általánosságban elmondható, hogy minden helyi rendőrségnél van egy vezető tudományos tanácsadó *(Scientific Support Manager)* és számos helyszínelő *(Scenes of Crime Officer)*. A vezető tudományos tanácsadók adminisztratív feladatot látnak el, ők koordinálják a helyszínelők munkáját, ellátják az igazságügyi tudományokkal kapcsolatos költségvetés kezelését, valamint elősegítik az igazságügyi tudományterületekre vonatkozó irányelvek fejlesztését a rendőrség szervezetén belül. Lehet tudományos, üzleti vagy rendőrségi hátterük, de közülük nagyon kevesen rendőrtisztek. A tényleges szakértői tevékenységet a helyszínelők végzik, ők azok, akik a bűncselekmény helyszínén DNS-maradványokat, ujjlenyomatokat, illetve más nyomokat keresnek és gyűjtenek. Komolyabb ügyekben ebbe a munkába a forenzikus szolgáltatásokat nyújtó vállalatok szakértőit is bevonják.

Összegzés

Az előbbiek alapján világos, hogy a britek már régóta foglalkoznak az informatikai bűncselekményekkel, ez idő alatt azonban náluk sem fejlődött ki olyan stabil szervezeti háttér, amely hatékonyan elláthatná az ilyen jellegű deliktumok nyomozását. Ha megfigyeljük az informatikai bűncselekmények nyomozásával foglalkozó rendőri szervek történetét, egyfajta útkeresést láthatunk, amit nagymértékben befolyásol az aktuálpolitikai helyzet. Figyelemre méltó azonban az a törekvés, hogy a digitális elemet tartalmazó bűncselekmények nyomozása a nemzeti szint mellett a helyi egységeknél is megjelenjen, illetve hatékonyan működjön.

Pozitívnak tekinthető az is, hogy a számítógépes visszaélésekről szóló törvényben nevesített deliktumok nagyjából követik az európai irányt, így a cybercrime egyezményben meghatározott deliktumok a brit jogrendszerben is bűncselekményeknek minősülnek. Ez azért kiemelkedő fontosságú, mert az informatikai bűncselekmények nagyon gyakran országhatáron átnyúló jellegűek, és az elkövetők felelősségre vonhatóságának egyik kulcseleme, hogy az informatikai bűncselekmények körébe tartozó deliktumok egész Európában egységes képet mutassanak. Ahogy *Parti Katalin* egyik tanulmányában rávilágít[28] az *„Internet legmarkánsabb tulajdonsága az államhatárok elhomályosítása az úgynevezett »láthatatlan zóna« jelleg”.* A kapcsolattartás a

28 Parti Katalin: Az internetes bűncselekmények nyomozásának egyes kérdései. In: Irk Ferenc (szerk.): Kriminológiai Tanulmányok 41. Országos Kriminológiai Intézet, Budapest, 2004, 257. o.

külföldi szolgáltatókkal, nyomozó hatóságokkal nehézkes, a hivatalos megkérés hosszú időt vesz igénybe, az információáramlás lassú, a külföldi online-hozzáférés-szolgáltató különféle okokból megtagadhatja az együttműködést, egyebek között azért, mert az adott országban a felhasználó cselekménye nem büntetendő.

IRODALOM

Angyal Miklós: Ismeretlen személyazonosságú holttestek kriminalisztikai és szakértői azonosítása. Doktori értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2014. http://ajk.pte.hu/files/file/doktori-iskola/angyal-miklos/angyal-miklos-muhelyvita-ertekezes.pdf

Finszter Géza: Rendőrségek a XXI. században. *Belügyi Szemle,* 2000/1.

Finszter Géza: Rendőrségek Európában (Nyugat-európai modellek). In: **Balogh Ágnes – Hornyák Szabolcs (szerk.):** Tanulmányok Erdősy Emil professzor 80. születésnapja tiszteletére. *Studia Iuridica Auctoritate Universitatis Pécs Publicata* 136., PTE Állam- és Jogtudományi Kar, Pécs, 2005, 129–156. o.

Katona Géza: A kriminalisztika és a bűnügyi tudományok. BM Kiadó, Budapest, 2002

Kozáry Andrea: Nemzetközi összehasonlító szervezettan. Rendőrtiszti Főiskola, Budapest, 2008. http://rtk.uni-nke.hu/downloads/tanszekek/tarstud/tema/nemz_osszh_modsztan.pdf

McGuire, Mike – Dowling, Samantha: Cyber crime: A review of the evidence. Research Report 75. Chapter 1: Cyber-dependent crimes. Home Office, October 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf

McGuire, Mike – Dowling, Samantha: Cyber crime: A review of the evidence. Research Report 75. Chapter 2: Cyber-enabled crimes – fraud and theft. Home Office, October 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Parti Katalin: Az internetes bűncselekmények nyomozásának egyes kérdései. In: **Irk Ferenc (szerk.):** Kriminológiai Tanulmányok 41. Országos Kriminológiai Intézet, Budapest, 2004, 249–275. o.

Salgó László – Tóth László: Rendészet a jogállamban. *Magyar Rendészet,* 2004/1.