JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

Eötvös Loránd Tudományegyetem

Állam és – Jogtudományi kar

Büntető Eljárásjogi és Büntetés-végrehajtási Jogi Tanszék

Szakdolgozat

Az online házkutatás helye és szükségessége a magyar büntetőeljárásban

Konzulens:

Dr. Mohácsi Barbara, PHD

és

Dr. Gazdag Tibor, megbízott óraadó

Romhány Gergely

jogász képzés

nappali tagozat

2010

Tartalom

Bevezetés

A virtuális házkutatás mint eszköz

2008. március 2. 11:19, Vasárnap – Sg.hu
Franciaország is online házkutatásokat tervez.

Svájc, Németország és Ausztria után egy újabb európai állam, Franciaország is komolyan fontolgatja az ilyen internetes akciók bevezetését.

Több ezer hitelkártya-adattal kereskedett

2008. május 20. 12:44, Kedd - Berta Sándor

Egy 19 éves schwerini fiatalembert azzal gyanúsítanak, hogy több mint 3600 személy hitelkártya-adatával élt vissza és ezeket az interneten is árulta.

Magyarország az internet-bűnözés első harmadában

2008. április 15. 15:46, Kedd - Forrás: MTI
Magyarország az internet-bűnözést illetően nyitott és fertőzött ország, s világszinten az első harmadba tartozik: a listán például 27. helyen áll a rosszindulatú robot-támadásokat illetően, azaz itt nagyon sok olyan számítógép található, amelyik automatikus támadással gyűjti a személyes adatokat.

Már volt online házkutatás Ausztriában

2008. március 7. 08:16, Péntek - Berta Sándor
A rögzített információkból kiderült, hogy Mohamed M. adatforgalmának 35 százaléka egy malájziai szerverhez irányult, amely segített az adatok elrejtésében. Mivel a nyomozók a kódolt anyagokat nem tudták megfejteni, ezért bevonták a munkába a "Megfigyelési

1984-ben Steven Levy megírta Hacker Etika címmel korszakalkotó művét, ezzel ismertetve meg a világgal a hacker szubkultúrát. Bár sokan valóban az ebben lefektetett alapelvek és eszmék szerint élnek, alakítják a hacker szubkultúra világát, igyekeznek moderálni, kontrollálni a valós-világ felé mutatott képet, az információs társadalom és szabadon fejleszthető számítógépes tudás rohamos növekedésével megjelenő új generációk már másképpen alkalmazzák a tudásukat. Természetszerűen várható volt, hogy előbb utóbb a szervezett bűnözés világa is felfedezi magának ezen szakemberek felhasználási módjait haszonszerzés illetőleg állami információs rendszerekbe való betöréssel adatok módosításának, manipulálásának céljából.

A White-Hat hacker és Black-Hat hacker kifejezések csupán ezen kultúra tagjai számára bírnak meghatározó jelentőséggel, mind a bűnözői csoportok mind a bűnüldöző szervek számára egységesen számítógépes rendszerbetörőket, illegális tartalom terjesztőket, illetőleg adatszerzőket jelentenek.

A büntető törvénykönyvben[1] már szabályozásra kerültek ezek a típusú bűncselekmények, de pusztán ezen cselekménye kriminalizálása kevés a hatékony megoldáshoz. Szükséges továbbá, hogy a büntető eljárásjog, különösen a nyomozási szakasz is igazodjon ezen bűncselekményekkel kapcsolatos speciális körülményekhez. Ez eljárásjogi kondíciók kialakításánál fontos szempont, hogy az segítse a bűnüldöző hatóságok munkáját, és mégis garanciát nyújtson az állampolgárok számára az Alkotmányban[2] és a büntetőeljárási jogban rögzített jogok védelmére.

Napjainkban elmondható, hogy az elektronikus eszközök használata megnehezíti a hatóságok hatékony munkavégzését, mert az információs technika számtalan lehetőséget teremt a kapcsolatfelvételre, kapcsolattartásra, bűncselekmények előkészítésére és végrehajtására. A törvényhozó ezért hozzáférhetővé teszi az információs technikai eszközöket a nyomozó hatóságok számára, a titkos beavatkozás lehetősége pedig még inkább lehetővé teszi a bűncselekmények hatékonyabb felderítését.

[1] 1978.évi IV. törvény a Büntető törvénykönyvről, továbbiakban Btk.

[2] 1949. évi XX. Törvény, a Magyar Köztársaság Alkotmánya, a továbbiakban: Alkotmány

Jelenlegi eljárásjogunkban nincsenek külön nevesített eszközök az ilyen típusú bűncselekmények hatékony felderítésére. Egy erre alkalmas nyomozási eszköz lehetne a közelmúltban kialakult és még folyamatosan formálódó online vagy más néven virtuális házkutatás. Dolgozatomban ennek az eszköznek a jelenlegi európai és magyar szabályozási környezetét, illetve lehetséges végrehajtását tekintem át, tekintettel a virtuális házkutatással érintett személyek jogi helyzetére.

I. Fejezet

Miért van szükség a virtuális házkutatásra mint nyomozási eszközre?

1.1. A büntetőeljárás válsága

A büntetőeljárás „ új kettős szorításban” [3]

Közismert, hogy a rendszerváltozás óta eltelt évtizedben Magyarországon körülbelül az ötszörösére – százezres nagyságrendről közel félmilliósra – növekedett az ismertté vált bűncselekmények száma. A nyomozások eredményessége 40%-ról mintegy 25%-ra csökkent, a büntetőperek megközelítőleg egyharmada egy éven túl is elhúzódik. A bűnüldöző és igazságügyi szervek túlterheltek. Egyfelől tehát a bűnözés robbanásszerűen megnövekedett. Ez a bűnözésnövekedés önmagában egy rendkívül nagy kihívás, szinte elviselhetetlenül nagy szorítás a büntető igazságszolgáltatással szemben.

Ami az „ új kettős szorítás” második elméletét illeti, közismert tény, hogy hazánkban a rendszerváltozással rohamléptekkel bontakozott ki a jogállam. Ezzel összefüggésben szükségszerűen került sor a nemzetközi emberi jogi dokumentumok, és általában a jogállamiság szerves részét képező egyéb egyezmények elfogadására, ratifikálására. Ez önmagában folyamatos és rendkívül kiterjedt jogharmonizációs szükséglettel, szorítással járt és jár.

[3] Tremmel Flórián: Magyar büntetőeljárás, 2001, Dialóg Campus Kiadó, 31. oldal

A büntetőeljárás „válságának” tehát a régi kettős szorításon túlmenően egy sajátosan és kivételesen új – magával a rendszerváltozással összefüggő – kettős kihívás van a hátterében, azaz a robbanásszerűen megnövekedett bűnözés és kampányszerűen felerősödött jogharmonizáció „új kettős szorítása”.[4]

Az Európa Tanács 1990-ben kiadott egy ajánlást a kriminalizálandó magatartásokról, ez útmutatóul szolgált a büntetőjog-alkotásban. Ez tulajdonképpen egy lista, ami összegzi az eddig ismert számítógépes deliktumokat. A lista a szankcionálandó cselekményeket sorolja fel:

- számítógépes csalás
- számítógépes hamisítás
- a számítógépes adatokban és programokban történő károkozás
- a számítógépes szabotázs
- a jogellenes behatolás
- a jogellenes titokszerzés
- a védett számítógépes programok jogellenes másolása
- a félvezető topográfiák jogellenes másolása

A fakultatív listán szereplő cselekmények:

- a számítógépes adatok
- a számítógépes kémkedés
- a számítógép jogellenes használata
- védett programok jogellenes használata[5]

„Garamvölgyi László rendőrségi szóvivő a Magyar Hírlapnak megerősítette, hogy az éves bűnügyi statisztikák jelentős tényezőjévé vált a tiltott pornográf felvételekkel való visszaélés bűntette. Az még nem büntetendő, ha valaki csupán megtekin*ti a felvételeket, de a Btk. szerint azzal szemben el kell járni, aki készíti, letölti, tárolja, publikálja, vagy kereskedik a fotókkal.”*

Az lehet, hogy büntetőpolitikai kérdés annak eldöntése, hogy mely bűncselekmények fokozottan üldözendőek, s melyek nem. Viszont ennek megfelelő eszközökkel is el kell látni az arra hivatott szerveket, hogy munkájukat hatékonyan tudják végezni.

[4] Tremmel Flórián: Magyar büntetőeljárás, 2001, Dialóg Campus Kiadó,41.-42. oldal

[5] Augusztinyi Krisztina: A számítástechnika felhasználásával megvalósuló bűncselekmények, Rendészeti Szemle, 56. évfolyam, 3. szám, 66.-77. oldalig

1.2. Internet és pedofília

Ilyen fokozottan üldözendő cselekmény napjainkban a pedofília. A nyomozó hatóságoknak mind több munkájuk akad az internetről letöltött kiskorúakat ábrázoló obszcén felvételek miatt. Míg 2003-ban nyolcvan ilyen jellegű bűncselekményről szereztek tudomást, egy évvel később már 5800 gyermekről készült felvételt foglaltak le a hatóságok. Tavaly pedig ez a szám is megduplázódott, meghaladta a tizenegy ezret.

A tízezer feletti szám azt jelenti, hogy ennyi gyermek szerepel a lefoglalt fotókon, videofelvételeken. Ilyenformán egy tetteshez, illetve eljáráshoz adott esetben több tucat, vagy akár több száz bűncselekmény is társítható.

> *„Tóth Ferenc alezredes, a Budapesti Rendőr-főkapitányság osztályvezetője azt mondta, hogy* tavaly 59 *nyomozás indult a fővárosban.* A *gyanúsítottak összesen 3500 bűncselekményt követtek el a fentebb említett tizenegyezerből.* A *rekordernek ezer gyermek képeit tartalmazó archívuma volt. A rendőrök főként külföldi jelzés alapján indítanak eljárást. Alig hat hónapja az* olasz *rendőrség jelezte, hogy huszonhét magyar* IP-*címről töltöttek le egy olasz pedofil honlapról képeket. Azóta már kaptak értesítést spanyol, német és a holland kollégáktól* is.
> *Az esetek többségében egyértelműen megállapítható, hogy az adott IP címen bejegyz*ett *számítógép hol található. A nyomozók ilyenkor megjelennek a helyszínen, házkutatást tartanak, lefoglalják a számítógépet és adathordozókat. Újabban a magánlakások mellett egyre többször kénytelenek felkeresni cégeket, hivatalokat, sőt állami intézmények*et *is.”*
> Gaál Zoltán: Pedofília: házkutatás már állami intézményeknél is, Magyar Hírlap Online, 2006.02.21.

A pedofilok zárkózott személyek, akik vágyaikkal nem léphetnek a nyilvánosság elé, így bűnös tevékenységüket titokban űzik. Az Internet elterjedésével ezek a személyek egy olyan kapcsolattartási eszközt kaptak, melynek előnyeit hamar felismerték és vágyaik titkos kiélésére fel is használják. Fenntartanak zárt levelező listákat, jelszóval védett honlapokat, melyeken keresztül kapcsolatot tarthatnak, illetve képeket, videókat küldhetnek egymásnak.

Egyes szervezett bűnözői csoportok is felismerték azt a lehetőséget, hogy a prostitúció ezen speciális alfaja segítségével még nagyobb anyagi haszonra lehet szert tenni, és ők is kihasználják az Internet adta anonimitást a kapcsolattartásra. A szexturizmus így könnyen és titokban megszervezhető, egyszerűbb érdeklődőket toborozni.

Hazánkban még leggyakrabban, ha internetes pedofíliáról beszélünk, akkor a tiltott pornográf felvétellel való visszaélést értjük alatta. A gyakorlatban ez azt jelenti, hogy az Interneten tesznek közzé olyan pornográf kép- vagy videó felvételeket, melyeken kiskorú személyek szerepelnek.

Sajnos az elmúlt időszakban egyre több ilyen bűncselekménnyel találkozunk. Ennyire megnőtt volna a pedofilok száma az elmúlt időszakban?

Véleményem szerint nem. Az elkövetők közt találhatók olyanok, aki úgymond csak polgár pukkasztásból készített ilyen honlapot, volt köztük olyan, aki bár szívesen nézegette, gyűjtögette az ilyen jellegű videókat, képeket, de ennél tovább soha sem ment, illetve olyan is, aki amellett, hogy ilyen képeket, videókat gyűjtött, cserélt, saját maga is készített tiltott pornográf felvételeket, illetve fajtalankodott gyermekkorúakkal.

A leginkább veszélyesnek azt az elkövetési magatartást találom, amikor tisztán anyagi haszonszerzésre használják fel a gyermekeket, és ezért készítenek róluk pornográf felvételeket. Akár gyermekek egymás közti szexuális játékairól, akár felnőtt részvételével.
A 90-es évek közepén egy vidéki kisvárosban, egy fényképész készített ilyen jellegű felvételeket tizenéves gyermekekről. Bűntársa egy tanítónő volt, aki szerepelt is a gyermekekkel a felvételeken. A tanítónőt a nyomozati anyagok alapján csak az anyagi haszonszerzés motiválta, míg a fényképész már volt korábban büntetve hasonló bűncselekmény miatt.
Az elmúlt időszakban felderített hasonló bűncselekmények közt találkozhatunk olyannal is, akiket szintén csak az anyagi haszonszerzés motivál. Ők a képek, videók tiltott jellegét használják ki, és az internetről gyűjtik be felvételeiket, majd azt összerendezve teszik fel egy-egy honlapra, melyet zárt körben hirdetnek, vagy CD-re kiírva árusítanak.
A pedofília mint szexuális aberráció jogi eszközökkel nem kezelhető, viszont a pusztán az anyagi haszonszerzés motiválta elkövetés és terjesztés megakadályozása, felderítése és elítélés létfontosságú kérdés a pedofília visszaszorításában.
A könnyű és gyors haszonszerzés lehetőségétől való elrettentés visszafogná az ilyen tartalmú weboldalak és képek terjedését, s csökkentené a kiskorúakkal szemben haszonszerzés okán és szexuális céllal elkövetett bűncselekmények számát.

Az Interneten a pedofil jellegű bűncselekmények közül a tartalomszolgáltatás körében elkövetett bűncselekmény a Btk. 195/A.§-ban meghatározott tiltott pornográf felvétellel való visszaélés a leggyakoribb. Ezt a törvényhelyet az 1997. évi LXXIII. törvény iktatta be a magyar jogrendbe a

nemzetközi szerződésekben foglalt kötelezettségeink alapján. Ilyenek a gyermekek jogairól szóló New York-i egyezmény, a Nemzetközi Munkaügyi Konferencia 1999. évi 87. ülésszakán elfogadott 192. egyezmény, valamint a 2001. novemberében Budapesten aláírt Számítástechnikai Bűnözésről Szóló Nemzetközi Egyezmény.

Azóta ezt a szabályozást többször változtatták, jelenlegi formája 2002. IV. 1-től hatályos. A jelenlegi szabályozás büntetni rendeli a kiskorú személyekről készült pornográf videó, film, vagy képfelvétel, illetőleg más módon előállított képfelvétel megszerzését, tartását, kínálását, átadását, készítését, forgalomba hozatalát, azzal való kereskedelmet, illetve nagy nyilvánosság számára hozzáférhetővé tételt.[6]

1.3. A gyanúsítotti kör meghatározása

A nyomozó hatóság munkáját nagyban megnehezítheti az internetes pedofil ügyekben, hogy a gyanúsítotti kör ismeretlen, vagy adott esetben túl széles. Előfordulhat például, hogy egy pedofil weboldalon nagy mennyiségű olyan személyes adatra lehet szert tenni, aminek alapján rendkívül sok személy gyanúsítható lenne pedofil képek tárolásával. A gyanú ilyen esetben nem alapos, így nem indítható büntetőeljárás. Megeshet ugyanis, hogy valaki más email címével regisztrál, ál-adatokat ad meg egy ilyen oldalon, illetőleg más személy internetkapcsolatát felhasználva tölt le és tárol pedofil tartalmú képeket.

Ál-adatok esetén a célszemély meghatározására vonatkozó cselekmények eredménytelenek lennének, amely a nyomozó hatóság munkájának jelentős akadályát jelentené. Ártatlan személyek gyanúba keveredése esetén pedig értelemszerűen szintén eredménytelen lenne a bizonyítási eljárás. A számítógéppel elkövetett bűncselekmények esetén a célszemély meghatározására technikailag van lehetőség. Ezen kívül, az online-házkutatás által megvalósított állami adatszerzés jelentős potenciált teremt az érintett személyiségének kifürkészésére. Az információs technikai rendszer komplex felhasználási lehetőségei következtében a célrendszer adatállománya az érintettre vonatkozó személyes adatokat, naplószerű feljegyzéseket, képeket, hangfelvételeket

[6] Dr. Peszleg Tibor r. őrnagy : Internet és pedofília, *Belügyi Szemle 2004. december*

tartalmazhat. Az adatok önmagukban vagy összességükben utalhatnak az érintett személy személyiségére, személyes életviszonyaira vagy életmódjára.[7]

A nyomozók feladata, hogy kiderítsék, ki töltötte le a képeket, videókat. Egy családon belül viszonylag könnyű kideríteni, ki nyomta meg az enter billentyűt, egy céges gépen esetében már két-három hónapig is eltarthat a beazonosítás.
A sértettek, vagyis a képen szereplő gyermekek többsége feltehetően külföldi. Ám akadt arra is sajnálatos példa, hogy Magyarországon készült fotókat foglaltak le, ilyenkor igyekeznek felkutatni a gyermekeket is. A bíróságok általában 60–100 ezer forint közötti összeggel büntetik azokat, akik csupán letöltötték a fotókat. Ám a készítők és kereskedők akár felfüggesztett börtönre is számíthatnak.

A számítógéppel elkövetett bűncselekmények esetén a nyomozó hatóság rendszerint a célszámítógép és személy ismertté válása után házkutatást rendel el a gyanúsított személy lakóhelyén, tartózkodási helyén, s az ott lévő adattároló egységeket, számítógépet, merevlemezt, egyéb adathordozókat lefoglalja. Ezt követően a lefoglalt tárgyakat átadják az erre kirendelt és szakosodott szakértőnek elemzés céljából, s jó esetben néhány hónappal később kiderül, volt e büntetőjogi tényállást kimerítő adat illetve az eljárás alapját képező, a feljelentést és lefoglalást megalapozó adat a számítógépen. Előfordulhat, hogy semmi érdemlegeset nem talál az elemzés, illetőleg kiderül, hogy téves következtetés és lefoglalás volt, ez felesleges használata az állománynak, s annak a személynek is felesleges tortúra annak a személynek is, akinek adattároló egységeit lefoglalták.

A Be. alapelvként és eljárási garanciaként kimondja, hogy a házkutatást, lefoglalást, a lehető legkörültekintőbben kell végezni, s a lehető legkevesebb sérelemmel és károkozással, a személyi jogok tiszteletben tartásával. Szükséges olyan jogintézmények illetőleg nyomozási eszközök kialakítása, ami a lehető legkisebb érdeksérelemmel jár az állampolgárok számára, és a nyomozó hatóságoknak is előnyös.

[7] 1 BvR 370, 595/07 vom 27. Februar 2008, 231, 232.

Különösen napjaink bűnelkövetési eszközei és módszerei szolgálták alapját annak, hogy az online házkutatás intézménye több nyugat-európai országban, így Svájcban, Németországban, Ausztriában, Franciaországban is nem csupán mint lehetőség és jövőbe mutató eljárási eszköz vetődött fel, hanem ezen országok közül többen is (pl. Németország,Ausztria, Franciaország) már jogszabály tervezetként tárgyalják, vagy már hatályba is lépett az ezt lehetővé tevő jogszabály.

1.4. A számítógépes adat mint bizonyítási eszköz

2001. november 21.-én Budapesten aláírták a Cyber Crime Convention egyezményt, ezzel egységesült a számítógépes bűncselekmények kriminalizálása. Az egyezmény nemzetközi jogi hátteret teremtett ezek üldözésének. Ezt követően megkezdődött a számítógéppel összefüggő bűncselekmények nemzeti büntető anyagi jogban való fejlődése, büntető tényállások kidolgozása. A büntető eljárásjog szempontjából ami újító és előremutató rendelkezése volt az egyezménynek, az a számítógépes adatok megőrzésére való kötelezettség. Bár az Eht.[8] már tartalmazott ilyen rendelkezést, fontos volt a büntető-eljárásjogi kodifikáció, amely megteremtette az alkalmazhatóság feltételeit.

Német kutatók kimutatták, hogy egy számítógépes adat „élettartama" az interneten átlagosan 5-6 nap. Ez adott esetben lehet kevesebb is, akár csak pár óra, jobb esetben akár néhány hónap. Az internet működési sajátosságaiból adódóan a nem használt adatok helytakarékossági okokból idővel felülíródnak. Átlagosan egy több országon átnyúló számítógépes nyomozás, célszemély meghatározás, IP címmel kapcsolatos adatok beszerzése s az előfizető meghatározása a jogsegélykérelmek és hosszas bürokratikus eljárások eredményeként akár fél évre is elnyúlhat. A német kutatók eredményei alapján egyértelmű, hogy a nemzetközi számítógépes bűncselekmények esetén mire eljutnánk nyomozási szakaszhoz, elveszhetnek a bűnjelek és az eljárás megindítását indokolttá tévő adatok.

A számítógépes adatok megőrzését lehetővé tevő rendelkezés azonban azt is eredményezi, hogy lehetőség nyílik az adatokat tároló egység lefoglalása helyett a megőrzés eszközével élve gyorsabban hozzájutni az esetleges bizonyítékként szolgáló adathoz.

[8] 2003. évi C. törvény az Elektronikus Hírközlésről

1.5. Mi a megoldás?

Az adatok megőrzése önmagában azonban még kevés. A számítógépes bűncselekmények, illetőleg a számítógép felhasználásával elkövetethető egyéb bűncselekmények (például csalás, rémhírterjesztés, rágalmazás, szomszédos jogok sérelme, stb.) adatai és nyomai akár néhány napon belül eltűnhetnek, illetőleg felderítésük az idő múlásával, sokkal nehezebbé vagy akár lehetetlenné válhat. Az ilyen cselekményeket elkövetőket az esetek jelentős részében magas fokú szakképzettség jellemzi, ami még nehezebbé teszi üldözésüket.

Így nem csupán az elkövetőkhöz hasonlóan szakképzett bűnüldözőkre van szükség, hanem olyan nyomozási eszközökre, eljárási eszközökre is, amelyek lépéselőnyhöz juttathatják a nyomozó hatóságokat a bűnelkövetőkkel szemben. Az elkövetési módszerekhez hasonlóan gyors eljárási és nyomozási eszközök szükségesek a hatékonyság növeléséhez. Ezzel nem áll szándékomban a bevált nyomozati eszközök és eljárások kritikáját adni, pusztán új nyomozási eszközök szükségességére hívnám fel a figyelmet, amely a megváltozott bűnelkövetési módszerekkel szemben hatékonyabb fellépést tehet lehetővé.

Azóta, hogy Steven Levy megírta Hacker etika című könyvét, 24 év telt el. Ez alatt a negyed évszázad alatt rohamos fejlődésnek indult az számítástechnika, az internet világa, s ennek folyományaként az ahhoz kapcsolódó, annak segítségével elkövetett bűncselekmények száma. Ez a tény szükségessé teszi, hogy a jogrendszer megfelelően reagáljon az új társadalmi, gazdasági jelenségekre.

II. fejezet

Az eljárás menete a gyakorlatban

2.1. Az adatgyűjtés fogalma, szerepe a nyomozásban[9]

A nyomozás – mint megismerési folyamat - adatokra támaszkodik. Az adatok beszerzése az egyszerű észleléstől kezdve a technikai eszközök, a tudományos vizsgálati eljárások alkalmazásáig sokféle módon történhet: az adott ügyre vonatkozó eljárási szabályok betartásával bármely adatforrás és adatszerzési mód felhasználható. A felderítésben és a bizonyításban fontos szerepük van a krimináltaktikában külön témaként nem tárgyalt rendőri intézkedésekhez, illetve egyes titkosszolgálati eszközökhöz és módszerekhez több pontos is kapcsolódó, a gyakorlatban mindig is széles körben alkalmazott krimináltaktikai adatgyűjtési módszereknek.

Az a gyakorlati tevékenység, ahogyan a nyomozás során az adott adatforrástól adathoz lehet jutni, mindig két mozzanatból áll: az alkalmazott módszerből, és annak jogi körülményeiből.

Egy-egy módszer többféle célt szolgálhat és többféle jogi környezetben is előfordulhat, pl. a környezettanulmány szerepet kaphat az államigazgatási eljárásban (lásd: körözés), a titkos információgyűjtésben, a büntetőeljárásban; irányulhat nyomozási cselekmény végrehajtásához, más adatgyűjtési módszer alkalmazásához vagy a nyomozás tervezéséhez-szervezéséhez szükséges adatok beszerzésére; emellett igen változatos adatforrásokra támaszkodhat.

Mivel egyáltalán nem mindegy, hogy az eredmény adat, információ vagy bizonyíték lesz, az aktuális célnak megfelelően kell megválasztani, hogy adott esetben melyik módszert milyen jogi keretek között alkalmazzuk.

[9] Krimináltaktika 1. 63. oldal, Budapest, 2001, Rejtjel kiadó, Rendőrtiszti főiskola

A nyomozási érdekkel legalább is egyenrangú szerepet játszik az állampolgári jogok tiszteletben tartása. Erre figyelemmel kap most jóval nagyobb szerepet a felderítés és a bizonyítás eszköz-és módszertárának megkülönböztetése.

Az alapvetően nem a jogszabályok által megfogalmazott kriminál taktikai adatgyűjtési módszerek tekintetében mindezek azzal a következménnyel járnak, hogy a korábbinál jóval pontosabban meg kell határozni, hogy mely adatgyűjtési forma, milyen körülmények között alkalmazható (milyen jogszabályokat kell figyelembe venni) és a beszerzett adatot mire lehet felhasználni és milyen formában kell rögzíteni.

2.2. Követés helye és a joghatóság

Ha hálózatban valósul meg a bűncselekmény, elképzelhető hogy egy magyar felhasználó egy Magyarország elleni támadást egy másik ország szerveréről vagy szervereinek hálózatán keresztül valósít meg.

Mivel az elkövetési magatartás egy mozzanata Magyarországon megvalósult, ezért a bűncselekmény elbírálására fennáll a magyar joghatóság.

2.3. A bizonyítási eszközök

A számítógép által vezérelt eszközök manipulálása természetesen elektronikai úton történhet, e manipulálás a legegyszerűbb módszertől (például impulzusgenerátor) a legbonyolultabbig (például programozott chip által vezérelt egyedik kapcsolás)[10] terjedhet. Ezért a helyszíni szemle folyamán, illetve a lefoglaláskor különös körültekintéssel kell vizsgálni, hogy mely tárgyak, illetve adathordozók lehetnek tárgyi bizonyítási eszközök.

[10] A hacker kultúrában és elkövetési eszközök között ismert egy úgynevezett VGA kártya, melybe un. behatolási pontot kereső programot integráltak, így jelentős mértékben felgyorsítva és hatékonyabbá téve a számítógépes rendszerbetörést. Bár egyes rendőrségi vélemények szerint ezen kártya létezése csak HOAX, városi legenda.

Egy átlagos kinézetű „mindennapos" kapcsolás „ártalmatlannak tűnhet, azonban részletes szakértői vizsgálat feltárhatja, hogy ez a parányi kapcsolás ténylegesen a bűncselekmény elkövetésének eszköze. A nyomozó hatóság a lefoglaláskor szembesül a „feketedoboz"-effektussal, vagyis hogy a nyomozó hatóság mindent lefoglal, amit talál, illetve relevánsnak ítél, majd később ezt vonja részletes szakértői vizsgálat alá.

Minden számítástechnikai úton rögzített adat bizonyítási eszköz, azonban ezen adatok megváltoztathatósága miatt fokozott figyelmet kell fordítani az adatok rögzítésére, a bizonyíték integritásának megőrzésére, a hitelesség garantálására. [11]

2.4. A bizonyítási eszközök biztosításának kérdése, a jogintézmény jelentősége és szabályozási köre

A számítástechnikai rendszerekbe bevitt és itt rögzített adatoknak akkora a jelentősége, mint az okiratokban vagy iratokban rögzített adatoknak. A törvényhozónak számolnia kellett ezzel a ténnyel és meg kellett határozni annak a technikáját, ahogyan az ilyen rendszerekben rögzített adatok a büntetőeljárásban szükség esetén a hatóságok számára is hozzáférhetővé válnak. Szerepük nyilvánvalóan elsősorban a bizonyítás területén igen jelentős, emellett azonban az eljárásban más szerep betöltésére is alkalmasak, például tájékoztatás szerezhető a gyanúsított vagy más személy hollétéről.[12]

A bíróság, az ügyész, valamint a nyomozó hatóság elrendeli annak a rögzített adatnak a megőrzését, amely bizonyítási eszközként szerepel, vagy a gyanúsított kilétének, tartózkodási helyének megállapításához szükséges.

A megőrzésre kötelezést elrendelő hatóság a megőrzéssel érintett adatot fokozott biztonságú elektronikus aláírással láthatja el.

Mivel a számítástechnikai adat bizonyíték jellege első pillantásra nem egyértelmű, ezért a bizonyíték felkutatása és rögzítése speciális szakértelmet igényelt és igényel.

[11] Augusztinyi Krisztina: A számítástechnika felhasználásával megvalósuló bűncselekmények, Rendészeti Szemle, 56. évfolyam, 3. szám, 66.-77. oldalig

[12] Király Tibor, Büntetőeljárási jog ,Osiris kiadó, Budapest, 2008, 333. oldal,

A szaktanácsadó szerepe ezekben az esetekben a büntetőeljárásról szóló törvény rendelkezéseivel összhangban a bizonyítékok felkutatását, azonosítását és rögzítését foglalja magában. A számítástechnikai úton rögzített informatikai bizonyítékok vizsgálata a szakértő feladata. A nyomozó hatóság azt a gyakorlatot is követheti, hogy ténylegesen a bizonyítékok felkutatására azt a szakértőt vonja be az eljárásba, akinek később feladata lesz a bizonyítékok kiértékelése és vizsgálata.

A számítástechnikai környezetben az adathordozót nem lehetséges az adatok fizikai szétválasztása (bizonyításra alkalmas, nem alkalmas), ezért a lefoglalás személyes, illetve gazdasági érdeket sérthet. Kialakult joggyakorlat van arra, hogy a cselekmény bizonyításához nem tartozó állományokat (fényképek, levelezés, házi videók) szakértő bevonásával lementik és a lefoglalást szenvedőnek átadják, de nincs törvényes lehetőség a másolt állományoknak a lefoglalt adathordozóról való törlésére.

A lefoglalt adathordozó integritásának megtartása alapvető garanciális követelmény, és az eljáró hatóságoknak, illetve a terheltnek is érdeke. Ezért a lefoglalt adathordozókon a nyomozó hatóság birtokába jutott személyes adatok kezelésének jogszerűsége alappal vitatható, noha a bizonyítás érdekében azokra szükség lehet.[13]

2.5. A virtuális házkutatás menete

Alapesetben, mikor a nyomozó hatóságnak bűncselekmény jut a tudomására, megindítják a büntetőeljárást. Számítógépes bűncselekmények esetén, illetőleg ha a bűncselekmény megvalósulásában bármilyen módon számítógépes adattárolás valósult meg vagy számítógépen illetőleg bármilyen adathordozón a bűncselekmény elkövetésére vonatkozó adat található, a nyomozó hatóság házkutatást rendel el a gyanúsított lakhelyén, illetőleg ott ahol a bizonyítékot tároló eszköz található, s azt lefoglalja.

[13] Augusztinyi Krisztina: A számítástechnika felhasználásával megvalósuló bűncselekmények, Rendészeti Szemle, 56. évfolyam, 3. szám, 66.-77. oldalig

A nyomozó hatóság, ha szükséges szakértő véleményét és segítségét kéri a tároló egységen található adatok megvizsgálása és kielemzése céljából, majd a megszerzett információk alapján folytatja a nyomozást, illetőleg ha elegendő az információ, továbbítja az ügyésznek vádemelés céljából.

A virtuális házkutatás több ponton is megegyezik a titkos adatszerzés, titkos információgyűjtés illetőleg a Be. által szabályozott házkutatás (titkos és nyílt) céljával és eredményének felhasználási módjával, viszont a megvalósításához szükséges eszközök már merőben mások.

Az online házkutatás elvégzéséhez az erre feljogosított hatóságok és a megfigyelést, online házkutatás végző nyomozók a hackerek által használt eszközöket alkalmazzák. Ezért szükséges, hogy olyan szakember folytassák ezt a munkát s ezen nyomozási cselekményeket, akik megfelelő szakismerettel rendelkeznek. Azokban az országokban, ahol alkalmazzák ezt a nyomozási eszközt, nem ritka hogy ex-hackereket alkalmaznak.

2.6. A virtuális házkutatás előkészületei

Egyes, a témában publikáló német cikkírók szerint az online megfigyelés egyébként roppant költséges. Az eljárás menetével kapcsolatban egyetértek velük, miszerint :

„A nyomozók egy "trójainak" nevezett kémprogramot csempésznek be a gyanúsított számítógépébe például egy e-mail függelékeként, vagy pedig a komputer biztonsági rendszerének valamely hézagán keresztül. (Egyfajta "komputerpoloska" felszerelése is elképzelhető, de ehhez egy nyomozónak titokban be kell hatolnia a gyanúsított lakásába.)”

„Ha sikerült kialakítani a feltételeknek megfelelő "trójait", és bejuttatták a kémprogramot a megfigyelendő számítógépbe, akkor a komputer merevlemezének teljes tartalma lemásolható titokban, és "jegyzőkönyvezhető" minden tevékenység, amelyet a felhasználó a számítógépen végzett. Lehetővé teszi ez az eljárás azt is, hogy a nyomozók hozzáférjenek röpke ideig tárolt adatokhoz, például jelszavakhoz, kódokhoz is. Az interneten folytatott telefonbeszélgetések is lehallgathatók ily módon.” [14]

[14] MTI: „Alkotmányellenesek az online házkutatások”, 2008. február 29.

Ahogyan a cikkíró is írja, s a dolgozatomban később kifejtem, az virtuális házkutatás egyik megoldási módja, ha az titkos házkutatás keretében történik. A fentebb hivatkozott cikkben az író megemlíti a „komputerpoloska" használatának lehetőségét. Úgy gondolom, hogy mivel ezen hardware-es eszköz beszerzéséhez és alkalmazásához is kizárólag a titkosszolgálatoknak van felhatalmazásuk és engedélyük, így ez nem tartozik a dolgozatom tárgyához.

Viszont a cikk további részével, melyben a szerző ennek költség és emberi erőforrás vonzatairól ír, már egyáltalán nem értek egyet: Egy-egy ilyen trójai előkészítése átlagosan 12 szakember egyhavi munkáját veszi igénybe, hiszen e kémprogramoknak sok követelménynek kell megfelelniük: a megfigyelés alá vont számítógép rendszerfeltételeire szabottnak kell lenniük, nem szabad feltűnőnek lenniük, és az sem engedhető meg, hogy biztonsági hézagokat hagyjanak maguk után. [15]

Ez a megállapítás abban az esetben igaz csak, ha egy teljesen új verziójú és eddig feltöretlen operációs rendszerbe kell behatolni. Ilyen esetben ugyanis egy értelemszerűen fel kell térképezni az új rendszert, megtalálni annak gyenge pontjait majd erre megtervezni és megírni egy új kémprogramot. Ez esetben valóban elképzelhető, hogy 12 szakember egyhavi munkája szükséges hozzá, bár én még ezt is túlzásnak tartom. Az esetek 98%-ban azonban már ismert és feltérképezett operációs rendszerekbe kell betörni, s ennek elvégzésére több száz már megírt és kipróbált program áll az ezt végző nyomozók rendelkezésére, s a betörések jelentős része egy kellően képzett szakembernek rutin feladat. Ennek oka, hogy ugyanazokat az eszközöket és megoldásokat kell alkalmazni egy ilyen eljárás során, mint amit a hackerek alkalmaznak, s akik a rendszerbetörési megoldásaikat az interneten számtalan helyen publikálják.

2.7. A virtuális házkutatás lehetséges alkalmazása Magyarországon

Az nyomozási eljárás pontos menetének kidolgozása, leírása és magyarázata részletekbe technikai részletekbe menően nem tárgya a dolgozatomnak, de a garanciális követelmények kidolgozása miatt, illetőleg az eljárás során esetlegesen érintett alkotmányos alapjogok feltérképezése miatt szükségesnek tartom az eljárás egymást követő pontjainak ismertetését. Ezen

[15] Lsd. 14. lábjegyzet

kívül az eljárás menete az intézmény további vizsgálatához, megismeréséhez és a magyar jogi környezetbe ágyazásához is szükséges.

Az eljárás lényege egy úgynevezett kémprogram elhelyezése a gyanúsított személy számítógépén. A kémszoftver (angolul spyware) olyan szoftver, amely a felhasználó tudtán kívül, engedélyezetlenül gyűjt személyes adatokat.[16]Adott esetben előfordulhat, hogy a célszemélynek több személyi számítógépe, notebook van a tulajdonában, használatában.[17] Ilyen esetben nézetem szerint valamennyi potenciálisan bizonyítékhordozó számítógépet az online megfigyelés tárgyává kell tenni.[18] Adott esetben előfordulhat, hogy a célszemélynek több személyi számítógépe, notebook van a tulajdonában, rendelkezési körében[19]. Ilyen esetben valamennyi potenciális bizonyítékhordozó, alapos gyanút alátámasztó potenciális adatot tartalmazó számítógépet az online megfigyelés tárgyává kell tenni.

Nézetem szerint a konfigurálandó kémprogram fajtáját gyakorlati és célszerűségi szempontból nem szerencsés és nem is szabad konkrétan meghatározni, mert ez nagyon behatárolná az elérhető eredményeket, s nem minden esetben lehet eredményes. Másfelől fontos a használható kémprogram típusok behatárolása, mivel így a törvény későbbi alkalmazói nem alkalmazhatják kiterjesztően az összes lehetséges, s adott célnak megfelelő kémprogramra, s az eljárás törvényessége is csak így biztosítható. Úgy gondolom a bírói engedélyhez kötött és nem kötött titkos információgyűjtési eszközöknél alkalmazott szabályozás itt is a legjobb megoldás. Az egyes használható programcsomagokat azok alapjogsérelemmel járó súlyosságuk szempontjából lenne érdemes engedélyhez kötni, vagy engedély nélkül alkalmazhatóvá minősíteni.

2.8. A lehetségesen használható kémprogram típusok

Keylogger: Billentyűnaplózó | Egy nagyon veszélyes fajtája a kémprogramoknak, ha nem a legveszélyesebb. Minden karaktert, amit a számítógép billentyűjén leütünk, összegyűjt egy

[16] Microsoft: http://www.microsoft.com/hun/security/protect/spywares.mspx

[17] Értsd: rövid időn belül, könnyen hozzáférhető számítógépek, melyek nem az ő tulajdonát képezik (pl. családtagé)

[18] Microsoft: http://www.microsoft.com/hun/security/protect/spywares.mspx

[19] Értsd: rövid időn belül, könnyen hozzáférhető számítógépek, melyek nem az ő tulajdonát képezik (pl. családtagé)

naplófileba (log) amit aztán továbbít a "feladónak", abban a pillanatban, hogy online állapotba kerülünk. Így a legszemélyesebb információkat is meg lehet tudni valakiről, beleértve az összes felhasználói nevét, jelszavait, elektronikus bankfiók belépési kódokat, bankkártya adatokat, és minden egyebet. Némelyik ezek közül képes rendszeres képet készíteni a képernyőről (screenshot) és azt (is) továbbítja.

Trojan horse: Trójai faló | Az összes, rejtett tartalommal bíró program gyűjtőneve. A gépükre alattomosan jön be, vagy mi magunk töltjük le, majd a legkülönfélébb merényletre képes. A veszélyesebb változatok egy úgynevezett backdoort (hátsó ajtót) nyitnak a gépünkön, aminek segítségével aztán a program készítője mindent lát, és mindent megtehet a géppel, amit csak akar. A trójaiak sokszor tartalmaznak újabban reklám modulokat is. Ezek úgy tűnnek, mintha leszedhetők lennének egy webkapcsolattal, de az esetek többségében bár úgy néz ki, mintha eltűnt volna, a trójai, vagy egyéb "ajándék" a gépünkön felejtődik. A trójaiak leggyakoribb fajtái:

Spyware: Kémprogram | Nyomon követi minden lépésünket. Figyeli hogy milyen webhelyeket látogatunk, és hogy mit keresünk a keresőben, és továbbítja az adatokat. Az eddig látogatott webhelyeink, nevünk és e-mail címünk pedig minden kémprogram számára azonnal szabad préda, ugyanis a spyware-ek kiszedik azt a Windows regisztrációs adatbázisából.

RAT: Remote Access Trojan, az angol rövidítés egy találó akronima, ami annyit jelent: patkány. Fordítása: Távoli Hozzáférés (t biztosító) Trójai. | Ez a fajta trójai backdoort, azaz hátsóajtót nyit a készítőjének a gépünkön.

Dropper: A dropper elnevezés fordítása: pottyantó. | Ez a trójai változat bejut, majd "lepottyantja" a "hasznos csomagot". A "hasznos csomag" lehet egy másik trójai, vagy backdoor program. Némelyik dropper nem csak fertőz, de fertőzés után is aktív marad, azaz éberen őrködik, hogy a szállítmányát meg nem semmisítsd, hogy az nyugodtan végezhesse a feladatát a háttérben. Ha kiírtjuk "a szállítmányt", akkor egy bizonyos idő elteltével (nem szükségképpen azonnal) újra "kézbesít" a dropper.

A felsorolt program típusok közül bármelyik használható a virtuális házkutatás fentebb ismertetett megvalósítási módjai esetében, s mindegyike sérti az Alkotmány 59. § (1) bekezdésében foglaltakat, miszerint: A Magyar Köztársaságban mindenkit megillet a jó hírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog." Nem kétséges, hogy a számítógépünk titokban történő átkutatása, ott lehallgató program, kémprogram elhelyezése, az adataink és bizalmas anyagaink átvizsgálása, az általunk használt jelszavak rögzítése súlyosan sérti az alkotmányos védelemben részesülő magánszférát. Annak korlátozása csak valamely más alapjog veszélyeztetése esetén indokolt. Ezért különösen fontos, hogy az alapjog sérelemmel járó eljárásokat csak szoros felügyelet mellett lehessen végezni.

2.9. Az eljárás lefolytatására vonatkozó javaslatom

Az eljárás menete távolról való behatolás esetén

1. A nyomozóhatóság vezetője megkeresi a virtuális házkutatás lefolytatására jogszabályban megjelölt rendőri szervet, s attól adott ügyre vonatkozóan a virtuális házkutatás lefolytatását kéri.

2. A megkeresett szerv az ügyből levonható információk alapján meghatározza a célszemélyeket, meghatározza a megfigyelés alá vonni kívánt számítógépeket.

3. Az adott szerv erre szakosodott tagjai az

Az eljárás menete titkos házkutatás esetén

1. A nyomozóhatóság vezetője megkeresi a virtuális házkutatás lefolytatására jogszabályban megjelölt rendőri szervet, s attól adott ügyre vonatkozóan a irtuális házkutatás lefolytatását kéri.

2. A megkeresett szerv az ügyből levonható információk alapján meghatározza a célszemélyeket, meghatározza a megfigyelés alá vonni kívánt számítógépeket.

3. Az adott szerv erre szakosodott

erre alkalmas eszközökkel feltérképezik a megfigyelni kívánt számítógép rendszer kiépítését, különös tekintettel az operációs rendszer típusára, annak verziójára, a hardware kiépítésre, tűzfal létére, számítógépes hálózat létére,kiépítettségére, az internet kapcsolat típusára.	tagjai az erre alkalmas eszközökkel feltérképezik a megfigyelni kívánt számítógép rendszer kiépítését, különös tekintettel az operációs rendszer típusára, annak verziójára, a hardware kiépítésre, tűzfal létére, számítógépes hálózat létére,kiépítettségére, az internet kapcsolat típusára.
4. A 3. lépésben megszerzett információk alapján és a virtuális házkutatási kérelemben megjelölt megszerezni kívánt információk alapán a virtuális házkutatást végző nyomozók eldöntik, a célszerűségi szempontok alapján milyen kémprogram telepítése szükséges, s azt milyen módon a legcélszerűbb kivitelezni.	4. Ha a szerv vezetője az előbb említett információk alapján úgy ítéli meg, hogy a távolról való behatolás nem lenne sikeres, vagy aránytalanul költséges és időigényes lenne, ez esetben a titkos házkutatás alkalmazása mellett dönthet.
5. A felkért szerv erre szakosodott tagjai elvégzik a megjelölt számítógépes rendszerekbe való behatolást, elhelyezik	5. A titkos házkutatással egybekötött virtuális házkutatásra az Rtv. 69.§[20]

20 69. § (1) A Rendőrség bírói engedéllyel a 63. § (1) bekezdésében meghatározott bűnüldözési célból a súlyos bűncselekmények esetében a nyomozás elrendeléséig

a) magánlakást titokban átkutathat (titkos kutatás), az észlelteket technikai eszközzel rögzítheti;

d) az Interneten vagy más számítástechnikai úton történő levelezés (E-mail) során keletkezett adatokat és információkat megismerheti és felhasználhatja.

(2) Az (1) bekezdés c)-d) pontjában meghatározott eszközök alkalmazása során gyűjtött, a titkos információgyűjtés alapjául szolgáló eljárásban nyilvánvalóan nem érintett személyekre vonatkozó adatokat haladéktalanul meg kell semmisíteni, azok a továbbiakban nem kezelhetők és nem használhatók fel.

a kémprogramot, majd elhagyják a feltört rendszert. A kémprogram elhelyezéséhez szükséges időn kívül nem tartózkodhatnak bent a rendszerben, s lehetőleg a legkevesebb adatmódosítással kötelesek azt végrehajtani.

foglaltak vonatkoznak, azzal az eltéréssel, hogy csak a magánlakásban található számítógép képezi a felderítés és rögzítés tárgyát. Ebben az esetben az erre szakosodott tagja a nyomozóhatóságnak közvetlenül konfigurálja a megfigyelni és kutatni kívánt számítógépre a célszerűség alapelvnek megfelelő kémprogramot.

6. Az elhelyezett kémprogramot úgy kell konfigurálni, hogy az a feltört rendszer megfigyelése közben, a program típusából következően megszerzett információkat már közvetlenül a virtuális házkutatást kérő nyomozóhatóság tagjához továbbítsa, s ezen információkról a virtuális házkutatást végző hatóság semmilyen formában sem kapjon másolatot

6. Az elhelyezett kémprogramot úgy kell konfigurálni, hogy az a feltört rendszer megfigyelése közben, a program típusából következően megszerzett információkat már közvetlenül a virtuális házkutatást kérő nyomozóhatóság tagjához továbbítsa, s ezen információkról a virtuális házkutatást végző hatóság semmilyen formában sem kapjon másolatot.

7. A virtuális házkutatás végző hatóság a program elhelyezésével és a feltört rendszerből való kilépéssel befejezte az

7. A virtuális házkutatás végző hatóság a program elhelyezésével és a feltört rendszerből való

eljárásban való közreműködését. A virtuális házkutatás során végzett minden cselekményt az eljárást végző szerv vezetőjének felügyelete mellett folytatják le, s a rendőrség belső szabályzata szerint dokumentálni kell.

kilépéssel befejezte az eljárásban való közreműködését. A virtuális házkutatás során végzett minden cselekményt az eljárást végző szerv vezetőjének felügyelete mellett folytatják le, s a rendőrség belső szabályzata szerint dokumentálni kell.

2.9.1. További eljárási kritériumok

Titkos házkutatás keretében történő behatoláskor továbbá 2 engedély beszerzésére is szüksége lenne, mivel ez az eljárási mód egyszerre érintené a titkos házkutatást és a virtuális házkutatást, s ezekhez külön-külön bírói engedély lenne szükséges.

Meg kell vizsgálni a nyert adatokat is, melyek azok, amelyek a magánszférát érintik, mert azokat törölni kell, a bűncselekményhez kapcsolódó adatokat lehet csak felhasználni (elképzelhető lehetne emellett hatósági tanú részvétele az eljárásban).

III. Fejezet

A virtuális házkutatás egy speciális esete – A kiszolgáló oldali megfigyelés

3.1. Technikai háttér

A későbbiekben ismertetendő megfigyelési technikai mikéntjéhez és megértéshez szükséges ismerni a web működésének alapját. A web megszületése előtt a legtöbb számítógépes program önálló volt, és egyetlen gépen vagy zárt (az Internettel kapcsolatban nem álló) ügyfél – kiszolgáló környezetben futott. A web azon az elven alapul, hogy vannak kiszolgálógépek, amelyeket ügyfél gépek látogatnak meg úgy, hogy az ügyfél gép előtt ülő felhasználó beírja a keresett webcímet (URL-t, ami a „universal resource locator" vagyis „egységes forráscím" rövidítése) a böngészőprogramba. Ez után a távoli kiszolgálóról letöltődik az oldal kódja a böngészőbe,és az ügyfélgép végrehajtja azt, mint egy programot.

A weben a helyzet teljesen más, mint egy önálló alkalmazás esetében, amikor is minden kód helyben tárolódik, és a felhasználót az alkalmazás vezeti végig a különböző ablakokon és beállító képernyőkön. Zárt környezetben könnyű megjegyezni, hogy merre járt a felhasználó, milyen adatokat vitt be, és melyik ablakot kell megjeleníteni a válaszától függően. A web azonban állapot nélküli, ami azt jelenti, hogy a bevitt adatokat és elvégzett műveleteket vagy a kiszolgálón vagy az ügyfélen kell tárolni. A hálózat maga nem kínál ilyen tárolási lehetőséget. A weben állapotról csak a kapcsolatok végpontjain beszélhetünk, de az állapotinformációk kezelését a webalkalmazások nehezen képesek megoldani, mivel a felhasználók tetszés szerint újraindíthatják az adott munkamenetet (az URL újbóli beírásával) , illetve megkerülhetik a javasolt sorrendet (hivatkozásokra kattintás helyett közvetlenül beírva a keresett webhely címét). [21]
Leegyszerűsítve, az internet alapvető tulajdonságából adódik a támadhatósága, abból hogy állapotnélküli, s ez teszi azt is lehetővé, hogy mind az ügyfél oldalon (a megfigyelt személynél)

[21] Mike Andrews: How to break web software : Functional and Security Testing of web applications and web services, Pearson Education Inc., 2006

mind a kiszolgálónál (ahol a weboldal fut) lehetőség legyen a megfigyelést komolyabb beruházás, energia és időráfordítás nélkül megvalósítani.

3.2. Mit tehet a rendőr jogsértő internetes tartalom esetén?

Mit tehet, illetve milyen szabályokat kell követnie a rendőrségnek, ha egy weboldal tartalma, felhívása illetőleg az azon folyó kommunikáció valósít meg büntetőjogi tényállást és teszi szükségessé az intézkedést? Magánlakás esetén, személyhez köthető számítógép esetén már bemutattam a lehetséges eljárási metódusokat, de weboldalak kapcsán a felelősi kör, illetve a hatósági jogkör megállapítása jóval nehézkesebb. Egy weboldal elhelyezhető a világ bármely pontján lévő szerveren, olyan szerveren, aminek helyzete meghatározhatatlan, vagy olyan szerver parkokban, szerver hotelekben ahol a pontos meghatározás rendkívül idő és energia igényes, s amiket nem mellékesen professzionális eszközökkel elrejtenek a rendőrség elől. Bár az ingyenes webtárhelyet szolgáltató vállalatok közül néhányan felhívják a figyelmet rá, hogy büntetőjogi tényállást megalapozó illetőleg meghatározott (szexuális,pedofil,uszító) tartalmú weboldalakat törölni fognak, az esetek többségében mégsem teszik ezt, sőt, a legtöbb ilyen szolgáltatást nyújtó webtárhely nem is köt ki ilyen szabályokat.

Németországba "költözött" a Kuruc.info

Az amerikai bezárás után az internetes adatok alapján a Kuruc.info egy németországi szerveren fut - *írta sz*ombaton az Amerikai Magyar *Népszava Szabadság című, New Yorkban megjelenő magyar nyelvű lap. Pénteken, magyarországi idő szerint délután 3 órakor lekapcsolták a Kuruc.info főszerverét, egy feljelentés nyomán - erről a radikális honlap szerkesztősége tájékoztatta a sajtót közleményben szombaton. A kuruc.info címén a lekapcsolás óta - az Egyesült Államokban is - egy néhány soros üzenet olvasható arról, hogy "Nemsokára visszajövünk (...) kedves fotelforradalmárok, javasoljuk kövessétek a helyszínről az eseményeket (...) ha pár napig nem vagyunk,* akkor elkaptak".

A magyar hatóságok korábban többször hiába próbáltak fellépni az uszító, gyalázkodó írásairól ismert Kuruc.info ellen, mert annak szerverét az Egyesült Államokban működtették, az amerikai hatóságok pedig megtagadták a Kuruc.info felszámolása érdekében az együttműködést."

MTI, 2008. július 5.

Legjobb példa erre a kuruc.info esete, ahol sok esetben kisebbségek elleni uszítás, államellenes bűncselekményekre való felbújtás is megvalósult. Ilyenkor a rendőrség az IP cím beazonosítása után meghatározza, hogy ki az az internetszolgáltató akihez a szerver fel van kapcsolódva, s ezek után

megpróbálja lokalizálni a szervert, majd pedig lekapcsolják azt a hálózatról, vagy jogsegély megkeresés keretében töröltetik a jogsértő weboldalt a szerverről. Ez esetben eltűnik az oldal, megszűnik a jogsértés, de kevés információnk marad az elkövetőkről.

Ennek okán, én egy újfajta eljárási metódust javasolnék, aminek célja alaposabb információ gyűjtés és az ilyen speciális elkövetői réteg feltérképezése. Kijelenthető, hogy mind az internetes pedofil vagy, hogy példámnál maradjak, a kuruc.info közönsége is egy jól behatárolható, szűk réteg. Tudomásom szerint viszont függetlenül a közeg zártságától és behatárolhatóságától, nem létezik egyelőre olyan nyilvántartás, ami naponta frissülve az ilyen gyanús személyeket tartaná nyilván, s könnyítené meg a rendőrség munkáját. Hogy miért nem? Egy személy érintettsége ilyen kérdésekben konkrét ügyekben szokott csak kiderülni, házkutatás eredményeképpen vagy feljelentést követő nyomozásnál.

3.3. Kitekintés – az FBI eljárása

Az első amerikai online házkutatási ügyről Declan McCullagh amerikai újságíró számolt be a blogjában. A riporter közölte, hogy az információkat az akciót engedélyező FBI-tiszttől kapta meg. A tiszt egy dokumentumban pontosan leírta a használt kémprogram jellemzőit, működését és azt is, hogy a megoldást az FBI CIPAV (Computer and Internet Protocol Address Verifier) néven tartja nyilván. A CIPAV egy Windows operációs rendszerek alatt működő program, amit az FBI egyik számítógépéről e-mailben vagy azonnali üzenetküldő hálózatokon keresztül küldenek el a célszemélynek vagy a MySpace vagy a Google Mail egyik ajánlata mögé bújtatják el.

Miután az alkalmazás feltelepítette magát a számítógépre, átnézi a teljes merevlemezt és elküldi a hivatalnak az összes felinstallált program nevét, a böngésző jellemzőit, az operációs rendszer nevét és típusát, a sorozatszámát és a registry minden, a felhasználóra vonatkozó adatát. Emellett a CIPAV továbbítja az FBI-nak az utoljára felkeresett internetes címeket és az összes IP-címet is, amivel az illető a böngészései közben kapcsolatba került.
Az akciót engedélyező bíró ugyanakkor kikötötte, hogy a szoftver kizárólag reggel 6 és este 22 óra között továbbíthatja az FBI-nak az összegyűjtött információkat.

Az FBI megfigyelési technikája azt vélelmezi, hogy mindenki követ el bűncselekményt.
Ezt az eszközt alkalmazva állandó értesítéseket kapnak a megfigyelt böngészéséről, amiből leszűrik az adott személy internetezési szokásait, illetőleg, hogy melyik „kriminalizált" csoportba tartozik, ha beletartozik valamelyikbe. Azaz, a meglátogatott webhelyek és internetes cselekmények, szokásos hosszadalmas és alapos elemzése után kiszűrik az állandó és súlyozott pontokat, majd utána ebben a „kategóriában" helyezik el az adott személyt, hátha később hasznos lesz egy nyomozás kapcsán, mikor a lehetséges elkövetőket akarják kiszűrni.

Úgy gondolom, ez megfigyelési technika figyelmen kívül hagyja az ártatlanság vélelmét, mint alapvető eljárásjogi garanciát. Bár a megfigyelésre vonatkozó szabályozást a rendőrségi törvény tartalmazza s nem a büntető eljárási törvény, ettől függetlenül az ártatlanság vélelme alkotmányos alapjog, s minden eljárásban érvényesülnie kell. Másfelől, ezen megfigyelési technika arra alapul, hogy minden az interneten folytatott tevékenységünk tudatos és kiszámítható, s hogy a számítógépünket csak és kizárólag mi használjuk. Ellenkező esetben a fent említett megfigyelés útján kapott információ nem lenne releváns és a nyomozási eljárásban felhasználható, hiszen ha nem biztos, hogy mi látogattuk meg a kérdéses oldalt, s nem abból a célból amit a rendőrség feltételezett s ami alapján minket „kategorizáltak", akkor az egész nyilvántartás hasznossága kétségessé válik. A saját számítógépünkön ugyanis csak azok az információk tárolódnak el, amit ügyfél oldali kliens program futtatásával és közben teszünk, amit oda begépelünk, ahogyan azt a programot futtatjuk. A világháló az ügyfél-kiszolgáló elven működő rendszerek különleges fajtája. Az elv alapja, hogy egy vagy több központi kiszolgálógép adatokat, erőforrásokat és programokat szolgáltat az ügyfélnek. Ez hagyományosan azt jelenti, hogy egy nagy teljesítményű központi kiszolgálóhoz távoli ügyfelek kapcsolódnak, amelyek gyakran „buták", vagyis nem végeznek számításokat, csupán felhasználói felületet biztosítanak a kiszolgálóhoz. A buta terminál olyan, mintha a távoli kiszolgálóhoz egy billentyűzetet és egy monitort csatlakoztatnánk. Bár ez felgyorsítja a kiszolgáló működését és a internetezést, viszont minél több kódot[22] hajtatunk végre az

[22] Mike Andrews – James E. Whittaker: How to break web software: Functional and security testing of web applications

ügyfélen, annál nagyobb a veszélybe kerül a biztonság, hiszen a felhasználó hozzáférhet az ügyfélen végrehajtott kódhoz, így kiismerheti a futtatott program biztonsági hibáit, s ezt kihasználva betörhet a kiszolgálóra. Így a biztonság fokozása miatt az érzékeny információkat kezelő programok a kiszolgálón futnak, ebből kifolyólag viszont lassul az kiszolgáló gép működése.

Ennek eredményeképpen az igazán fontos adatok és követhető vagy büntetőjogilag releváns cselekményeink nem hagynak feltétlenül nyomot a nálunk lefoglalható számítógépen, csak a kiszolgáló gépen, így lefoglalást vagy megfigyelést azon lenne fontos foganatosítani.

3.4. A kiszolgáló megfigyelése

Az én elképzelésem szerint éppen a fentiekben vázoltak miatt lenne szükséges megfordítani az elméletet, s nem az ügyfél gépeket megfigyelni, azaz a gyanúsítottakat vagy gyanúsnak vélt személyeket, hanem webkiszolgálókon futó weboldalak forgalmát, az oda történő bejelentkezéseket, az egyes bejegyzéseket, kapcsolatokat, megosztott tartalmat kellene figyelni. Nyomozási és bűnmegelőzési szempontból sokkal hasznosabb és adott ügyön túlmutató információk lennének így beszerezhetőek, mintha csak egyes személyek számítógépét vizsgálnák át (ez nem a virtuális házkutatásra vonatkozik, hanem az FBI által is alkalmazott online megfigyelésre), hiszen így rögtön összefüggésében, hálózatban és súlyozottan (az egymással való kapcsolattartás mértéke) lehetne látni az ilyen bűncselekmény elkövetésére hajlamos személyek egymással való kapcsolatát. Hasonlatos lenne ez a megfigyelés, és így a eljárási helyének besorolása is, ahhoz a megfigyelési illetve rendőrségi felderítési eljáráshoz, mikor példának okáért egy, a szervezett bűnözés találkozóhelyeként ismert szórakozóhelyet figyel meg a rendőrség, abból a célból, hogy az ott megfordulók, és megfordulásuk sűrűsége alapján következtetéseket vonhassanak le a bűnözői csoportok viszonyrendszeréről.

Egy ilyen megfigyelés hasonló eszközöket illetve hasonló szakértelmet igényel, mint a gyanúsított személy számítógépébe való behatolás. A különbség annyi, hogy a megfigyelést egy elrejtett program, kód segítségével lehetne megvalósítani, ezt viszont rendkívül körültekintően kell elhelyezni a weboldal kódjában, hogy lehetőleg minél később fedezzék fel. A megfigyelést előkészítő és a programot elhelyező nyomozónak lehetőség szerint igyekeznie kell kreatív és új

megoldásokat találni, viszont vannak olyan alapvető behatolási technikák, amiket végig próbálva egy nem professzionális tűzfallal ellátott szerverre viszonylag gyorsan lehet behatolni.
Ilyennek használható és gyors behatolási technikának tartom az SQL és parancs befecskendezéses technikákat, az ujjlenyomat vételt, a hitelesítés feltöréses módszereket. A használandó eljárásnak abból a szempontból van jelentősége, hogy a „betörés" ne legyen észrevehető, ne tűnjön fel az oldalt üzemeltetőnek és a „poloska" könnyen és feltűnés nélkül elhelyezhető legyen. Miután a behatolást elvégző nyomozó számára szabad tereppé válik a kérdéses weboldal, annak programkódjában (általában HTML kód) elhelyez egy olyan kiegészítő kódot, aminek értelmében a megfigyelt oldal minden tevékenységről, történésről jelentést küld a megfigyelést végző nyomozónak. Ilyen megkapható információ lenne az oldalra belépők IP címe (ami alapján meghatározható akár személyük is), az ott végzett tevékenységük (regisztráció, képek feltöltése, megtekintett oldalak, cikkek, bejegyzések, bejegyzések kommentálása) az oldalra bejelentkezések száma, ideje. Ezen információk alapján nem csak, hogy személyiség profilt lenne könnyű felállítani, de egy néhány hónapos megfigyelés után feltérképezhetővé válna az az állandó kör, aki nem csak véletlenül, kíváncsiságból vagy ritkán érdeklődik ilyen típusú, az állam illetve a társadalom szempontjából is elítélendő dolgok iránt, hanem ennek a terméknek rendszeres fogyasztója.

Viszont bármennyire is hangzik jól ez a fordított megfigyelés, megvalósítása meglehetősen sok ponton ütközik korlátokba, melyek inkább jogiak, mint gyakorlatiak.
Mivel ezek a weboldalak a világ bármely szerverén futhatnak, így a jogsértés hiába irányul pl. a Magyar állam ellen (államellenes bűncselekményekre való felbújtás, lázítás) vagy valamely magyar kisebbségi csoport ellen, ha a jogsértés nem magyarországi szerveren valósul meg, akkor nincs joghatósága a magyar rendőri szerveknek felette. Ez volt a kuruc.info esetében is, mikor nagy valószínűség szerint, bár hivatalos megerősítést ez az információ nem nyert, az igazságügyért felelős miniszter megkeresésére jártak el soron kívül a jogsértő tartalomnak helyt adó szerver ellen az amerikai hatóságok. Ettől a rendkívüli esettől eltekintve azonban ilyen esetben a Cyber Crime Convention-ben lefektetett speciálisan internetes ügyekre vonatkozó jogsegély kérelemben kellene folyamodni a partner hatósághoz, hogy segítsenek az ilyen ügyben. A magyar hatóság tehát csak a magyar szervereken futó jogsértő webhelyek kapcsán intézkedhet, így ebből kifolyólag csak az ilyen helyeket tudja megfigyelni is.

A webkiszolgálók megfigyelésének jogi elemzésénél abból indultam ki, hogy mint megfigyelési eszközként sorolnám be a rendőrségi törvény ugyanezen pontja alá, s azonos jogi garanciák, feltételek illetőleg engedélyezési eljárás vonatkozna erre is. Különbség annyiban áll, hogy ez nem egy speciális fizikai eszköz amit elhelyezünk a számítógépen vagy annak közelében, hanem az adott szerveren futó biztonsági réseket, szoftverhibákat kihasználva hatolna be a nyomozó kívülről s integrálná a megfigyelési jelentéseket küldő programot az egyébként is futó programba (weboldalba).

IV. Fejezet

A virtuális házkutatás mint nyomozási eszköz jogi környezete Magyarországon

4.1. A titkos nyomozási eszközök jogi és dogmatikai háttere

Az előző fejezetben vázoltakból látható, hogy az online házkutatás azt a célt szolgálja, hogy hozzásegítse a nyomozó hatóságokat az állam büntetőjogi igényének érvényesítéséhez. A nyomozás hatékony lefolytatásához egyes esetben szükséges lehet a nyomozási cselekmények titkossága. A Be. szabályoz titkos nyomozási eszközöket, például a bírói engedélyhez kötött titkos adatszerzést, és tartalmaz szabályokat a titkos információgyűjtésre is.

A virtuális házkutatás, mint nyomozási eszköz további vizsgálata előtt hasznos lehet azonban a nyomozási eszközök, mind a rendészeti mind a bünügyi felderítési eszközök dogmatikai áttekintése.

A titkos felderítésnek hazai jogunkban két formája ismeretes:

a) A titkos információgyűjtés a büntetőeljárás megindítását megelőző szakasz, amelynek szabályait a szervezeti törvények foglalják magukba.[23]

63. § (1) A Rendőrség bűncselekmény elkövetésének megelőzésére, felderítésére, megszakítására, az elkövető kilétének megállapítására, elfogására, körözött személy felkutatására, tartózkodási helyének megállapítására, bizonyítékok megszerzésére, valamint a büntetőeljárásban részt vevők és az eljárást folytató hatóság tagjainak, az igazságszolgáltatással együttműködő személyek védelme érdekében - törvény keretei között - titokban információt gyűjthet.[24]

23 1994. évi XXXIV. törvény A Rendőrségről /továbbiakban Rtv

24

b)A titkos adatszerzés a büntetőeljárás keretei között, a nyomozás elrendelését követően teljesített titkos felderítés. (A büntetőeljárásról szóló 1998. évi XIX. törvény 200. §)

A titkos nyomozási eszközök a bűnüldöző hatóságoknak a bűncselekmények feltárására irányuló, titkos módszerekkel végrehajtott megismerő tevékenységének részei, amelyek a bűncselekmények megelőzése, megakadályozása és bizonyítása céljából történhetnek.

A titkos nyomozási eszközökkel kapcsolatban négy fontos elemet különíthetünk el:

- Cél (nemzetbiztonsági, bűnüldözési és/vagy igazságszolgáltatási).
- Tárgya: a büntetőeljárás alapjául szolgáló magatartás (vagy annak közvetlen kockázata),
- Alanya a nemzetbiztonsági szolgálatok, a bűnüldöző hatóságok, és
- Módja (erők, eszközök, módszerek és alkalmazásuk eljárási formája).[25]

A titkos nyomozási eszközök bűnüldözési célja olyan információk megszerzése, amelyek segítségével a bűncselekmények megelőzése, megakadályozása és bizonyítása a legrövidebb idő alatt, minimális legitim erőszakkal és maximális hatékonysággal biztosítható. A bűnüldözési eredményességet célszerű úgy mérni, hogy a felderítésre fordított összegek és az elhárított károkat és hátrányokat állítjuk arányba. Ez az arány gyakran pénzben is kifejezhető. Máskor azonban a bűnüldözés olyan erkölcsi értékek épségét szolgálja, hogy azok megvédelmezésének „gazdaságossága" kvantitatív módon nem mérhető.

Az igazságszolgáltatási cél a bizonyítási eszközök biztosítása, amelyekből a büntetőeljárásban jogszerűen felhasználható bizonyítékok meríthetőek, ennek eredményeként pedig az állam büntető igénye az igazságszolgáltatás előtt érvényesíthető.[26]

Az időszerűség kapcsán hangsúlyozni kell, hogy a megismerés a múlton kívül a jelenre és a jövőre is irányulhat. A múlt tekintetében a bűnüldözési célú megismerésnek az időbeli (anyagi jogi) korlátját az elévülés jelenti. Az eljárásjogi korlátot az eljárásjogi határidők jelentik.

.

[25] Finszter Géza: A titkos felderítés kriminalisztikája., Kriminalisztika tnkv. 2. kötet

[26] Finszter Géza: *A titkos információgyűjtés szabályozása a hatályos jogban*. Kriminológiai Tanulmányok, 37. kötet, Budapest, 2000. 101-123. p.

Az alanyi oldal kettős értelemben is meghatározható. A közjog szempontjából ez mindig olyan nemzetbiztonsági illetve bűnüldözési hatósági jogkörrel felruházott állami szervezet, amelynek hatáskörébe és illetékességébe törvény által meghatározott felderítési ügyek tartoznak. (Jelenleg a rendőrség, a határőrség, a vám- és pénzügyőrség, az ügyészség, a rendvédelmi szervek védelmi szolgálat, valamint a polgári és a katonai nemzetbiztonsági szolgálatok rendelkeznek felderítési kompetenciával.) Kriminalisztikai megközelítésben az alanyi oldal az előbbiekben meghatározott szervezetekkel közszolgálati viszonyban lévő és különleges szakértelemmel rendelkező munkatársat jelenti. A nyomozó hatóságok beosztottaival szemben a közszolgálat valamennyi tagjára kötelező követelmények érvényesek, miszerint szolgálati feladataikat szakszerűen, jogszerűen és szolgálatszerűen kell végrehajtaniuk. A felderítés kriminalisztikája lehetővé teszi a felderítés szakszerűségét, ennek a munkának a tanulhatóságát és taníthatóságát, az eredményesség mérését és a felderítésben dolgozók munkájának szakmaként való elismerését.[27]

A felderítés módja a felhasználható erőknek, eszközöknek és módszereknek az alkalmazási lehetőségeit és eljárási rendjét fogja át.

A felderítés kriminalisztikájának tárgya a titkos információgyűjtés, illetve a titkos adatszerzés során teljesített megismerés, amelynek legitim célja annak eldöntése, hogy szükséges-e a nyomozás formális megkezdése, illetve, hogy várható-e elegendő információ a vádemelés megalapozására. [28]

A széles cselekvési autonómia ellenére a titkos felderítés jogilag szabályozott eljárás, amennyiben:

- törvény határozza meg, hogy melyek a bűnüldöző hatóságok,
- törvény határozza meg, hogy mely bűncselekmények esetében megengedett a titkos nyomozási eszközök igénybevétele
- törvény határozza meg az eszközöket és a módszereket, és végül,
- törvény határozza meg az eljárási formáját.

[27] Finszter Géza: *A titkos információgyűjtés szabályozása a hatályos jogban*. Kriminológiai Tanulmányok, 37. kötet, Budapest, 2000. 101-123. p.

[28] Finszter Géza: A titkos felderítés kriminalisztikája., Kriminalisztika tnkv. 2. kötet

Jelenleg a bűnüldöző hatóságok három típusa ismeretes:

- azok a szolgálatok, amelyek jogosultak bűncselekmények felderítésére, de nem minősülnek nyomozóhatóságnak, ezért nyomozást nem folytathatnak (rendvédelmi szervek védelmi szolgálata és valamennyi nemzetbiztonsági szolgálat),
- továbbá nyomozó hatóságok, amelyek titkos információgyűjtést és nyílt nyomozást egyaránt végezhetnek (rendőrség, határőrség, vám- és pénzügyőrség),
- az ügyészség.

Az ismertetett hatósági kompetenciák arra az eljárási rendre épültek, amikor a gyanú foka alapján élesen különbséget lehetett tenni a nyomozás előtt folytatott titkos információgyűjtés és a nyomozás között. Az új eljárási törvény ezeket a határokat felismerhetetlenné teszi azáltal, hogy már a bűncselekmény gyanúja elegendő a nyomozáshoz. Ugyanakkor a legalitás parancsa alapján a gyanú felmerülése kötelezővé is teszi a nyomozás elrendelését.

A titkos nyomozási eszközök alatt nem a bizonyítás eszközeit értjük (Be 76. § /1/ bekezdése), hanem azokat a titkos eszközöket, eljárási módszereket, valamint titokban felderítési feladatot teljesítő személyeket, amelyek, és akik segítségével a bűnüldöző hatóság bizalmas információhoz (titkos adathoz) juthat. A titkos nyomozási eszközöket a bűnüldöző hatóság hozza létre (az informátort beszervezi, fedővállalkozást létesít, lehallgatásra alkalmas berendezést fejleszt ki, titkos adattárakat létesít,[29] stb.) és ezt követően teszi alkalmazhatóvá és veti be az egyedi felderítési ügyben.

Ha azonban az információk bűncselekmény gyanújára utalnak, akkor nyomozás elrendelésének van helye. Ilyenkor a titkos információgyűjtés nem folytatható tovább, hanem át kell adnia a helyét a titkos adatgyűjtésnek. A Be 200. § (3) bekezdése érelmében: „E cím rendelkezései nem érintik a nyomozás elrendelését megelőzően a bírói, illetőleg az igazságügy miniszteri engedélyhez kötött titkos információgyűjtést; e tevékenységet a külön törvényekben meghatározottak szerint az erre feljogosított szervezetek a rájuk irányadó szabályok szerint végzik. A (4) bekezdés így folytatja: „Ha a nyomozás elrendelését megelőzően külön törvény alapján a

[29] 21/1996. (VIII. 31.) BM rendelet a belügyminiszter irányítása alatt álló titkos információgyűjtésre feljogosított szervek adatkezelésének egyes szabályairól

bíró, illetőleg az igazságügyi miniszter által engedélyezett titkos információgyűjtés végrehajtása során az ügyben a nyomozást elrendelik, a titkos információgyűjtést a továbbiakban csak e törvény szerint mint titkos adatszerzést lehet folytatni."

4.2. A virtuális házkutatás mint titkos nyomozási eszköz

A virtuális házkutatásnál, mint felderítési módnál is szükséges vizsgálat tárgyává tennünk annak eszközeit, módszereit, alkalmazási lehetőségeit és eljárási rendjét. A megfigyelés és a titkos nyomozási cselekmények jogi szabályozottságából kitűnik, hogy azok a számítógépes bűncselekményekkel szemben, azok felderítésére nem alkalmazhatóak. A titkos információgyűjtés keretében a számítógépes adatforgalom figyelése igen kevés és nem hatékony eszköz az informatikai bűncselekmények megelőzéséhez, felderítéséhez. Ahogy már korábban említettem, nem csupán a számítástechnikai rendszer elleni bűncselekmények felderítéséhez fontos a szükséges eljárásjogi intézmények kialakítása, hanem a számítógéppel elkövetett nem számítástechnikai bűncselekmények felderítésére is.

Az internet és számítógép korunk társadalma számára a mindennapi élet meghatározó elemévé vált, az információszerzés, ügyintézés, szórakozás elsődleges forrásává, s így átlagosan megállapítható, naponta 2-3 órát töltünk „online" üzemmódban. Egyes szociológiaelemzések némi túlzással a mindennapi életet „online" és „offline" szakaszra bontják, elvetve a hagyományosan használt terminológiákat. Ebből következően, akarva és akaratlanul is rengeteg olyan adat kerül lementésre a használt számítógépünkön, ami egy nyomozás során értékes információkkal bírhat.

Nem csupán a számítógépes, s számítógéppel elkövetett bűncselekménye szaporodik rohamosan évről évre, hanem az azt elkövetők száma is. A számítógéppel elkövetett bűncselekmények bizonyításához szükséges bizonyítékok alapvetően az elkövetéshez használt eszközön „hagynak" nyomot, annak lefoglalásával és elemzésével lehet elsődlegesen biztosítani őket.

A büntetőeljárásnál kriminalisztikai alapvetés, hogy az idő múlásával egyenesen arányosan csökken az esélye a bizonyítási eszközök megtalálásának, biztosításának, s így a nyomozás sikerességének. A korábban már ismertetett német tanulmány alapján pedig kijelenthetjük, hogy a

számítógépes bűncselekmények esetén ez hatékonysági mutató sokkal gyorsabban változik, mint a hagyományos nyomozás esetében.

Így a számítógépes, online felderítés célja nem csupán a gyanúsított számítógépen lévő, a bizonyítás és nyomozás szempontjából releváns bizonyítékok feltérképezése, hanem szükséges esetben azok online módon való rögzítése. Az eljárásjog hatályos szabályozása szerint, lehetőség van a lefoglalásra a Be 151.§ alapján.[30] Míg egy halott test, gyilkossághoz használt fegyver vagy gazdasági bűncselekményre vonatkozó bizonyítékok eltűntetése nem lehetséges egyik pillanatról a másikra, addig a számítógépen rögzített adatok megsemmisítése, így a bizonyítékok eltűntetése még egy laikus számára is gyorsan és könnyen megoldható feladat.

Mindazonáltal, hosszas és költséges szakértői munka eredményeként az adatok egy része visszanyerhető, 100%osan az elveszett, megsemmisített adatok nem állíthatóak vissza. Ennek okán létfontosságú az ilyen bűncselekményekkel kapcsolatos nyomozások során a különválasztott rendészeti felderítési szakasz és a bűnügyi felderítési szakasz egybe olvasztása, vagy lehetőség szerint a két eljárási szakasz közötti időtartam minimálisra szorításra.

Ez nem csupán az általános büntetőeljárási alapelvek érvényesítése szempontjából fontos, hanem,a nyomozás eredményességének esélyét is növeli a bűncselekmény elkövetésétől számított időtartam csökkenése.

Hatályos eljárásjogunk már ismeri az ilyen eljárásjogi problémákra a megoldást, a titkos adatszerzés szabályainál megtalálhatjuk, hogy : „

Ha az engedélyezés olyan késedelemmel járna, amely a titkos adatszerzés sikerét veszélyeztetné, az ügyész legfeljebb hetvenkét óra időtartamra elrendelheti a titkos adatszerzést (halaszthatatlan elrendelés). Ez esetben az elrendeléssel egyidejűleg az engedélyezés iránti indítványt is elő kell terjeszteni.„[31]

Emellett a törvény rendelkezik arról is, hogy:

„Ha a nyomozás elrendelését megelőzően külön törvény alapján a bíró, illetőleg az igazságügyért felelős miniszter által engedélyezett titkos információgyűjtés végrehajtása során az ügyben a

[30] BE.: **151. §** (1) A lefoglalás a bizonyítás érdekében vagy az elkobzás, illetőleg a vagyonelkobzás biztosítására a dolog birtokának elvonása a birtokos rendelkezése alól.

[31] 1998.évi XIX. Törvény a Büntetőeljárásról, 203.§ (6)

nyomozást elrendelik, a titkos információgyűjtést a továbbiakban csak e törvény szerint mint titkos adatszerzést lehet folytatni."[32]

Ezen rendelkezések értelmezéseként kimondható, hogy adott esetben a számítógépes felderítés, online házkutatás során, mint titkos nyomozási eszköz (lsd. titkos információgyűjtés értelmezése) keretében olyan információ kerül a nyomozó hatóságok látókörébe, ami megalapozhatja az állam büntetőjogi igényének hatékony érvényesítését.

Általános esetben a titkos információgyűjtés befejezése és titkos adatszerzés megkezdése között hosszabb idő is eltelhet, ennek oka a nyomozásra jogosult hatóság meghatározása, az ügy áttétele, s a titkos adatszerzés megkezdése, melyek mind időt igénylő eljárási cselekmények. A számítógépes bűncselekmények esetén ez a „titkos adatszerzés sikerét veszélyeztetné" így a törvényben lehetővé tett halaszthatatlan elrendelést a rendészeti felderítési szakasz és bűnüldözési szakaszra is szükséges lenne alkalmazhatóvá tenni.

Ezen eljárási intézmények közötti váltás, átmenet problematikája, hogy a leggyorsabb megoldás abban az esetben realizálódhatna, ha ugyanaz a szolgálat folytathatná a titkos adatszerzést, mint amelyik a titkos információgyűjtést elkezdte. Titkos információgyűjtést a hatályos jogszabályok alapján a rendőrségi szervek és a társ szervek végezhetnek. A különbség az egyes szervek eljárása között, hogy a rendőrségi titkos információgyűjtés bírói engedélyhez kötött, a társszervek (lsd. 1995.évi CXXV.trv. A nemzetbiztonsági szolgálatokról) eljárása pedig a rendészeti- és igazságügy miniszteri engedélyhez kötött. Az információgyűjtést végző szerv kiválasztása célszerűségi és hatékonysági szempontok alapján történik. Fontos különbség még az egyes szervek között, hogy a hatályos magyar jog szerint csak a rendőrségnek van hatásköre és jogosultsága nyomozást folytatnia.

A kérdés az, milyen jogi garanciák, megoldások mellett lehetséges az, hogy a megfigyelést végző személyek ne manipulálhassák az adatokat, illetve később ne lehessen az eljárás tisztaságát és a bizonyítékok hitelességét megkérdőjelezni.

Abban különbözik még a virtuális házkutatás az eddig ismertetett felderítési eszközöktől, megoldásoktól, hogy a gyanú alapján általában egy személy, helyszín vagy jól körülhatárolható információ megszerzése céljából végzik a nyomozást, a virtuális házkutatás alkalmazása kapcsán

[32] 1998.évi XIX. Törvény a Büntetőeljárásról, 200.§ (4)

előfordulhat, hogy a gyanú alapján akár száz számítógép „ellen" folytatnak egy időben virtuális házkutatást.

A magyar büntető eljárási törvényt átható alapelv szükségesség és a fokozatosság elve. Titkos nyomozásra akkor kerülhet sor, ha az információ más módon nem szerezhető meg. Az alkalmazott eszközök sorában a legcsekélyebb jogkorlátozással járó formát érdemes bevetni, ha a cél elérésére az is alkalmas. A virtuális házkutatás csekélyebb jogkorlátozással jár? Egyrészről igen, mert nem kell elviselni a házkutatással járó kellemetlenségeket, másrészről viszont nem, mert azzal, hogy az érintett nem is tud róla, önmagában súlyosabban érintettek az alkotmányos alapjogai.

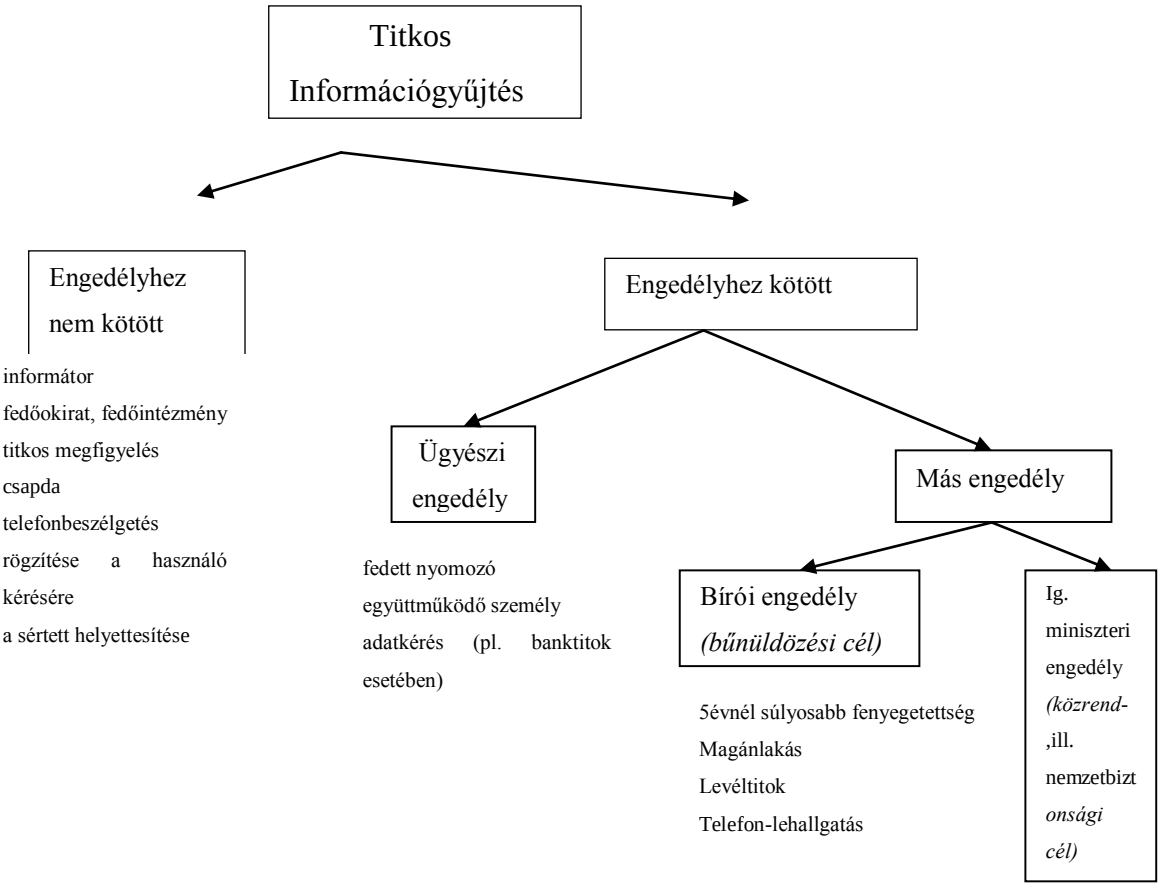
A virtuális házkutatásnak előnye lehet az univerzalitás. Ugyanaz a megoldás hatékony lehet az erőszakos és a gazdasági bűncselekményeknél egyaránt. Különösen nagy hangsúlyt kaphat alkalmazása kábítószer kereskedelmet és a terrorizmust az egyik póluson, másfelől a zsarolást, az útonállást, a biztosítási csalások erőszakos formáit (gyújtogatás a nyereség reményében), végül pedig egy harmadik kategóriát, a fehér galléros gazdasági bűncselekményeket és a politikai korrupciót. Ezzel összefüggésben azonban hangsúlyozni kell, hogy meg kell találnia az egyensúlyt a szükségesség, fokozatosság és az univerzalitás között. Igaz, hogy alkalmas bármilyen bűncselekmény felderítésére, azonban a fokozatosság miatt, már ha elfogadjuk a virtuális házkutatás erősebb jogkorlátozó jellegét, akkor nem lehet minden bűncselekmény esetén lehetővé tenni. Éppen ellenkezőleg nagyon le kell szűkíteni azoknak a bűncselekményeknek a körét, ahol alkalmazható lehet. Ezen bűncselekmények csak a legsúlyosabbak közül kerülhetnek ki, mint például a nemzetközi terrorizmus vagy a szervezett bűnözés. Megfontolandó lehet a pedofília, illetve egyes gazdasági bűncselekmények esetén a virtuális házkutatás megengedhetősége.

Kriminalisztikai szempontból a virtuális házkutatás különlegességét az adja, hogy a bűncselekmény elkövetésének színterei közé tartozhat a magánlakás, továbbá a személyes kapcsolatokra rendelkezésre álló bizalmas kommunikáció szolgálhat a kriminalitás eszközeként. Ráadásul az így keletkezett bizonyítékok egy része mással nem pótolható, ezért a bírói engedély a későbbiekben a tárgyalás anyagává tett bizonyítás hitelességét erősítheti.

4.3. A bírói engedélyhez kötött titkos adatszerzés és a titkos információgyűjtés egymáshoz való viszonya

A Titkos információgyűjtés szerkezete

[33]



A titkos adatszerzés és a titkos információgyűjtés kényes, alkotmányos és személyiségi jogokat sértő eljárás, amely szigorúan csak a törvény szoros értelmezése mellett végezhető.

[33] Tóth Mihály: A magyar büntetőeljárás az Alkotmánybíróság és az európai emberi jogi ítélkezés tükrében, KJK-Kerszöv, Budapest, 2001

Az új Be 200. § (1) szerint az ügyész és a nyomozó hatóság bírói engedély alapján az elkövető kilétének, tartózkodási helyének megállapítása, elfogása, valamint bizonyítási eszköz felderítése érdekében a nyomozás elrendelésétől a nyomozás iratainak ismertetéséig titkos adatszerzést végezhet. A Be. 200. § (1) bekezdés a)-c) pontjai sorolják fel azokat az eszközöket, amelyek bírói engedéllyel alkalmazhatók a titkos adatszerzés során, így az érintett tudta nélkül magánlakásban lehallgatást kezdeményezhet, levelet, más postaküldeményt és telefonbeszélgetést ellenőrizhet, végül számítástechnikai rendszereken továbbított adatokat megismerhet. A nyomozás elrendelését követően bírói engedélyhez kötött titkos adatszerzés csak a Be alapján történhet. (Amiből egyenesen következik, hogy a bírói engedélyhez nem kötött eszközök alkalmazásával tovább folyhat a rendészeti felderítés, amely akár a jogerős ítéleten túl is tarthat.)
A titkos információgyűjtés részletes szabályai a rendőrségről szóló 1994. évi XXXIV. (továbbiakban Rtv.), és a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben (továbbiakban Nt.) találhatóak. Mindazok a rendvédelmi és bűnüldözési szervek, amelyek ezen túl felhatalmazást kaptak a titkos felderítésre, a rendőrségi törvényre hivatkozással folytathatják ezen hatósági tevékenységüket. A titkos információszerzéssel összefüggő egyes részkérdések a büntetőeljárási törvényben is helyet kaptak.

A helyzetet tovább bonyolítja, hogy vannak nyomozóhatósági jogosítványokkal nem rendelkező felderítő szolgálatok, amelyek titkos információgyűjtést igen, de titkos adatgyűjtést már nem folytathatnak. Ide sorolható valamennyi nemzetbiztonsági civil és katonai hivatal, a nemzetbiztonsági szakszolgálat (amely utóbbi szolgáltatásait viszont a nyomozó hatóság a nyomozás elrendelését követő titkos adatgyűjtéshez igénybe veheti), végül pedig a Rendvédelmi Szervek Védelmi Szolgálata.

Mind a titkos adatszerzés, mind a titkos információgyűjtés során alkalmazott nyomozási eszközök alkotmányos alapjogok sérelmét eredményezhetik.
Kiemelést érdemel, hogy a taxatív felsorolásból valami oknál fogva kimaradt a titkos házkutatás lehetősége. Az Rtv. lehetőséget teremt a Titkos információgyűjtés során arra, hogy a nyomozó hatóság magánlakást titokban átkutasson, az ott észlelteket technikai eszközzel rögzítse. Úgy gondolom, ezen eszköz lehetőségének elmaradása az „új” büntetőeljárásról rendelkező törvényben

súlyos hiba a jogalkotó részéről, melyet a lehető legrövidebb időn belül pótolni kell. A 200. § (1) bekezdés a) pontja a magánlakásban történtek megfigyeléséhez és rögzítéséhez szükséges technika elhelyezését jelenti, a kutatást azonban nem engedélyezi. A rögzítéshez, megfigyeléshez szükséges technika elhelyezése akár jelentheti a korábban említett „komputer poloska" vagy akár az internetes adatforgalmat figyelő kémprogram telepítést is. A magánlakásba történő behatoláshoz az Rtv. és a Be. alapján sem kell külön engedély.

A Be. 201. § (2) bekezdése alapján, amennyiben a nyomozást az ügyész (ügyészségi nyomozó, katonai ügyész) végzi, úgy a 201. § (1) bekezdésében fel nem sorolt bűncselekmény miatt is helye van a titkos adatszerzésnek.

A Be. 202. §-a meghatározza azt a személyi kört, akikkel szemben a titkos adatszerzés alkalmazható:

· elsősorban a gyanúsítottal, illetve azzal a személlyel szemben, aki a bűncselekmény elkövetésével a nyomozás adatai alapján gyanúsítható;

· azokkal a személyekkel szemben, akik a gyanúsítható személlyel bűnös kapcsolatot tartanak fent;

· bizonyos esetekben az ügyben eljáró ügyvéddel szemben, valamint

· a lelkésszel, egyházi személlyel szemben, aki titoktartási kötelezettségére hivatkozva tagadta meg a tanúvallomást, valamint az olyan személyekkel szemben, akik a törvény által nyújtotta lehetőséggel élve tagadták meg a tanúvallomást.

Az Rtv. és a Be. engedélyezési szintje azonosnak nevezhető, ha úgy fogalmazunk, hogy mind a titkos információgyűjtés, mind pedig a titkos adatszerzés bírói engedélyhez kötött.

A titkos információgyűjtés során alkalmazni kívánt különleges eszközök igénybevételét az engedélyt kérő nyomozó hatóság székhelye szerint illetékes helyi bíróságnak a megyei (fővárosi) bíróság elnöke által kijelölt bírája engedélyezi.

Halaszthatatlan elrendelés esetén – amennyiben a különleges eszköz alkalmazásának engedélyezése olyan késedelemmel járna, amely sértené a bűnüldözés eredményességéhez fűződő

érdeket – a nyomozó hatóság vezetője 72 óra időtartamra elrendelheti a különleges eszköz alkalmazását az engedélyezés iránti kérelem bíróságra történő egyidejű benyújtásával.

A titkos adatszerzés engedélyezéséről a bíróság (nyomozási bíró) az ügyész indítványára határoz. Itt is lehetőség van halaszthatatlan elrendelésre, amennyiben az engedélyezés olyan késedelemmel járna, amely a titkos adatszerzés sikerét veszélyeztetné. Ebben az esetben az ügyész ugyancsak 72 óra időtartamra elrendelheti a titkos adatszerzést az indítvány bíróságra történő egyidejű előterjesztésével.

A nyomozás elrendelése általában határozattal történik.[34]

A Be. szabályoz azonban olyan eseteket is, amikor a nyomozást még nem rendelik el alakszerű határozattal, de késedelmet nem tűrő okból az ügyész vagy a nyomozó hatóság nyomozati cselekményt végez vagy bizonyítási cselekmények elvégzését rendeli el. Nyilvánvaló, hogy a nyomozás megindult, de annak határozattal történő elrendelésére nem került sor. Ebben az esetben kérdésként merül fel, hogy lehetőség van-e titkos adatszerzés engedélyezésére? Álláspontom szerint a jogszabály kiterjesztő értelmezését jelentené, ha az el nem rendelt, de folyamatban lévő nyomozásban is lehetőség lenne a titkos adatszerzésre. Egyébiránt a törvény kifejezetten az elrendelés nyelvtani kifejezést használja és nem a nyomozás megindulásától, hanem a nyomozás elrendelésétől adja meg a lehetőséget a titkos adatszerzésre. Ezt a gondolatot továbbfűzve arra a következtetésre jutok, mely szerint ilyen esetben az ügyész sem jogosult a 72 óra időtartamú halaszthatatlan elrendelésre azért, mivel az ügyésznek kötelessége megvizsgálni, hogy a nyomozás elrendelése határozattal megtörtént-e vagy sem. Természetesen a nyomozás ezen szakaszában az Rtv. alapján helye van titkos információgyűjtésnek a nyomozás határozattal történő elrendeléséig.[35]

A koncepció alapja, hogy a biztonság szempontjából nélkülözhetetlen, de az alapvető jogok és a szabadság tekintetében nagyon veszélyes eszközről van szó, amelyet a jogállami intézmények ellenőrzése alatt kell tartani.

---

[34] Be. **170.** § (1)

[35] Dr. Fekecs Gyula: Titkos információgyûjtés avagy titkos adatszerzés? Publikációk, Jogi Forum, 2005.március

V. Fejezet

A virtuális házkutatással kapcsolatban felmerülő problémák

„59. § (1) A Magyar Köztársaságban mindenkit megillet a jóhírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog."

5.1. Titkosszolgálati környezet

Amikor a büntető eljárásjog egyes titkosszolgálatokat érintő, titkos eljárásokat tartalmazó szabályaival foglalkozunk s ezen eszközöket bármiféle vonatkozásban, de egy dolgozat tárgyává tesszük, fontos megismernünk a titkosszolgálatok jogi hátterét is Magyarországon.
Nem csak azon okból, hogy sok esetben ezek a szolgálatok végzik az egyes titkos információgyűjtéssel, adatszerzéssel kapcsolatos cselekményeket[36], hanem szabályozásuk módja és háttere kihat a büntető eljárásjog szabályozására is, bár jogágilag eltérő helyen lettek szabályozva, s a Be.-ben lefektetett garanciális szabályok és alapelvek nem hatják át a Nemzetbiztonsági törvényt.

Az Országgyűlés a Nemzetbiztonsági törvény elfogadásával a nemzetbiztonsági tevékenységet, mint feladatrendszert és a hozzá kötődő eszközrendszert, továbbá a nemzetbiztonsági tevékenységet ellátó szervezeteket, a kormányzati irányítást, a parlamenti ellenőrzést funkcionálisan egybefüggő egységként azonos elvek és garanciák mellett szabályozta. Ezzel egyben kijelölte a nemzetbiztonsági tevékenységgel összefüggő részletes szabályok tárgyköreit, amelyek megváltoztatása a jövőben csak kétharmados törvénnyel lehetséges, mivel az Alkotmány előírása szerint minősített többséggel megalkotott törvényt egyszerű többséggel hozott törvénnyel nem

36 1995.évi CXXV. Törvény, 8. § (1) A Nemzetbiztonsági Szakszolgálat

a) a jogszabályok keretei között a titkos információgyűjtés, illetve a titkos adatszerzés különleges eszközeivel és módszereivel - írásbeli megkeresésre - szolgáltatást végez törvény által erre feljogosított szervezetek titkos információgyűjtő, illetve titkos adatszerző tevékenységéhez;

lehet módosítani. Az Alkotmánybíróság állásfoglalásából az olvasható ki, hogy egyszerű többséggel hozott törvény is tartalmazhat a nemzetbiztonsági tevékenységgel összefüggő olyan rendelkezést, amely az Nemzetbiztonsági törvényben lefektetett szabályozások irányával – azt nem módosítva – összhangban van.

Alkotmánytani szempontból érdemes a titkosszolgálatoknak a szuverenitásvédelemhez való viszonyát is érinteni.

A nemzetbiztonsági törvény preambuluma a nemzetbiztonsági tevékenységnek, a nemzetbiztonsági szolgálatok működésének célját a Magyar Köztársaság szuverenitásának biztosításában és alkotmányos rendjének védelmében határozza meg. Természetesen a nemzet biztonságának garantálása jóval túlmutat a nemzetbiztonsági szolgálatok rendeltetésén és feladatkörén, hiszen ez közvetlenül vagy áttételekkel valamennyi állami szerv feladata. A szuverenitás biztosítása, az alkotmányos rend védelme, a nemzet biztonságának garantálása az állami szervezetrendszer egészének funkciója, amelyben –speciális eszközeikkel – a nemzetbiztonsági szolgálatok is részt vesznek.

5.2. Alkotmányossági aggályok

Az állam kötelessége az alapjogok tiszteletben tartása, illetve az alapjogok érvényesülésének biztosítása. Az alkotmányos alapjogok korlátozására van lehetőség, de csak a szükségesség-arányosság követelményének megtartása mellett.

A virtuális házkutatás több alkotmányos alapjogok is érint. Például az Alkotmány 59. § (1) bekezdésében foglaltakat, miszerint: A Magyar Köztársaságban mindenkit megillet a jó hírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog.”

+ magánlakás sérthetetlenségéhez való jog

+ információs önrendelkezési jog

+ emberi méltósághoz való jog

Nem kétséges, hogy a számítógépünk titokban történő átkutatása, ott lehallgató program, kémprogram elhelyezése, az adataink és bizalmas anyagaink átvizsgálása, az általunk használt jelszavak rögzítése erősen érintik az alkotmányos védelemben részesülő magánszférát. Annak korlátozása csak valamely más alapjog veszélyeztetése esetén lehet indokolt. Ezért különösen fontos, hogy az alapjog sérelemmel járó eljárásokat csak megfelelő garanciák mellett lehessen végezni. Ilyen garanciák lehetnek: csak meghatározott bűncselekmények esetén lehessen elrendelni, bírói engedély, pontosan megfogalmazott jogszabály.

Az alkotmányos demokráciák eltérő módon gondoskodnak arról, hogy bűnüldözésük titkosrendőrségi módszerekkel felvértezve vegye fel a harcot a bűnözés legveszélyesebb formáival szemben, és eközben e módszerek ne okozzanak kárt a demokratikus értékekben.

Vannak országok, ahol az állampolgári jogoknak ezeket a titkos korlátozásait a büntetőeljárási kódexekbe foglalják (Ausztria, Németország)[37], más megoldás szerint a szervezett bűnözés és az illegális kábítószer forgalom elleni különleges felhatalmazások körébe illeszkednek a szabályok (Egyesült Államok, Egyesült Királyság, Spanyolország), esetenként jogforrásnak kínálkozik a rendőrségi törvény. (A volt szocialista országok majd mindegyikében.)[38] Meglepő módon több fejlett polgári demokrácia a mai napig nélkülözi a megfelelő jogi szabályozást, és ez visszatérően zavarokat okoz a felderítő szolgálatok működésében.(Ide sorolható Belgium és Hollandia.)[39] Azt azonban érdemes hangsúlyozni, hogy a társadalomvédelmi funkciók törvényessége felett az alkotmányos demokrácia egész intézményrendszere őrködik, néha hatékonyabban, mint a speciális rendvédelmi törvények. Igazán kifogástalan biztosítékokat a kettő együtt képes adni.

Németországban 2007 óta folyik egy jogalkotási és jogalkalmazási vita, melynek középpontjában az online megfigyelés, virtuális házkutatás áll. Dolgozatom témáját és célját tekintve ennek

[37] Kertész Imre: Rendőrség, rendőrállam, jogállam, I. rész, Belügyi Szemle 1989/10.

[38] John Mcenany: A bűnügyi nyomozás és büntetőjogi felelősségre vonás az Amerikai Egyesület Államokban. II. rész – Rendészeti Szemle 1992/12. szám.

[39] Chantal Joubert. A titkosrendészet holland és nemzetközi vonatkozásai, Belügyi Szemle, 1997/5. szám, 9. old.

részletes elemzésébe itt nem bocsátkoznék, viszont fontosnak tartom a német Alkotmánybíróság határozatának ismertetését.

A német jog is ismeri az információs önrendelkezési jogot, illetőleg az alkotmánybírósági határozat kitér egy „új" jogintézményre is, az „információs technikai rendszer integritása és bizalmassága"-ra. Ezen utóbb említett jogintézmény esetében felmerül a kérdés, hogy tekinthetjük e alapjognak, illetőleg levezethető-e ezen intézmény Magyarországon egy már az alkotmányban szabályozott jogintézményből.

5.3. Az információs önrendelkezési jog[40]

A telekommunikációs rendszerbe történő technikai beavatkozás lehetővé teszi az egész rendszer kifürkészését, így olyan adatokat is megfigyelhetnek, amelyeknek semmi köze a telekommunikációs rendszer működéséhez. Ilyen például a személyi számítógép magáncélra történő használata esetén meghatározott szolgáltatások felhívásának gyakorisága, illetve a lakásban lévő más háztartási eszközökre vonatkozó adatok, amelyeket szintén a megfigyelt információs technikai rendszer működtet.[41]

Az információs önrendelkezési jog túlmutat a magánszféra védelmén. Az egyéneknek alapvetően joguk van saját maguknak meghatározni személyes adataik kiszolgáltatását és felhasználását.[42] Az információs önrendelkezési jog védelme nemcsak a szenzitív adatokra terjed ki, hanem azokra az információkra is, amely informatív értéke önmagában csekély, de más adatokkal összekapcsolva hatással lehet az érintett személyiségére és cselekvési szabadságára.[43]

Az információs önrendelkezési jog azonban nem számol teljes körűen a személyiség veszélyeztetettségével, amely abból adódik, hogy az egyén egyre jobban rá van utalva személyisége

[40] Mohácsi Barbara: Az online-házkutatás szabályozásának és alkotmányosságának kérdése Németországban – a titkos adatszerzés legújabb formája?, Jogi tanulmányok, Eötvös Lóránd Tudomány Egyetem Állam-és Jogtudományi Kar, Budapest, 2008, 179-203.

[41] 1 BvR 370, 595/07 vom 27. Februar 2008, 188.

[42] 1 BvR 209/83 vom 15. 12. 1983, BVerfGE 65, 1 (43); 1 BvR 239/90 vom 11, 06. 1991, BVerfGE 84, 192 (194)

[43] 1 BvR 1550/03 vom 13 Juni 2007 in: NJW 2007, 2464, 2466.

kibontakoztatásához az információs technikai rendszer használatára, amelynek során kényszerűen adatokat szolgáltat. Az a harmadik személy, aki beavatkozik a rendszerbe, potenciálisan nagy adatállományhoz juthat hozzá anélkül, hogy adatszerzési vagy adatfeldolgozási tevékenységet kellene végeznie. Ez a beavatkozás túlmutat az információs önrendelkezési jog által védett egyszeri adatfelderítésen.[44]

5.4. Az információs technikai rendszer integritásának és bizalmasságának védelme

Az egyének személyiségük kibontakoztatása során rá vannak utalva az információs technikai rendszerre, ezért az általános személyiségi jognak biztosítania kell az információs technikai rendszer integritásának és bizalmasságának védelmét.[45] Ez a jog az információs önrendelkezési jogon alapszik, védi az alapjog jogosultjának személyes és magánéleti viszonyait az információs technika révén történő állami beavatkozásokkal szemben. A védelem az információs technikai rendszer egészébe történő beavatkozásra is kiterjed, nemcsak az egyes kommunikációs folyamatok vagy a mentett adatok a védelem tárgyai.

A személyiség különleges védelmét nem szükséges minden információs technikai rendszer tekintetében garantálni, amely személyes adatok létrehozására, feldolgozására vagy tárolására képes, mert bizonyos esetekben elegendő az információs önrendelkezési jog által biztosított védelem. Akkor kell az információs technikai védelemre vonatkozó alapjogot alkalmazni, ha a beavatkozás olyan rendszer esetén áll fenn, amely önmagában vagy hálózatos csatlakozásán keresztül személyes adatokat tartalmaz, amely lehetővé teszi, hogy az érintett személy életének jelentős részébe bepillantást nyerjenek, vagy a személyiségéről általános képet kapjanak.[46] Ez a jog elsődlegesen a felhasználó érdekeit védi biztosítva azt, hogy az információs technikai rendszer által létrehozott, feldolgozott és tárolt adatok bizalmasak maradjanak.

Az alapjogba akkor történik beavatkozás, ha az információs technikai rendszer funkcióihoz, tárolt adataihoz harmadik személy hozzáférhet, megszüntetve ezzel a rendszer kifürkészésének,

[44] 1 BvR 370, 595/07 vom 27. Februar 2008, 200.

[45] 1 BvR 370, 595/07 vom 27. Februar 2008, 201.

[46] 1 BvR 370, 595/07 vom 27. Februar 2008, 202.

megfigyelésének és manipulációjának technikai akadályait. Az információs technikai rendszer védelme különösen kiterjed a titkos beavatkozásokra.[47]

A technikai beavatkozás során kihasználják az információs technikai rendszer biztonsági hiányosságait, amely konfliktust okozhat a sikeres beavatkozáshoz fűződő általános érdek és az információs technikai rendszer biztonságához fűződő érdek között.

A rendszerbe való behatoláskor ugyanis a megfigyelést végző szakszolgálat emberei korábban már említett „backdoort" nyitnak a megfigyelés tárgyává tett számítógépen. Ezen beavatkozás eredményeképpen nem csupán a virtuális házkutatást végzők juthatnak be a hátsó ajtón, hanem mindenki más is, aki támadási pontot keres az adott számítógépen, mivel a használt kémprogramok nyitva hagyják azt amin keresztül a nyomozást végzők is bejutottak. Ez kiszolgáltatottá, sebezhetővé teszi a megfigyelt számítógépét, így nem csupán az információs önrendelkezési jog és a számítógépes rendszer integritása és bizalmassága sérül, hanem védtelenné teszi a megfigyeltet, s ily módon potenciálisan bűncselekmény elkövetését segíti elő. Magyar jog szerint ilyen esetben a hatóság segítené elő a Btk. 300.§/C, 300.§/E-ben foglalt bűncselekmények megvalósulását.

Szakértők szerint a beavatkozás olyan károkozással is együtt járhat, amely nem áll összefüggésben a nyomozással. Akár az intézkedő hatóságok, akár harmadik személy visszaélhet a hozzáférést lehetővé tevő programmal, manipulálhatja, törölheti, megváltoztathatja az adatokat vagy újakat hozhat létre.[48]

Az információs technikai rendszer fogalmába beletartozik a számítógép winchestere, valamint a rendszerhez csatlakoztatott adathordozók. Az alapjogvédelem az adatszerzés olyan eszközével szemben is érvényesül, amely az érintett rendszer adatfeldolgozási folyamatától technikailag független, de az adatfeldolgozási folyamatok képezik az intézkedés tárgyát. Ilyen eszköz például a Keylogger[49], vagy a képernyő, illetve a billentyűzet elektromágneses kisugárzásának mérése.[50]

---

47 1 BvR 370, 595/07 vom 27. Februar 2008, 204-205.

48 1 BvR 370, 595/07 vom 27. Februar 2008, 240.

49 A Keylogger egy olyan vírus, amely fő funkciója, hogy valamennyi billentyű lenyomását begyűjti, rögzítve ezzel a felhasználói neveket és a jelszavakat is. A felhasználó által alkalmazott jelszó ismeretével hozzá lehet férni akár a különösen védett adatokhoz. A Keylogger segítségével az is megállapítható, hogy a felhasználó az internetről milyen adatokat mentett le a számítógépre, vagy külső adathordozóra.

50 1 BvR 370, 595/07 vom 27. Februar 2008, 206.

Büntető eljárásjogi intézmények vizsgálatakor úgy gondolom a két legfontosabb alapelv, amit szem előtt kell tartanunk, az arányosság elve és célszerűség alapelve.

Az arányosság elve értelmében az alapjogi beavatkozásnak legitim célt kell szolgálnia, a cél elérésére alkalmasnak, valamint szükségesnek és arányosnak kell lennie.[51]

A német jog az arányosság elvének szűkebb értelmezése alatt megköveteli, hogy az intézkedés által okozott alapjogi korlátozások arányban álljanak az elrendelés indokaival.[52] A törvényhozó feladata az alapjogkorlátozás érdekeinek és a korlátozás súlyának egymás mellé rendelése. Előfordulhat, hogy egy intézkedést nem lehet az általános érdekek védelmében alkalmazni, mert az abból következő alapjogi korlátozások súlyosabbnak tekintendők, mint az érvényesítendő érdekek védelme.

Tovább fokozza a beavatkozás intenzitását, hogy az adatszerzés információt nyújthat az érintett és harmadik személyek közötti kommunikációjáról, amely közvetetten érinti az állampolgárok szabadságát azáltal, hogy a megfigyeléstől való félelem akadályozhatja a zavartalan kommunikációt, illetve harmadik személyeket is érinthet, akikkel szemben nem valósulnak meg a beavatkozás feltételei.[53] A beavatkozás súlyosságát befolyásolja a titkos megfigyelés időtartama. A hosszabb ideig tartó megfigyelés lehetővé teszi az adatok folyamatos begyűjtését, amely nagyobb kiterjedésű és többféle adat megszerzését teszi lehetővé, mint egyszeri beavatkozás esetén.

Az intézkedések titkossága fokozza az alapjog korlátozás súlyát. A titkos nyomozási intézkedések kivételesen alkalmazhatóak, és elrendelésükhöz különleges jogalap szükséges.

Ez a konfliktus csökkentheti az állampolgárok bizalmát abban, hogy az állam az információs technológia lehető legnagyobb biztonságának megteremtésére törekszik.[54]

[51] 1 BvR 1084/99 vom 03. 03. 2004, BVerfGE 109, 279 (335)

[52] 2 BvL 43/92 vom 09. 03. 1994, BVerfGE 90, 145 (173); 1 BvR 1084/99 vom 03. 03. 2004, BVerfGE 109, 279 (349)

[53] 2 BvR 454/71 vom 31. 01. 1973, BVerfGE 34, 238 (247); 1 BvR 330/96, 1 BvR 348/99 vom 12. 03. 2003, BVerfGE 107, 299 (321)

[54] Mohácsi Barbara: Az online-házkutatás szabályozásának és alkotmányosságának kérdése Németországban – a titkos adatszerzés legújabb formája?, Jogi tanulmányok, Eötvös Lóránd Tudomány Egyetem Állam-és Jogtudományi Kar, Budapest, 2008, 179-203.

5.5. Technikai jellegű problémák

- vírusírtó programok veszélyt jelenthetnek a hatósági kémszoftverre – megoldás lenne-e a vírusítű programok előállítóival történő megállapodás?
- a nyert adatok valódiságának problémája, mi igazolja, hogy azokat a megfigyelt személy nem hamisította meg, nem jelent-e az utánajárás annyi időt és energiát, amely a virtuális házkutatással nyert előnyöket elhomályosítja
- olyan harmadik szermélyek is lehetnek a megfigyelés tárgyai, akiknek adott esetben semmi közük nincs a bűncselekményhez, csak például véletlenül megkapják az emailt, hogyan lehet ezt technikailag kikerülni?
- törölt adatok problémája, technikailag visszaállíthatóak, megismerhetőek, de felhasználhatóak-e a büntetőeljárásban?

VI. fejezet

A virtuális házkutatás helye a magyar büntető eljárásjogban

A kérdés nem csupán az, van e helye a magyar eljárásjogban ennek az eszköznek, szükséges-e és szabad-e beemelni ezt az eszközt a lehetséges nyomozási eszközök közé. Hiszen felmerül az a kérdés is, hol helyezzük el? Egyáltalán nem mellékes, hogy a törvény mely részébe integrálja a jogalkotó, miként definiálja, valamint, hogy milyen eszközként, s az eljárás mely szakaszába helyezi el.

Joggal merül fel ugyanis a kérdés, hogy egy ilyen eljárási, nyomozási cselekményt nem a szakszolgálatoknak kell e végezniük, s ha igen, milyen körülmények fennállása esetén vonhatja be őket a nyomozást végző szerv. A másik oldalról viszont az alkotmányos alapjogok érintettsége miatt felmerülhet a virtuális házkutatás bírósági jogkörbe történő utalása.

A következő kérdéseket szükséges megvizsgálnunk:

- Mely törvényben keretében célszerű szabályozni? Ennek milyen büntetőpolitikai következményei vannak?
- Mely esetekben lehetne ezt az eszközt alkalmazni?
- Mely szerv lenne jogosult az eljárás lefolytatására? Milyen feltételek teljesülése mellett?
- Szükség lenne e törvényességi felügyeletet végző szerv engedélyére?
- Milyen engedélyezési követelmények vonatkoznának az eljárásra? Ügyészi, bírói, vagy igazságügy miniszteri engedélyre lenne e szükség?
- Az eljárás során megszerzett információk felhasználhatóságának kérdése. Az ügyész nyílttá tehetné e, milyen feltételekkel minősülhetne a büntetőeljárás során bizonyítás eszköznek?

Jogpolitikai szempontból, s gyakorlati szempontból a következő alternatíva lehetséges véleményem szerint:

6.1. A virtuális házkutatás mint büntető eljárásjogi intézmény

A legjobb megoldási lehetőség az lenne, ha ez a szabályozás a Be. V. címe alatt, a bírói engedélyhez kötött titkos adatszerzés mellett, önálló eszközként kerülne szabályozásra. Elképzelésem szerint ugyanaz a nyomozó hatóság végezhetné el a virtuális házkutatást, aki az eljárás során a bizonyítási eszközöket is felderíti. Nem lenne szükség a váltásra információgyűjtés és adatszerzés között, ezzel a nyomozóhatóság nem veszítene időt az egyes cselekmények között, a virtuális házkutatás során szerzett információkra pedig így nem minősülnének államtitoknak.

Ha az eljárás során bizonyosodik, hogy a megfigyelt személy kapcsolatba hozható a bűncselekmény elkövetésének tényével, a nyomozó hatóság elrendeli a házkutatást a gyanúsított és a bizonyítási eszköz lelőhelyén, s lefoglalja a lehetséges bizonyítási eszközöket. A virtuális házkutatás szabályaiban lehetőséget adnék a nyomozó hatóságnak, hogy rendkívüli esetben, ha a

lefoglalás megkezdése olyan késedelemmel járna, ami a bizonyítási eszközözök biztosításának sikerét veszélyeztetné, online úton rögzítsék a számítógépen található, a gyanúsítottra nézve, a büntetőeljárás szempontjából releváns adatokat, bizonyítékokat.
Természetesen ezt rendkívül pontos, s a törvényességet és hitelességet biztosító, technikailag is elfogadható garanciális eszközök beiktatásával tartom elképzelhetőnek. Szakértő bevonásával vagy hatósági tanú jelenlétében, az átmásolt adatok speciális, hitelesített elektronikus aláírással való ellátásával.

Érdekes viszont egy pillantást vetnünk a Titkos adatszerzés, Be. 200.§ 1) c)[55] pontjára. Abban az esetben ha ezt a jogalkalmazó szemszögéből nézzük, kiterjesztően értelmezhető a jogszabály úgy, hogy abba beletartozik akár a virtuális házkutatás is. Ha ezt az értelmezést helyesnek fogadnánk el, úgy a Be. ezen szabálya meglehetősen „gumiszabály" jelleget mutat. Hiányzik ugyanis annak részletezése, vagy arra való utalás, hogy milyen módon kell ezt a „megismerést" megvalósítania a hatóságoknak. A törvény további szakaszaiban egyáltalán, és a törvényi kommentárban sem találtam ebben a kérdésben útbaigazító szabályozást.

Azon értelmezést alapul véve, hogy a virtuális házkutatást a Be. 149.§[56]-ban definiált helyiségben lévő számítógépen végzik, ez esetben a titkos házkutatás szabályai adnak további keretet a titkos adatszerzésben foglalt eljárásnak. Az adott számítógépet ugyanis az interneten keresztül, közvetetten kell megközelítenie a hatóságnak, az internetes kapcsolatot biztosító, a számítógépbe csatlakoztatott kábelen keresztül hatolnak be a helyiségbe és a számítógépbe. Enélkül nem lenne rá lehetőségük, így előbb a helyiségbe hatol be a hatóság (úgymond időrendileg is előbb valósul meg a helyiségbe való behatolás mint a számítógépbe való behatolás). A virtuális házkutatás törvényes végzéséhez így a nyomozó hatóságnak szüksége lenne egy titkos házkutatási engedélyre és egy titkos adatszerzésre elvégzésére felhatalmazó bírói engedélyre.

55 Be. 200.§ 1) *c)* a számítástechnikai rendszer útján továbbított és tárolt adatokat megismerheti és felhasználhatja (a továbbiakban: titkos adatszerzés)

56 Be. **149. §** (1) A házkutatás a ház, lakás, egyéb helyiség vagy azokhoz tartozó bekerített hely, továbbá az ott elhelyezett jármű átkutatása, illetőleg számítástechnikai rendszer vagy ilyen rendszer útján rögzített adatokat tartalmazó adathordozó átvizsgálása az eljárás eredményessége érdekében.

A fentebb vázoltak alapján bár lehetőség van a virtuális házkutatás lefolytatására hatályos jogunk szerint, nem hagyhatjuk figyelmen kívül a garanciális szabályok további szabályozását.
A titkos adatszerzésnek a törvényben meghatározott bűncselekmények[57] előkészülete, kísérlete és elkövetése esetén van helye. A titkos adatszerzés alkalmazhatóságát bizonyos bűncselekmények nem pedig a meghatározott jogi értékek veszélye esetén engedi meg a jogalkotó
Nézetem szerint, bár hasznos lenne ezen eljárás szélesebb körben való alkalmazásának lehetővé tételére, de arányosság és célhoz kötöttség elvei mentén kétféle csoportosítás keretében szabályoznám az alkalmazási területeket:

1. A német jogi szabályozással analógiát vonva, a 10 évnél súlyosabb börtönbüntetéssel büntetendő bűncselekmény esetén tenném lehetővé a virtuális házkutatás alkalmazását.
2. Az eszköz jellegéből, kialakulásából szerintem értelemszerűen adódik, hogy a számítógéppel elkövetett bűncselekmények, azaz a Btk. 300/C. §, 300/E. § , és én kiterjeszteném alkalmazhatóságát még a gazdasági bűncselekmények felderítésére és az összes olyan kiskorúak sérelmére elkövetett pedofil bűncselekményekre, amelyeknél a számítógép mint elkövetési eszköz szerepelt.

Fontos továbbá annak szabályozása, hogy milyen eszközöket, milyen hosszú időtartamra, milyen dokumentációs kötelezettségek mellett végezhetné a hatóság ezt a fajta házkutatást.
Úgy gondolom, a legalitás, arányosság, és célhoz kötöttség elvei alapján kizárólag bírói engedély birtokában lenne mód ennek a nyomozati eszköznek az alkalmazására, s az ezzel szerzett bizonyítási eszközökre a titkos adatszerzés eredményének felhasználására[58] vonatkozó szabályok az irányadóak.

[57] Be. 201.§(1)bek. a) –e) pontok

[58] Be. 206.§ A titkos adatszerzés eredményének felhasználása

VII. fejezet

Összegzés

Új típusú bűnözők, bűncselekmények és fenyegetések logikusan újfajta eljárásokat tesznek szükségessé. A számítógépes bűncselekmények az anyagi jogban már szabályozva lettek, de ezt nem követte az eljárásjog modernizálása. A dolgozatommal a célom az volt, hogy egy olyan eljárási eszköz bemutatását és megvédését kíséreljem meg, ami több mint adatszerző tevékenység. Fontosnak tartom ezen intézmény súlyát és jövőben való jelentőségét kiemelni. Ahogy több ponton is kiemeltem, vannak olyan bűncselekmények amelyek bizonyítása napjainkban más módon, mint számítógépes eszközök lefoglalása, elemzése, virtuális házkutatás nélkül nem is lennének bizonyíthatóak! Az aktuális jogpolitikai, jogalkotási tendenciákba beleillik az alapjogok korlátozásának ilyen téren való kiterjesztése, ha a virtuális házkutatás eljárásának módját és eredményét ilyennek tekintjük.

Hajlamosak vagyunk elfelejteni, hogy nem mindig az állam teszi meg az első lépést magánéletünk megsértésében. Az internetet és számítógépet felhasználó bűnözők sértették meg először ezt a láthatatlan határt, ennek eredményeképpen minden állampolgár egyénileg is rászorul a számítógépes, internetes önvédelem megtanulására, kifejlesztésére, de az államnak is meg kell tennie a szükséges ellenlépéseket. Nem az állami önkény, a magánéletbe való behatolás, a titkosszolgálati eszközök mindennapi alkalmazásához való kondicionálása a társadalomnak az oka a virtuális házkutatás kialakításának az oka. Az első lépést, támadást azok tették, akik az internet nyújtotta szabadsággal és magas szintű szakértelmükkel visszaéltek haszonszerzés és saját büntetőjogilag is elítélendő vágyaik kielégítése végett. Az internet, ami a születésekor hatalmas lehetőséget, szabadságot és kapcsolatot jelentett a világ minden polgárai között az azt használók számára, mára az elsődleges veszélyforrássá lépett elő. Mondhatni, az internet használók és az internet közötti „társadalmi szerződést” szegik meg azok, akik az általa nyújtott lehetőséggel visszaélnek.

Az államnak kötelessége az ilyen elkövetőkre a társadalom ítélete alapján a megfelelő büntetés kiszabása, s az ilyen személyek ezen módon való eltávolítása az internetes közösségből.

Ezért feladata a büntető eljárásjognak, s a büntetőpolitikának, hogy az erre leghasznosabb eszközökkel vértezze fel az állam bűnüldöző szerveit.

A virtuális házkutatás a legfontosabb kezdő lépés ezen az úton.

IRODALOMJEGYZÉK:

Augusztinyi Krisztina: A számítástechnika felhasználásával megvalósuló bűncselekmények, Rendészeti Szemle, 56. évfolyam, 3. szám, 66.-77. oldalig

Kriminalisztika 1-2. szerk: Bócz Endre BM Kiadó, Budapest, 2004.

Belovics Ervin-Molnár Gábor-Sinku Pál: Büntetőjog Különös rész Budapest, 2005. 21-40. oldal

Büntető eljárásjogi olvasókönyv, Osiris Kiadó, Budapest, 2003, Bócz Endre, 306. oldal

Büntető eljárásjog, Dr. Tóth Mihály, Budapest, 2006, HVG-Orac Kiadó, 324.-329. oldal

Herke Csongor: Büntető eljárásjog, Dialóg-Campus kiadó, Budapest, 2004. 164.-167. oldal

Finszter Géza:Titkos adatgyűjtés kriminalisztikája - Bíbor Kiadó, Miskolc, 2003.

Finszter Géza: A titkos információgyűjtés szabályozása a hatályos jogban. Kriminológiai Tanulmányok, 37. kötet, Budapest, 2000. 101-123. p.

Finszter Géza: A rendvédelemről szóló AB határozatok elemzése, Kriminológiai Tanulmányok 44. , Országos Kriminológiai Intézet, Budapest,2008, 11-46. oldal

Kriminál taktika 1. Budapest, 2001, Rejtjel kiadó, Rendőrtiszti főiskola, 63. oldal

Mike Andrews: How to break web software : Functional and Security Testing of web applications and web services, Pearson Education Inc., 2006

Mohácsi Barbara: Az online-házkutatás szabályozásának és alkotmányosságának kérdése Németországban – a titkos adatszerzés legújabb formája?, Jogi tanulmányok, Eötvös Lóránd Tudomány Egyetem Állam-és Jogtudományi Kar, Budapest, 2008, 179-203.

Peszleg Tibor: Internet és pedofília, Bűnügyi szemle, 2004

Tremmel Flórián: Magyar büntetőeljárás, 2001, Dialóg Campus Kiadó, 31. oldal

Titkos adatgyűjtés kriminalisztikája - Bíbor Kiadó, Miskolc, 2003.

Titkos információgyűjtés szabályozása a hatályos jogban - Kriminológiai Tanulmányok 37. , Országos Kriminológiai Intézet, Budapest, 2000.

Tóth Mihály: A magyar büntetőeljárás az Alkotmánybíróság és az európai emberi jogi ítélkezés tükrében, KJK-Kerszöv, Budapest, 2001

Internetenes források jegyzéke:

http://www.mszh.hu/szerzoijog/cikkek2007/2007-08-papp.pdf, Letöltés: 2008-11-25

http://www.jogiforum.hu/publikaciok/66, Letöltés: 2008-10-18

http://www.jogiforum.hu/publikaciok/127 Letöltés: 2008-11-05

http://www.jogiforum.hu/publikaciok/307 Letöltés: 2008-09-27

http://www.jogiforum.hu/publikaciok/52 Letöltés: 2008-11-26

http://www.jogiforum.hu/publikaciok/75 Letöltés: 2008-07-28

http://www.jogiforum.hu/publikaciok/50 Letöltés: 2008-07-29

http://www.jogiforum.hu/publikaciok/40 Letöltés: 2008-08-13

http://abiweb.obh.hu/abi/index.php?menu=beszamolok/1995-96/7/1/2&dok=27_A_1995, Letöltés: 2008-11-14

http://abiweb.obh.hu/abi/index.php?menu=mediaszemle/archivum/2004/07/12&dok=8808 Letöltés: 2008-11-14

http://abiweb.obh.hu/abi/index.php?menu=jogszabalyok&dok=1880 Letöltés: 2008-11-14

http://abiweb.obh.hu/abi/index.php?menu=mediaszemle/archivum/2004/07/12&dok=8808 Letöltés: 2008-11-14

http://www.heise.de/newsticker/meldung/95629 Letöltés: 2008-11-14

http://www.heise.de/newsticker/meldung/93307 Letöltés: 2008-11-14

http://www.rp-online.de/public/aritcle/aktuelles/politik/deutschland/497373

Letöltés: 2008-11-14

http://www.sueddeutsche.de/deutschland/artikel/955/1317200 Letöltés: 2008-11-14

Jogforrások:

2/2007. (I. 24.) AB határozat – a titkos adatszerzéssel kapcsolatban

1978. évi IV. törvény a Büntető Törvénykönyvről

1995. évi CXXV. Törvény a nemzetbiztonsági szolgálatokról

1998. évi XIX. Törvény A büntetőeljárásról

1994. évi XXXIV. Törvény a Rendőrségről

Ulf Buermeyer: Die Online-Durchsuchung. Die technische Hintergrund des verdecken hoheitlichen Zugriffs auf Computersysteme In: Online Zeitschrift für Höchstrichterliche Rechtssprechung im Strafrecht April, 4/2007. 154-166. 159.

BvR 370, 595/07 sz. (2008. február 27.) a Német AB döntése az online-házkutatásról