DR. DORNFELD LÁSZLÓ
doktorjelölt

MAGÁNSZFÉRA VÉDELME ÉS NYOMOZÁSI ÉRDEK KONFLIKTUSA A KIBERTÉRBEN

1. Bevezetés

A magánszféra védelme és a nyomozási érdek közötti konfliktus a modern jogállamok büntetőeljárásának egyik sarkalatos kérdése. Az egyik oldalon érvként az állam büntetőigénye áll, és egyúttal társadalmi szempontból is fontos elvárás, hogy a bűncselekményt elkövetők a végén bűnhődjenek tetteikért. A másik oldalról szemlélve ugyanakkor ennek megvalósítása nem írhatja felül a magánszféra védelméhez való jogot, hiszen ez a totális rendszerek nem túl kellemes emlékét idézi vissza. Ma már nincs vita az európai jogrendszerek egyikében sem azt illetően, hogy a magánérdek védendő értéknek tekintendő. Számos álláspont létezik a fogalompárost és valamelyik elsőbbségét illetően, ám ezek bemutatása nem témája írásomnak, hanem a kérdéskör egy speciális területét kívánom bemutatni.

A kibertér legegyszerűbben megfogalmazva „emberek, adatok és számítógépek hálózata", ami a fizikai világban létező infrastruktúra révén tud működni, ám attól függetlenül. Életünk egyre nagyobb része folyik ezen a sajátos új csatornán, ahol nemcsak a felhasználók érdeklődési köre, politikai véleménye, kapcsolatrendszere tárható fel, hanem például egészségügyi állapotuk, pénzügyi helyzetük, vallási nézeteik, és a sort még hosszan lehetne folytatni. Ahogy az élet egyre nagyobb része válik digitalizálttá, a szokványos tevékenységek is hatalmas ilyen mennyiségű adatot képesek előállítani. Éppen ezért a magánszféra védelme minden eddiginél fontosabb kérdéssé lépett elő.

Ahogy a bűnözés egyre jobban kihasználja az új technológia nyújtotta lehetőséget, úgy kerülnek elő újabb és újabb összeütközési pontok a nyomozási érdek és a magánszféra védelme között. Hiszen pl. bűnüldözési szempontból fontos adat nemcsak az elkövető eszközén található, hanem sok esetben a sértett vagy harmadik felek (pl. szolgáltató) rendszerében is fellelhetők. Ahogy nemcsak információs rendszer elleni bűncselekmények esetén lehetnek elektronikus bizonyítékok, hanem szinte bármilyen esetben, pl. egy chatbeszélgetés

egy erőszakos bűncselekményt megelőzően. A legalapvetőbb kérdés, hogy ki és milyen mértékben jogosult arra, hogy ezeket az adatokat megismerje egy eljárás során, és hogyan gondoskodnak a már nem szükséges adatok törléséről.

A következőkben felvetett kérdések mindegyike akár egy-egy önálló tanulmány témája is lehetne, és a megítélésüket igencsak nehezíti, hogy a kibertérrel kapcsolatos diszkusszióban folyamatosan keverednek a büntetőjogi, rendészeti és nemzetbiztonsági érvek. Az alábbiakban ezért ezek részletes bemutatására nem vállalkozom, elsődleges célom az egyes kérdéskörökkel kapcsolatos vita lényegének feltárása.

2. Anonimitás és az azonosítás kötelezettsége

Az anonimitás, a névtelen közlés joga igen sokat vitatott megítélésű a kibertéren belül és kívül, míg az interneten elsődlegesen technikai okok miatt jelent meg. Ugyan a személyes adataink nem kerülnek rögzítésre internetezés közben, ez nem jelenti azt, hogy teljesen láthatatlanok lennénk. Minden felhasználó egy IP címet kap, amely alapján az internetszolgáltatója képes őt visszaazonosítani, és ez egy büntetőeljárás során is használható. Ugyanakkor a jelenlegi rendszer legnagyobb buktatója, hogy dinamikus, vagyis a címek folyamatosan más számára kerülnek kiosztásra. Sőt, az is elképzelhető, hogy az internetszolgáltató előfizetői egyetlen IP cím alatt jelennek meg, és annak 65535 portjának valamelyikén keresztül kommunikálnak, ez a szolgáltató-szintű hálózati címfordítás (Carrier-grade network address translation, CGN). A nyomozóhatóságnak ilyenkor már nem csak az IP címet, és az elkövetés idejét, de a kiinduló- és célportokat is ismernie kell. Mivel a szolgáltatók gyakran nem őrzik meg az ezzel kapcsolatos naplókat, sokszor lehetetlenné válik a felhasználó azonosítása.

Mivel egyre növekvő számú eszköz használja az internetet, ez azzal a veszéllyel fenyeget, hogy az elkövetők felkutatása is nehezebbé válik. A felhasználók egy része különböző technikai megoldásokat is igénybe vesz, hogy a digitális nyomait eltüntethesse. Ennek számos oka lehet, például a megnövekedett igény a magánszféra védelmére, ami miatt a támogatói ezeket gyakran nevezik privát szférát erősítő technológiáknak. Azonban ennek lehetőségeit a bűnelkövetők is könnyedén kihasználhatják saját nyomaik leplezésére. Ilyenek például a proxy szerverek, amelyek segítségével a felhasználó könnyedén szerezhet a maga számára olyan IP címet, amely a világ bármely pontjára mutat. Hasonló célt tölt be az Amerikai Egyesült Államok Haditengerészete által katonai célokra kifejlesztett TOR (The Onion Router), amely igen nehezen feltörhető titkosítási módszerrel védi a kommunikáció tartalmát. Ugyan történtek kísérletek a felhasználók azonosítására, ezek igen nagy erőbefektetést igényelnek, és kizárólag bizonyos felhasználók azonosítása nem lehetséges a módszerrel. További lehetőség még a torrentoldalak technológiai alapját képező peer-to-peer (p2p)

technológia használata is, amely két rendszer közötti közvetlen adatmegosztást tesz lehetővé, bármilyen központi szerver érintése nélkül. Léteznek speciális célú rendszerek is, így például a kriptovaluták, amelyeknek még a jogi megítélése sem teljesen egyértelmű, egyfajta pszeudofizetőeszköznek tekinthető. Számos fajta kriptovaluta létezik, a legismertebb közülük a Bitcoin, ugyanakkor mind megegyezik abban, hogy az adott érték tulajdonosa nem ismert, csak az ún. blokklánc, amely az eddigi tranzakciókat tartalmazza. Az összes Bitcoin tranzakció átvizsgálását követően született eredmény szerint az összes létező bitcoin fele volt már valaha érintett illegális tranzakcióban; valamint évi 36 millió illegális tranzakció történik, ami az összes tranzakció 44%-a, és ezek összértéke évi 72 milliárd dollár, vagyis az összes tranzakció értékének ötöde.

Az anonimitás tehát kétélű fegyver, hiszen egyrészt védheti a felhasználókat is a bűncselekményektől, másrészt a bűnelkövetés következményeinek elkerülésére is lehetőséget teremt. Az Európa Tanács 2003-ban elfogadott, az internetes kommunikáció szabadságáról szóló deklarációjának hetedik pontja szerint „az online megfigyeléssel szembeni védelem biztosítása és a szabad véleménynyilvánítás elősegítése érdekében a tagállamoknak tiszteletben kell tartania az internet felhasználók azon döntését, hogy nem azonosítják magukat." A dokumentum egyúttal hangsúlyozza, hogy ennek nem kell kiterjednie a büntetőjog szabályaiba ütköző cselekmények elkövetőire.

A probléma megoldásának egyik lehetséges módszere tehát, ha a felhasználónak valamilyen módon azonosítania kell magát bizonyos tevékenységek előtt. Dél-Koreában pl. a kommentelés volt ilyen. Itt az információs és kommunikációs törvény módosításával bevezetésre került a „valódi nevet igazoló rendszer", vagyis a leglátogatottabb – napi százezernél több egyedi látogatóval rendelkező – weboldalakat üzemeltető szolgáltatókat kötelezték arra, hogy az őket felkereső felhasználókat egy közintézmény honlapjára irányítsák, ahol személyigazolvány számuk segítségével azonosítaniuk kellett magukat, mielőtt tartalmat tehettek közzé. Ez a megoldás azonban inkább rendészeti, semmint büntetőjogi jellegű, hiszen nem a már megtörtént bűncselekmény (közzétett becsületsértő komment) nyomozására, hanem előzetesen, mintegy megelőző jelleggel került rá sor. 2012-ben a dél-koreai Alkotmánybíróság megsemmisítette a jogszabályi rendelkezést, ugyanis nemcsak súlyos beavatkozást jelentett a felhasználók magánéletébe, de nehezen betartható és kis hatékonyságú is volt. Ráadásul sok adatot kellett tárolni a felhasználókról, ami aztán az adatlopó bűnözők célpontjává tette az adatbázisokat. Az Európai Unióban a kriptovaluták közösségi szabályozása kapcsán merült fel annak lehetőséget, hogy az azokat használóknak kötelező legyen regisztráltatniuk magukat, ám maga az összegzés is megjegyezi, hogy ez némileg „tolakodóbb" megoldás, mint az önkéntes regszitráció.

Egészen másfajta megközelítéssel éltek Németországban, ahol 2011-ben kiderült, hogy a bajor bűnüldöző szervek egy trójai programot, becenevén a Bundestrojaner-t használták arra, hogy a felhasználók rendszeréhez egy titkos hátsó kaput nyissanak. A program elsőd-

leges célja a gyanúsítottak Skype hívásainak rögzítése volt, mivel az egyébként titkosítva folyik, így tartalmát csak a hívó és fogadó fél ismerheti meg. Az ilyen bűnügyi célú megfigyelés azonban törvénytelennek számít Németországban. Idehaza a büntetőeljárásról szóló 2017. évi XC. törvény 231. szakasza szerint bírói engedélyhez kötött leplezett eszköz az információs rendszer titkos megfigyelése, amely a gyakorlatban megfeleltethető ennek. Fontos azonban mérlegelni ebben az esetben, hogy a megfigyelés ideje alatt számos olyan információ derülhet ki a rendszerből, amely egyáltalán nem kapcsolódik az adott bűncselekményhez, és ez az ügyben nem érintett harmadik felek személyes adata is lehet. A németországi szövetségi alkotmánybíróság éppen ez utóbbi tényező miatt is döntött úgy 2008-ban, új alapjogként az információs önrendelkezési jogból levezeti az információs rendszer bizalmasságához és integritásához való jogot, még nehezebbé téve a rendszerek felhasználó tudta nélküli megfigyelését.

Véleményem szerint az anonimitás problémáját nem lehet úgy általános eszközökkel megoldani, hogy az ne avatkozzon bele túlságosan az átlagfelhasználók magánszférájába. Ehelyett inkább az egyes eseteknél kell különböző nyomozási technikákkal, illetve technikai eszközökkel megoldani a problémát. TOR felhasználó esetén például meg kell próbálni olyan helyzetet előteremteni, ahol a felhasználó hibát vét, és így leleplezi magát, vagy pedig más módon, pl. pszichológiai manipulációval rávenni erre.

3. Titkosítás és önvádra kötelezés tilalma

A titkosítás problematikája szorosan összefügg a már ismertetett anonimizációval, ám korántsem rokon értelmű. Az anonimizáló megoldások egy része valóban a titkosítást használja fel arra, hogy a továbbított információ tartalma, valamint a kommunikációban résztvevők ne legyenek ismertek, ám mások más módszerrel érik ezt el. A titkosítás ráadásul nemcsak a kommunikációt, hanem a rendszerben tárolt adatokat is érintheti, vagyis jóval tágabb körben alkalmazható, mint az anonimizáció. A titkosítás a mindennapi életünk része, bizonyos kommunikációk (pl. netbank) nem is lennének használhatók nélküle, hiszen egyébként bárki megismerhetné belépési adatainkat és visszaélhetne vele. A fő problémát az jelenti, hogy a titkosított adatok nem megismerhetők a nyomozóhatóság számára, így a bizonyításban sem használhatók fel. Mivel nem lehet olyan rendszert tervezni, ami szándéktól teszi függővé annak használatát, így ennek az ellentmondásnak a feloldása igen nehéz.

A modern titkosítások többsége „brute force" technikával, vagyis a lehetséges kombinációk egyesével történő végigpróbálgatásával nem törhető fel a variációk igen magas lehetséges száma miatt. Több országban is alkalmazott az a megoldás, hogy törvényben kötelezik a tikosítót arra, hogy az adatai titkosítását feloldó kulcsot a hatóság rendelkezésére bocsássa. A belga büntetőtörvénykönyv egy, míg a francia kódex 434-15-2. szakasza három, illet-

ve minősített esetben öt évig terjedő szabadságvesztéssel rendeli büntetni azt, aki megtagadja a feloldáshoz szükséges jelszó átadását a hatóságoknak. Nagy-Britanniában a 2000. évi Regulation of Investigatory Powers Act 53. szakasza nemzetbiztonsági és gyermekeket érintő ügyekben 5 évig, egyéb estekben 2 évig terjedő szabadságvesztést helyez kilátásba, ha valaki nem adja át a kulcsot a nyomozóhatóság számára. Ezek a rendelkezések a terheltre is vonatkoznak, ami felveti az önvádra kötelezés tilalmának megsértését is.

A rendelkezés támogatói az ittas vezetéshez hasonlítják a fennálló helyzetet: az intézkedés alá vont sofőr sem tagadhatja meg, hogy alávesse magát a hatósági intézkedésnek. A probléma gyökere onnan ered, hogy nem egyértelmű, a kulcs átadása már bizonyíték szolgáltatásának minősül-e. A brit felfogás szerint az adat a személy akaratától függetlenül létezik, a kulcs átadása pedig olyan, mint a vér vagy DNS, vagyis önmagában semleges adat. Ez a kötelezés sem jelent azonban egyértelmű megoldást: bizonyos programok, így például a VeraCrypt nevű program már képes úgy titkosítani adatokat, hogy maga a felhasználó sem ismeri az azt feloldó jelszót.

A kérdés az Amerikai Egyesült Államokban is felmerült, itt az Alkotmány ötödik kiegészítésébe ütközését illetően folynak a viták. 2007-ben Sebastian Boucher gyermekpornográfia birtoklásával kapcsolatos ügyében (In re Boucher, No. 2:06-mJ-91, 2009 WL 424718) a szövetségi kerületi bíróság úgy ítélte meg, hogy az ötödik kiegészítésbe ütközne, amennyiben a vádlottat köteleznék a kód megadására, ugyanis azzal beismerné, hogy rendelkezik a gépen tárolt fájlok felett. 2009-ben Sessions bíró megváltoztatta a magisztrátusi bíró döntését, és kötelezte Bouchert a jelszó átadására, arra hivatkozva, hogy az eljárás elején már megmutatta gépe tartalmának egy részét a hatóságoknak, így ez nem tekinthető önvádra kötelezésnek. 2012-ben a United States v. Fricosu ügyben a kerületi bíróság arra kötelezte a terheltet, hogy a titkosítással védett számítógépen található fájlok másolatát adja át a hatóságoknak.

Lehetséges megoldási mód még bizonyos kormányzati gyengepontok beépítése a rendszerekbe, amelyeken keresztül a hatóságok hozzáférhetnek a titkosított adatokhoz. Ezzel azonban a fő probléma az, hogy a rosszindulatú felhasználók számára támadási felületet biztosít, és idővel kiderülhet, hol sebezhető egy-egy szolgáltatás. Amennyiben eredeti funkcióját képtelen betölteni, úgy a felhasználók más alternatívák után néznek, így a titkosítást fejlesztő vállalkozások részéről is igen alacsony az együttműködési hajlandóság a hatóságokkal.

4. Adatmegőrzés és adatvédelem

Az adatoknak, mint már láthattuk, alapvető szerepe van abban, hogy a kibertérben történt elkövetést felderítsék, illetve az itt található bizonyítékok is adatként vannak jelen. A forgalmi adatoknak alapvetően három formáját különböztethetjük meg: a kommunikáció tartalmára, jellemzőire és az előfizetőre vonatkozó adatokat. Ezek összességéből kiderül, hogy az

adott kommunikáció küldője és fogadója, annak ideje és tartalma, így a küldemény teljes egészében helyreállítható, és fontos szerepe lehet egy bűntetőeljárás során. Éppen ezért kiemelten fontos, hogy az adatok elérhetők legyenek a nyomozás idején.

Az Európai Unió igyekezett válaszolni erre a kihívásra, és elfogadta a 2006/24/EK irányelvet, amely előírta a hírközlési szolgáltatásnyújtók számára, hogy mely adatokat kötelesek megőrizni, hogy ezek súlyos bűncselekmények kivizsgálása, felderítése és üldözése céljából elérhetők legyenek. Az ötödik cikk alapján a kötelezettség a kommunikációs jellemzőkkel kapcsolatos, valamint az előfizetői adatokra vonatkozik, míg a tartalmi adatokra nem. Azt az időtartamot, amíg az adatok megőrzésére kötelezhető a szolgáltató, a közléstől számított 6–24 hónapos időszakban határozta meg, valamint előírta, hogy kérelemre az adatokat az illetékes hatóságok számára haladéktalanul továbbítani kell.

Az irányelv átültetése azonban számos országban igen nehéznek bizonyult az alapjogokkal kapcsolatos kérdések miatt. 2015-ig kilenc tagállamban a helyi alkotmánybíróság megsemmisítette az instrumentumot implementáló rendelkezéseket. A döntésekben közös volt, hogy kiemelték az arányosság hiányát, annak pontos meghatározását, hogy mely szervek kérhetik a megőrzött adatok átadását, valamint a „súlyos bűncselekmények" részletesebb meghatározását. Ezt követően két előzetes döntéshozatal iránti kérelem is érkezett a Bíróság elé, a Digital Rights Ireland és Seitlinger beadványával kapcsolatban, amiket egyesítve tárgyaltak (C 293/12. és C 594/12). 2014. április 8-i ítéletében a nagytanács érvénytelennek mondta ki az irányelvet, mivel az megsértette az Európai Unió alapjogi chartájának 7. (magánélethez való jog) és 8. (személyes adatok védelméhez való jog) cikkét, és az arányosság követelményét.

A döntés következményei nem érintették közvetlenül az átültető jogszabályokat, amennyiben azt nemzeti bíróság vagy törvényhozás nem helyezte hatályon kívül, ugyanakkor konkrét kötelezettség már nincs ezek megtartására. A Tanács 2015. novemberi információi szerint tizenhat tagállamban – köztük hazánkban is – hatályban maradtak az implementáló jogszabályok, míg az hatályon kívül helyezésre 10 országban került sor. Legalább hét törvényhozás új jogszabályokat alkotott az adatmegőrzés szabályozására. Az Eurojust jelentése szerint a tagállami szabályozások széttöredezettsége súlyos következményekkel járhat az elektronikus bizonyítékok gyűjtése, és a bűnügyi együttműködése terén.

A probléma orvoslásának égető szükségességére mutat rá az EU új elektronikus bizonyítékokra vonatkozó rendelettervezete, amely számos előremutató javaslata ellenére ezt a kritikus kérdést egyáltalán nem érinti. Hiába jön létre a közlésre kötelező európai határozat jogintézménye, amikor gyakran hónapok is eltelhetnek az elkövetéstől számítva addig, amíg a bizonyítékok egyáltalán felmerülnek, és akkorra már jó eséllyel törlik azokat a szolgáltatók a rendszerükből. Mindezek alapján mihamarabb szükséges egy új, a Bíróság megállapításainak és kiemelten az arányosság elvének megfelelő szabályozás kidolgozása. Ebben különös tekintettel kell lenni a megfelelő garanciák beépítésére, amelyek biztosítják, hogy nem

történik visszaélés a személyes adatokkal. Egyúttal szükséges annak meghatározása is, hogy mely hatóságok férhetnek hozzá ezekhez az adatokhoz, és milyen esetekben.

5. Összefoglalás

A fentiekből látható, mennyire összetett és egymással összefüggő problémák alkotják a magánszféra védelme és a nyomozási érdek konfliktusát a kibertérben. Az anonimizáció, a titkosítás és az adatmegőrzés mind technikai jellegű kihívások, amelyekre a jognak megfelelő választ kell adnia. Néhol, mint például az első két problémánál, nehéz vagy inkább a lehetetlennel határos egyértelmű, általános megoldást kidolgozni. Itt elsősorban azokat a nyomozási technikákat, jó gyakorlatokat kell kidolgozni, összegyűjteni és más tagállamok hatóságaival kicserélni, amelyek a konkrét ügyekben megoldást kínálnak. Mivel a kibertérben zajló bűnözés globális probléma, fontos az ilyen szempontú hozzáállás az ott felmerülő nehézségek leküzdésére.

A bemutatott problémakörök is remekül jelzik, hogy a technológia fejlődése hogyan feszíti szét a jog megszokott kereteit, és a jogi szempontból legideálisabb megoldások sokszor egyáltalán nem, vagy csak nagyon rossz hatásfokkal működnek a kibertérben. A jövő legfontosabb kihívása nem a realitások joghoz való igazítása, amely sokszor lehetetlennek ígérkezik, hanem a jogrendszerek megfelelő átgondolása, akár nagy múltú jogintézmények elhagyása, ha azok nélkülözhetők, és csak a megoldás útjában állnak. Remek példa erre az innovatív jogi gondolkodásra a már említett elektronikus bizonyítékokról szóló rendelettervezet, amely például a joghatóság és a bűnügyi együttműködés terén hozna nagy változásokat.