DOI: 10.38146/BSZ.2018.10.2

PARTI KATALIN

Az elektronikus hírközlési szolgáltatók együttműködési kötelezettsége a büntetőeljárás során a gyakorlat tükrében

Egyre több bűncselekmény valósul meg informatikai környezetben, éppen ezért az elektronikus hírközlési (telekommunikációs és internet-) szolgáltatók egyre több megkeresést kapnak a felhasználói adatok kiadása iránt.[1] Az elektronikus hírközlési szolgáltatóknak a bűnüldözési célú adatátadással kapcsolatos jogszabályi kötelezettségeiről azért is időszerű említést tenni, mert a 2018. július 1-jén hatályba lépő új büntetőeljárási törvény (a büntetőeljárásról szóló 2017. évi XC. törvény, a továbbiakban: új Be.), valamint az elektronikus hírközlésről szóló 2003. évi C. tv. (a továbbiakban: Eht.) és az elektronikus kereskedelmi szolgáltatásokról szóló ágazati jogszabályok (2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről, a továbbiakban: Ekrtv.) is megerősítik a szolgáltatók bűnmegelőzéssel, felderítéssel és bűnüldözéssel kapcsolatos feladatait. Ezen túl az Európai Bizottság büntetőügyekre vonatkozó, elektronikus bizonyítékok átadásának meggyorsítását célzó európai rendelettervezete is 2018 áprilisában látott napvilágot. A rendelettervezet, a tagállami szabályozás egységesítése mellett, a szolgáltatókra telepítené a külföldről érkező adatmegőrzési és -átadási kérelmek jogszerűségének vizsgálatát és közvetlen teljesítését. Mindezen jogszabályi módosításokra tekintettel a jelen tanulmány célul tűzi ki a szolgáltatók bűnüldözési célú adatkezelési kötelezettségeinek áttekintését a legutóbbi törekvések tükrében.

1 Lásd például a Deutsche Telekom átláthatósági jelentését: https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/hungary-363562; továbbá Google and Apple report jump in requests for user data. BBC News, Oct 2, 2017. https://www.bbc.com/news/technology-41442857; valamint Stephen Nellis: Apple sees steep increase in US national security-related data requests. Businessinsider.com, May 25, 2018. http://www.businessinsider.com/apple-nsa-data-request-transparency-report-2018-5

A szolgáltató együttműködési kötelezettsége a büntetőeljárás során

Az elektronikus hírközlési szolgáltatók együttműködési kötelezettségét az adatok átadására a büntetőeljárás során a büntetőeljárásról szóló törvény írja elő [új Be. 244. § (6) bek.]. A büntetőeljárási célú adatkérésen túl létezik még rendészeti (bűnmegelőzési, felderítési) [Rtv. 68. § (1) bek.] és nemzetbiztonsági, honvédelmi célú adatkérés is, amelyek rendjét külön ágazati törvény [Nbtv. 41. § (1) bek. l) pont], valamint az Eht. [Eht. 92. §; 155. § (5) bek.] szabályozza. A szolgáltató együttműködési kötelezettségét a büntetőeljárás során az elektronikus adat ideiglenes hozzáférhetetlenné tétele kényszerintézkedés és az elektronikus adat végleges hozzáférhetetlenné tétele szankció (régi Be. 158/A §; új Be. 335. §; Btk. 77. §) végrehajtásában az Eht. 92/A §-a szabályozza. A szolgáltató és a felsorolt szervek közötti, büntetőeljárási, felderítési, nemzetbiztonsági és honvédelmi célú együttműködés részletes rendjét a 180/2004. (V. 26.) kormányrendelet (a továbbiakban: kormányrendelet) szabályozza[2].

A büntetőeljárásról szóló törvény tartalmazza azoknak a szerveknek a megnevezését, amelyek megkereséssel fordulhatnak a szolgáltatóhoz adatkérés céljából [új Be. 262. § (1) bek.], ezek a következők: a nyomozó hatóság és a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve, valamint a rendőrség terrorizmust elhárító szerve. Az új Be. rendelkezése, hogy az arra feljogosított szervek kizárólag az ügyészség engedélyével kérhetnek adatszolgáltatást a törvényben meghatározott szervektől, egyebek mellett az elektronikus hírközlési szolgáltatótól [új Be. 262. § (1) bek. c) pont]. Megjegyzendő, a 1998. évi XIX. törvény szerint a nyomozó hatóságnak a büntetőeljáráson belüli adatkéréseihez (nyílt eljárásban) nem volt szüksége ügyészi engedélyre.

A jelen tanulmány elkészítéséhez interjúkat készítettem a Nemzeti Nyomozó Iroda munkatársaival és a nagyobb telekommunikációs szolgáltatókkal. Mind a nyomozó hatóság, mind pedig a szolgáltatók kifejezték szkepticizmusukat a tekintetben, hogy az új Be. által megkívánt ügyészi engedélyezési rendszer teljesíthető lesz anélkül, hogy ez szükségtelenül megnövelné az adminisztrációt és az adatkiadási időt.

2 180/2004. (V. 26.) kormányrendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről.

Az elektronikus hírközlési szolgáltatók *adatmegőrzési és -átadási kötelezettsége,* az általuk kezelt adatok körére, meghatározott célra és időintervallumra az elektronikus hírközlésről szóló törvényben szabályozott (Eht. 159/A §). A nagyobb telekommunikációs szolgáltatók (Magyar Telekom, Vodafone, Pannon, Telenor, UPC) bűnmegelőzési és bűnüldözési célból kötelesek megállapodást kötni a rendőrséggel, ügyészséggel, nemzetbiztonsági célból pedig a Belügyminisztériummal arról, hogy milyen módon engedik a rendszerükön átmenő adatok átadását, azaz milyen módon és feltételekkel (jogszabályi és formai követelmények) működnek közre az automatikus adatkérések teljesítésében (kormányrendelet 3. §). A rendőrség és a titkosszolgálatok kihelyezett tisztek segítségével tartják a kapcsolatot a telekommunikációs szolgáltatókkal. (Ezek olyan titkos megállapodások, amelyek utaló jelleggel sem megismerhetők a nyilvánosság számára.)

Az automatikus adatátadási rendszer

Az *automatikus (elektronikus) adatátadási rendszer* kidolgozására az elektronikus közigazgatás projekten belül került sor – a NAV, a TEK, az ORFK, a BRFK és az ügyészség esetében. De nem minden, nyomozati jogkörrel felruházott hatóságnál van lehetőség automatikus adatkérésre, ezt technikai és szervezeti okok indokolják. Az ügyészséget például direkt interfész köti össze a szolgáltatóval, ezen keresztül az ügyész maga kereshet, közvetlenül a szolgáltató adatbázisában. Ez a nyomozó hatóság automatikus megkeresési rendszerénél (Robotzsaru) is direktebb, gyorsabb keresést tesz lehetővé, elektronikus formanyomtatványok kitöltése nélkül.

Az automatikus adatkérések előtt a nagyobb szolgáltatóknál hozzávetőlegesen ötven-ötven ember kellett az adatok manuális leválogatásához, a papíron és telefaxon érkező adatkiadás iránti kérelmek kiszolgálásához. Ma, az automatikus adatkérések idején a hatósági megkeresésre kiadandó adatok leválogatásához csupán átlagosan öt ember kell szolgáltatónként. Az automatikus adatkérést a nagy szolgáltatók és az ORFK között kiépült dedikált interfészek teszik lehetővé. A rendőrség a Robotzsaru hálózaton keresztül használja ezt a rendszert, itt húsz-harminc adatkérési *template* áll rendelkezésre, ezt kitöltve az adatok lehívhatók a szolgáltató rendszeréből. Ebben a rendszerben nemcsak a lekérés, hanem a keresés is automatikus, emberi beavatkozást nem igénylő tevékenység (telekommunikációs szolgáltatók, nyomozó hatóság, interjúk).

Szükségességi és arányossági generálklauzula az adatkérések teljesítésére

Ilyen generálklauzula az adatkérés ügyészi engedélyezése, amelyet az új Be. vezet be [új Be. 262. § (1) bek.]. [Az új Be. 261. § (1) bekezdése szerint bíróság adatkérése esetén ügyészi engedélyre nincs szükség.] Az új Be. vezeti be a szükségességi és arányossági [új Be. 264. § (4) bek.], a célhoz kötöttségi [új Be. 264. § (4) bek.] klauzulákat is, valamint az adattörlési kötelezettséget [új Be. 264. § (5) bek.] az adatkérés céljával össze nem függő adatra vonatkozóan. Ugyancsak az új Be. szerint az érintettet tájékoztatni kell az adatkérésről, amely tájékoztatás elhalasztható, ha a büntetőeljárás eredményességét veszélyeztetné [új Be. 264. § (7) bek.]. A szolgáltató az adatkérés tényéről és tárgyáról másnak nem, csak az érintettnek adhat tájékoztatást [új Be. 264. § (7) bek.].

A szolgáltatók adatmegőrzési és -átadási kötelezettségének kiterjesztése az alkalmazásszolgáltatókra

A telekommunikációs és internetszolgáltatókat kötelezettség terheli a nemzetbiztonsági és a bűnüldözési feladatokat ellátó hatóságok irányában metaadatok és kommunikációs (tartalmi) adatok kiadására vonatkozóan. Az Ekrtv. 2016-os módosítása következtében a metaadatokat az *alkalmazásszolgáltatók* is kötelesek megőrizni, legfeljebb egy évig, illetve megkeresésre átadni a hatóságoknak (Ekrtv. 13/B §). Ennek megszegése estére szankciók is kiszabhatók (Ekrtv. 16/H §). A módosítás indokolása szerint *„a technikai fejlődés következtében az internet alapú globális kommunikációs rendszerek, valamint ezen szolgáltatások egyre szélesebb körben terjednek el és megfizethető áron vehetők igénybe, így reális veszélyt jelent, hogy az általános kommunikációs szokások megváltoznak, és a hagyományos hírközlési szolgáltatók helyett ezen szolgáltatásokat veszik igénybe a bűnözői körök. Tekintettel arra, hogy a mobiltelefonok kommunikációjának védelmét ellátó rendszernek egyik elemét képező mobiltelefonos alkalmazás az egyes alkalmazásszolgáltatók interneten elérhető, kereskedelmi céllal létrehozott felületén megtalálható, onnan telepíthető, így kivédhető, hogy az egyes országok szolgálatai a kommunikációt, vagy az ahhoz kapcsolódó információkat megszerezhessék, valamint dekódolhassák. A probléma megoldását jelentheti az alkalmazásszolgáltatókra vonatkozó jogi kötelezettségeknek az előírása. [...] Az Ekrtv.*

módosításának célja az Ekrtv. hatálya alá tartozó szolgáltatók adatmegőrzési, adatszolgáltatási és együttműködési kötelezettségének megteremtése. Az Ekrtv.-t érintő módosítási javaslat egyrészt megteremti annak a lehetőségét, hogy a szolgáltató köteles legyen megadni mindazokat az adatokat és információkat, amelyek a titkos információgyűjtés eszközeinek, módszereinek alkalmazásához nélkülözhetetlenek, így a titkosítási szintet érintő információkat is, másrészről pedig a módosítás a szolgáltató részére kötelező jelleggel írja elő a Nemzetbiztonsági Szakszolgálattal történő, a titkos információgyűjtés feltételeit érintő megállapodások megkötését."[3]

Szankció a szolgáltatóval szemben

Büntetőeljárásban rendbírsággal sújtható a szolgáltató, illetve minden, *„az adatkérés keretében megkeresett szervezet",* ha a kérelemben foglaltakat határidőn belül (alapesetben harminc, sürgős esetben nyolc nap) nem teljesíti (telekommunikációs szolgáltatók, interjú), annak teljesítését alaptalanul megtagadja, vagy az adatkérésről történő tájékoztatás szabályait megszegi (például a büntetőeljárás eredményességét veszélyeztetve tájékoztatja az adatkéréssel érintett személyt vagy az adatkérésről másnak is tájékoztatást nyújt – tehát túllépi a tájékoztatási jogkörét) [új Be. 265. § (1) bek.]. Ha annak feltételei fennállnak, akkor a szolgáltatóval szemben kényszerintézkedés – a kért adatok lefoglalása, illetve az adatkérések teljesítéséért felelős személy letartóztatása – is alkalmazható [új Be. 265. § (1) bek.].

Amennyiben a hozzáférést biztosító elektronikus hírközlési szolgáltató nem teljesíti kötelezettségét az elektronikus adat ideiglenes vagy végleges hozzáférhetetlenné tétele tekintetében, úgy a felügyeletet gyakorló Nemzeti Média- és Hírközlési Hatóság rendbírságot szabhat ki a szolgáltatóval szemben [Eht. 92/A § (3) bek.].

A szolgáltató titoktartási kötelezettsége

Az elektronikus hírközlési szolgáltatókat titoktartási kötelezettség terheli a titkos információgyűjtéshez nyújtott, törvényben meghatározott közreműködésük mivoltát illetően. Ezt két jogszabály határozza meg: az elektronikus hírköz-

3 Indokolás a T/10307. számú törvényjavaslathoz, a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról. https://itcafe.hu/dl/cnt/2016-04/127478/10307.pdf

lési szolgáltatóknak a titkos információgyűjtésben való közreműködését előíró 180/2004. (V. 26.) kormányrendelet és a 2009. évi CLV. törvény a minősített adat védelméről (Mavtv.). *„A titkos információgyűjtéssel összefüggő tevékenység végzésében, valamint a monitoring alrendszer, berendezés telepítésében, üzemeltetésében, rendszerfelügyeletében, javításában, karbantartásában az a személy vehet részt, aki az Nbtv.-ben meghatározott nemzetbiztonsági ellenőrzésen megfelelt és rendelkezik az elektronikus hírközlési szolgáltató vezető tisztségviselője által az NBSZ egyetértésével kiadott megbízással”* (kormányrendelet 13. §). A biztonsági feltételekről a Mavtv. rendelkezik: *„Elektronikus biztonsági intézkedéseket kell tenni az elektronikus rendszeren kezelt minősített adat és az elektronikus rendszer bizalmassága, sérthetetlensége és rendelkezésre állása érdekében”* [Mavtv. 10. § (7) bek.]. Az adathoz hozzáférő, együttműködő személy „személyi biztonsági tanúsítványt” kap, amelyet a Nemzeti Biztonsági Felügyelet bocsát ki [Mavtv. 17. § (2) bek. a) pont].

Az elektronikus hírközlési szolgáltatónak a titkos információgyűjtésben közreműködő tagja titoktartási kötelezettsége megszegésének esetén „minősített adattal visszaélés” bűncselekményéért felel [Btk. 265. § (3) bek.]: *„Az a minősített adat felhasználására törvény alapján jogosult személy, aki a minősített adattal visszaélést korlátozott terjesztésű, bizalmas, titkos vagy szigorúan titkos minősítésű adatra követi el [...] két évtől nyolc évig terjedő szabadságvesztéssel büntetendő.”* Az előkészület és a gondatlan alakzat is büntetendő.

Az átadott adatok integritásának védelme

Az elektronikus hírközlési szolgáltatás rendszeréből kinyert, avagy „elektronikus adat” többféle módon juthat el a nyomozó hatósághoz: *a)* az automatikus adatkérési rendszerben; *b)* a szolgáltató manuális lekérése, leválogatása esetén adathordozón (régebben CD, DVD, ma már inkább pendrive); *c)* titkos információgyűjtésre kiépített monitoring-alrendszeren keresztül – ilyenkor először a minősített adatok titkosítását fel kell oldani (új Be. 256–260. §). Az automatikus adatkérési rendszerben megszerzett adat időbélyegzővel és elektronikus aláírással ellátva kerül a nyomozó hatósághoz. A szolgáltató által átadott adathordozót és a titkos információgyűjtés során megszerzett adatot tartalmazó adathordozót először lefoglalja a nyomozó hatóság, majd hiteles másolatot készít róla, amelyet eljuttat az informatikai szakértőhöz. A szakértő véleményével ellátott hiteles másolatnak lesz bizonyító ereje a büntetőeljárásban. A bíróság a közvetlenség elve alapján a tárgyalásra beidézhe-

ti az adatszerzésben közreműködőt – a nyomozó hatóságnak a házkutatáskor, lefoglaláskor jelen lévő tagját vagy a Nemzetbiztonsági Szakszolgálat titkos információgyűjtésben részt vevő tagját –, aki szóban, tanúként válaszol a bíróság kérdéseire. A kérdések az adat megszerzését, illetve a megszerzés körülményeit is érinthetik. A bíróság előtt tett tanúvallomás a bizonyítás része, de nem bővíti a bizonyítékok körét (hacsak a vallomással összefüggésben új bizonyítékra nem derül fény).

A dinamikus IP-cím kiadása

Lehetséges dinamikus IP-címek lekérése, mind a szolgáltató megkeresésével, mind pedig az automatikus adatkérés rendszerében. A feltétele, hogy nagyon pontosan meg kell tudni határozni, milyen időintervallumra nézve szeretné leválogatni az adott IP-címhez tartozó felhasználói kört az arra jogosult szerv. Lehetséges, hogy egyetlen dinamikus IP-címet két nap alatt harminc felhasználó használt, ebből a körből hosszadalmas munkával – azonosítás, tanúkutatás stb. – lehetséges leválogatni a büntetőeljárás szempontjából releváns személyeket. Az, hogy a dinamikus IP-cím az automatikus rendszeren keresztül lekérdezhető-e, függ az országrész mobil- és/vagy vezetékestelefon-szolgáltatással való lefedettségétől. Ha egyetlen IP-cím sok felhasználóhoz kapcsolódhat rövid időn belül, akkor az arra jogosult szervek inkább megkereséssel élnek a szolgáltatónál, amely manuálisan teljesíti a leválogatást. Ha a nyomozó hatóság megkeresése a „szokásostól eltérő" széles felhasználói körre vagy „a szokásostól eltérő", túlságosan hosszú időre vonatkozik, a szolgáltató ezt a kérést is teljesíti, nem bírálhatja felül a hatóság célját. Elegendő a lekérés/megkeresés céljának megnevezése (milyen bűncselekmény miatt, milyen ügyben van szükség a kért adatokra), a szolgáltató nem bírálja felül a hatóság kérését, és nem szűkíti önkényesen az adatok körét (telekommunikációs szolgáltatók, interjúk). A nyomozó hatóság által kért felhasználói adatok nemcsak közvetlen bizonyításra, hanem a nyomozás irányának meghatározására (verzióállítás) is felhasználhatók.

Az adatkérés teljesítésének megtagadása

A gyakorlatban nem jellemző, hogy a bűnüldözési, honvédelmi, vagy nemzetbiztonsági célú adatkérést megtagadja a szolgáltató. Ennek megvan a for-

mája és a tartalmi kellékei (jogszabályi hivatkozás, célhoz kötöttség), amit betart a megkereső. Egy alkalommal azért utasította vissza az egyik nagy telekommunikációs szolgáltató a rendőrség adatkiadás iránti megkeresését, mert azt csak az ügy előadója írta alá és nem a felettese. Az aláírás pótlásával azonban az adatkiadás megtörtént. Ez egy évekkel ezelőtti adatkérés volt, még papíralapon nyújtotta be a nyomozó hatóság a megkeresést – a ma hatályos, automatikus adatkérési rendszer még nem működött. Ahogy a technika fejlődik, egyre inkább marad el a papíralapú ügyintézés, ezzel együtt a nyomozó hatóság olyan adatokat is lekér, amelyek körét a jogszabály (az Eht.) konkrétan nem szabályozza. Erre példa, hogy korábban csak papíralapú ügyfélszerződések köttettek, de ma már elektronikusan is köthető felhasználói szerződés (webshopon keresztül). Az elektronikus úton megkötött szerződéseken nincs ügyfélaláírás, így azok másolata nem szolgál bizonyítékul, csak az IP-címek, amelyeket a szerződés megkötésekor használt az ügyfél. Ezen a ponton egyeztetésre volt szükség a nyomozó hatósággal: a webshopba való belépéskor használt IP-cím vagy a webshopban, navigálással töltött időintervallumban kiosztott dinamikus IP-címekre van-e szükség a bizonyításhoz. Ilyen és ehhez hasonló kérdésekben folyamatos a nyomozó hatósággal való egyeztetés.

A szolgáltató dekriptálási (titkosításfeloldási) kötelezettsége

Az elektronikus hírközlési szolgáltató dekódolási kötelezettségét előírják a jogszabályok. Az együttműködési kötelezettség körébe tartozik a szolgáltató titkosításfeloldó kötelezettsége is, amennyiben a titkosítást a szolgáltató (és nem maga a felhasználó) végezte [új Be. 264. § (2) bek.]. Az új Be. minden, „az adatkéréssel megkeresett szervezetet", tehát az elektronikus hírközlési szolgáltatót is kötelezi az adatok titkosságának feloldására: *„A rejtjelezett vagy más módon megismerhetetlenné tett adatot az adatkérés keretében megkeresett szervezet köteles az átadás vagy a közlés előtt eredeti állapotába visszaállítani, illetve az adatszolgáltatást kérő szerv számára az adat tartalmát megismerhetővé tenni"* [új Be. 264. § (3) bek.].

A szolgáltató a titkos információgyűjtés keretében is köteles biztosítani, hogy a lehallgatás során az arra jogosult szervek az általa titkosított vagy tömörített információt az eredeti formájában ismerhessék meg: *„Amennyiben az elektronikus hírközlési szolgáltató az előfizető által kezdeményezett vagy foga-*

dott kommunikáció tartalmát bármely módon megváltoztatja, kódolja vagy tömöríti, a kommunikáció tartalmán a visszaalakított, dekódolt vagy tömörítés előtti alakot kell érteni" [kormányrendelet 6. § (2) bek.]. A *felhasználó* által titkosított kommunikáció dekódolására azonban a szolgáltató nem kötelezhető.

2016 óta hatályos az Ekrtv.-nek az a módosítása, amely az alkalmazásszolgáltatókat kötelezi a nem végpontok között, hanem a szerveroldalon titkosított üzenetek tartalmának megőrzésére és a titkos információgyűjtésre jogosult szerv megkeresése esetén történő átadására.[4] A törvény értelmében az alkalmazásszolgáltató *„az a természetes, illetve jogi személy vagy jogi személyiséggel nem rendelkező más szervezet, aki, vagy amely elektronikus hírközlő hálózat felhasználásával valamilyen szoftverhez vagy hardverhez való hozzáférést, szoftveres alkalmazást, valamint kapcsolódó szolgáltatásokat biztosít specifikus szoftveren vagy webes felületen több felhasználó számára [...]"* [Ekrtv. 2. § m) pont].

A törvénymódosítás bevonja a törvény hatálya alá a nemzetközi vállalatok Magyarországon elérhető online szolgáltatásait is [Ekrtv. 2. § g) pont].

A végpontok közötti *(end-to-end)* titkosítást kínáló szolgáltatók kötelesek megőrizni, és a külső engedélyhez kötött titkos információgyűjtésre jogosult szervek megkeresésére átadni a forgalmi (meta-) adatokat és az üzenetek tartalmát is (Ekrtv. 3/B §).

A szabályozás szerint a szolgáltatónak csak akkor kellene dekriptálnia az üzenetek tartalmát, hogyha *nem végpontok* között folyna a kommunikáció (ilyen alkalmazás például a Signal), hanem a szolgáltató szerverén keresztül.[5] Ami az alkotmányosság tesztjének való megfelelést illeti, a szabályozás éppen az előbbiek miatt az alkalmasság tesztjén bukna el, hiszen a bűnelkövetők, a terrorcselekmények megvalósítói nagy valószínűséggel a végpontok közötti titkosító alkalmazásokat veszik igénybe, amely esetben a szolgáltatónak nincs dekriptálási kötelezettsége.

A jogalkotó ezzel a rendelkezéssel gondolhatott például a 2015 novemberében, San Bernardinóban történt terrortámadásra, amelynek során az öngyilkos merénylők iPhone-ját nem sikerült feltörnie az NSA-nak, és ebben a szolgáltató sem segített. Ebben az időszakban történt az az eset, amikor Brazíliában letartóztatták a Facebook egyik dolgozóját, mert a Facebook megtagadta egy WhatsApp-üzenet dekriptálását. Ugyanebben az időszakban az Egyesült Királyságban is olyan törvényjavaslatot nyújtottak be, amely tiltotta volna az ano-

4 Megállapította a 2016. évi LXIX. tv. 45. § (3) bek., hatályos 2016. július 17-től.

5 Dornfeld László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle, 2018/2., 115–135. o.

nim és titkosított üzenetváltást lehetővé tevő applikációk alkalmazását. Jellemző azonban, hogy a magyar jogalkotó egyfajta folyamatos visszavonulást végzett a témában, és ennek a következménye volt a hivatkozott szabályozás bevezetése. A magyar jogalkotó első ötlete nagyon merész volt, például bűncselekménnyé nyilvánították volna a végpontok közötti titkos kommunikációt lehetővé tevő alkalmazások (így például a Signal) használatát. Ehhez az eredeti elképzeléshez képest a jogalkotó fél év alatt folyamatosan hátrafelé lépdelve adta fel kezdeti radikális elképzeléseit a kriminalizációra. Volt egy olyan verzió is, amely szerint kötelezték volna a szolgáltatókat a végpontok között titkosan folytatott kommunikáció tartalmának a megőrzésére. Ennek a folyamatnak a végén maradt a jelenleg hatályos, 2016-ban bevezetett, a nem végpontok közötti titkosított üzenetek dekriptálásának a kötelezettsége.[6]

Az elektronikus hírközlési szolgáltatókra az alkalmazásszolgáltatókat érintő szabályozás csak akkor vonatkozhatna, ha maguk is kínálnának csevegőszolgáltatásokat. Jelenleg a hírközlési szolgáltatónak nincs titkosításfeloldó kötelezettsége a rendszerét használó, úgynevezett Over The Top (OTT) applikációszolgáltatások keretében folyó kommunikáció tartalmára. Ezt úgy lehetne kiküszöbölni, ha az OTT applikációszolgáltató szerződést kötne az elektronikus hírközlési szolgáltatóval az infrastruktúrája használatára. A másik lehetőség, hogy az elektronikus hírközlési szolgáltató létrehozná a maga applikációit, és a vele szerződő felhasználóknak csak az általa kínált applikációkat engedné használni a mobilinternet-szolgáltatáson keresztül. Ebben az esetben a szolgáltató az általa kínált applikációk tekintetében is érvényesítené a törvényes lehallgatás és az adatmegőrzési kötelezettségeit, azaz ezekre is vonatkozna az applikációban folyó kommunikációra a titkosításfeloldási kötelezettség. A saját applikációk létrejöttéig és azok letöltésének exkluzív felhasználói jogosultságokhoz kötéséig azonban erre nincs sem technikai, sem jogi lehetőség.

Kölcsönös jogi segítségnyújtás a telekommunikációs adatok átadása terén

Az elektronikus hírközlési szolgáltatás, vagy számítástechnikai eszköz vagy rendszer útján továbbított kommunikációnak az érintett személy tudta nélkül, leplezett módon történő megismerése és rögzítése végett előterjesztett *eljárá-*

6 A Társaság a Szabadságjogokért álláspontja a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló törvény tervezetéről, 2016. https://tasz.hu/files/tasz/imce/a_tasz_allaspontja_a_terrorizmus_elleni_fellepessel_osszefuggo_egyes_torvenyek_modositasarol_szolo_torveny_tervezeterol.pdf

si jogsegély iránti megkeresést az ügyész a Be. bírói engedélyhez kötött titkos adatszerzésre, illetve az egyéb adatszerző tevékenység során végezhető titkos információgyűjtésre vonatkozó szabályai szerint hajtja végre (lásd az Európai Unió tagállamai közötti bűnügyi együttműködésről szóló 2012. évi CLXXX. törvény 69/E §). Az eljárási jogsegély iránti megkeresés akkor teljesíthető, ha tagállami hatóság a saját államának joga szerint engedéllyel rendelkezik. Ha a megkeresésbeli adatszerzés bírói engedélyhez kötött titkos adatszerzés keretében hajtható végre Magyarországon, akkor a megkeresésről az ügyész indítványára a nyomozási bíró határoz. Ha a bíró elutasítja a megkeresési indítványt, akkor az ügyész tájékoztatja erről a tagállami igazságügyi hatóságot. Az eljárás iránti megkeresés eredménye vagy az eljárási cselekmény befejezését követően (rögzített adat formájában), vagy közvetlen továbbítással irányítható át a megkereső állam eszközére, ha annak technikai feltételei megvannak. Az ügyész a megkereső tagállam kérésére itt is elrendelheti az adatok írásba foglalását.

A Magyarországon tartózkodó személy megfigyelésére irányuló eljárási jogsegély iránti megkereséseket a Fővárosi Főügyészség bírálja el a szerint, megvannak-e a magyar jogban a titkos információgyűjtés feltételei. Erről a bíró a kézhezvételtől számított 96 órán belül dönt, de szükség esetén ez a határidő további 8 nappal meghosszabbítható.

Ha a Magyarországon folyamatban lévő büntetőeljárással érintett személy nem tartózkodik Magyarországon, de az elektronikus kommunikációja megfigyeléséhez nem szükséges a tartózkodási helye szerinti tagállam közreműködése, akkor az ügyész az érintett kilétének felfedését követően haladéktalanul tájékoztatja a tartózkodási hely szerinti tagállamot. Ha a tagállam 96 órán belül (vagy határidő-hosszabbítás esetén 12 napon belül) arról tájékoztatja az ügyészt, hogy nemzeti joga szerint nincs lehetőség a titkos megfigyelésre, vagy a már végrehajtott titkos megfigyelés eredménye nem vagy csak meghatározott feltételekkel használható fel, az ügyész a Be. alapján megteszi a szükséges intézkedéseket. Ha az ügyész ezzel nem ért egyet, akkor az Eurojust közreműködésével egyeztetést kezdeményezhet.

A jövő: külföldi nyomozó hatóság adatkérésének közvetlen kiszolgálása?

Az Európai Unió tagállamaival folytatott bűnügyi együttműködésről szóló 2012. évi CLXXX. törvény 65/A–65/D és 69/E, 65/H § alapján nincs lehető-

ség arra, hogy az elektronikus hírközlési szolgáltató a külföldről érkező adatkéréseket közvetlenül, a nemzeti kontaktpont (Nebek) bevonása nélkül teljesítse. A nemzetközi bűnügyi jogsegélyről szóló 1996. évi XXXVIII. törvény 4. § (2) szerint a bűnügyi jogsegélyt a miniszter vagy a legfőbb ügyész teljesíti.

Ahhoz, hogy a szolgáltatók közvetlenül ki tudják szolgálni a külföldi hatóságok adatok iránti megkereséseit, egyértelmű és átfogó jogszabályi háttérre lenne szükség. Azonban az állami szuverenitás, a nemzetbiztonsági érdekek elsőrendűsége, valamint az elektronikus hírközlési vagy kereskedelmi szolgáltatók piaci szerepe mind akadályokat gördít a jelen idejű kéréskiszolgálás megvalósulásának útjába.

Az Európai Bizottság 2018. április 17-én terjesztette elő a büntetőügyekre vonatkozó, elektronikus bizonyítékok közlésére és megőrzésére kötelező európai rendelettervezetet[7] (a továbbiakban: rendelettervezet), valamint az ezzel szorosan összefüggő, a jogi képviselőknek a büntetőeljárásban bizonyítékok összegyűjtése céljából történő kinevezéséről szóló irányelv tervezetét.[8] A jelen tanulmány készítésének idején folyamatban van a magyar kormányzat álláspontjának kialakítása a két tervezettel kapcsolatban, ezeket a Hírközlési Érdekegyeztetési Tanácson keresztül véleményezésre kiküldték az elektronikus hírközlési szolgáltatást nyújtó vállalatok számára. Jelenleg nincs jogszabályi felhatalmazásuk a hírközlési szolgáltatóknak, hogy a szuverén államok erre feljogosított hatóságai helyett vizsgálják, van-e alapja a külföldi megkereső fél kérésének. Előállhat egy olyan helyzet, amely szerint az európai rendelettervezet előírja a szolgáltatónak, hogy külföldi kéréseket is közvetlenül fogadjon és teljesítsen, miközben a helyi (nemzeti) jogszabályok szerint az adott ügyben erre jelenleg nincs lehetőség, hiszen hiányzik a nemzeti jogalap, vagy egyenesen veszélyezteti a nemzetbiztonságot a külföldi hatóság által kért adatok kiadása (minősített adat). Ehhez járul, hogy a hírközlési szolgáltató piaci szereplő, nem tartozik a szolgáltatása körébe sem a külföldi megkeresés jogalapjának, sem a forrásának (tudniillik hogy a kibocsátójának van-e jogköre az adatkérésre) vizsgálata, ezt jelenleg a kölcsönös jogsegélykérelmeket teljesítő szervek végzik el. A rendelettervezet kikapcsolná a jogsegélykérelmek teljesítéséből a hatóságokat, és a jogalap vizsgá-

7 Javaslat az Európai Parlament és a tanács rendelete a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról COM/2018/225 final – 2018/0108 (COD). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN

8 Javaslat az Európai Parlament és a tanács irányelve a jogi képviselőknek a büntetőeljárásban bizonyítékok összegyűjtése céljából történő kinevezéséről szóló harmonizált szabályok meghatározásáról COM/2018/226 final – 2018/0107 (COD). https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vknmikug23z1

latát a szolgáltatókra bízná. Jelenleg ennek nincsenek meg sem a jogi, sem a technikai feltételei. A rendelettervezet által előrevetített hatósági kontroll hiányát nem oldaná meg a hozzá csatolt *Melléklet az adatkiadás közvetlen teljesítéséről szóló formanyomtatványokról* sem.

Konklúzió

A bizonyítékszerzés terén egyre nagyobb szerep hárul az elektronikus kereskedelmi és hírközlési szolgáltatókra, hiszen a rendszerükben kezelt adattömeg akár egy egyszerű bűncselekmény esetén is fontos bizonyítékul szolgálhat. Az Európa Tanács számítástechnikai bűnözésről szóló (budapesti) egyezménye[9], az eddigi legátfogóbb nemzetközi dokumentum a számítástechnikai rendszerben tárolt adatok átadásának rendjét illetően is iránymutatást ad a tagállamok számára. A szolgáltatót érinti egyebek mellett a számítástechnikai adat gyors megőrzésére és részbeni átadására kötelezés szakasza.[10] Az Európai Bizottság jelen tanulmányban ismertetett, új rendelettervezete ennek a szakasznak a nemzetközi bűnügyi együttműködésben való érvényesülését hivatott biztosítani az adatok gyorsabb átadása érdekében. Kérdés, hogy a szolgáltató, piaci szereplőként kötelezhető-e a hatáskörének ilyen mértékű kiterjesztésére, és ha igen, hol marad a jogállamiság *(rule of law)* megvalósulása.

9 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt számítástechnikai bűnözésről szóló egyezményének kihirdetéséről

10 17. Cikk, Forgalmi adat gyors megőrzése és részbeni átadása.