



Elektronikus bizonyítékok az időprésben

Electronic Evidence under Time Pressure

Csizner Zoltán

Dr., PhD, tanszékvezető, rendőr ezredes
Nemzeti Közszerológiai Egyetem,
Rendészettudományi Kar
csizner.zoltan2@uni-nke.hu



Absztrakt

Cél: Digitalizálódott életünkben a bűncselekmények felderítése és bizonyítása során megkerülhetetlen az elektronikus adatok bizonyítékként történő felhasználása. Ez különösen igaz a kibertérben vagy azzal összefüggésben elkövetett bűncselekmények esetén, melyek meghatározóvá váltak az elmúlt években. A privát életünk védelme ugyanakkor megköveteli az adatok kezelésének időbeli korlátozását, ami miatt az igazságügyi hatóságoknak rövid idő alatt kell intézkedniük ezek beszerzésére. Még nehezebb a bizonyítékok határon átnyúló beszerzése, melynek eddig alkalmazott módszerei lassúak, nehézkesek és gyakran adatvesztéseket eredményeznek. Az EU 2023-ban fogadta el azt a normacsomagot, mely az elektronikus bizonyítékok határon átnyúló beszerzését hivatott egyszerűsíteni. A 2026. augusztus 18-tól alkalmazandó rendelet és az érvényesülését elősegítő irányelv tíz napra rövidíti majd a bűnügyi adatkéréseket, de ehhez ki kell alakítani az előírt feltételrendszert. A tanulmány ezt a normacsomagot, illetve a végrehajtandó feladatokat mutatja be az eredményes felkészülés érdekében.

Módszertan: A szerző hazai és nemzetközi jogi normák alapján, gyakorlati tapasztalatok figyelembevételével vizsgálta az elektronikus bizonyítékok határon átnyúló beszerzését és az új szabályozás fontosabb pontjait. A tanulmány ismerteti a jelenleg hatályos jogszabályok nyújtotta lehetőségeket, és részletesen bemutatja a rendelet által megteremtett új szabályozási környezetet. Ismerteti az adatok megőrzésére és közzétételére kötelező határozatokat, az adatok körét,

A szerző a kéziratot magyar nyelven nyújtotta be. Benyújtás: 2025. 06. 22. Átdolgozás: 2025. 07. 20.
Elfogadás: 2025. 07. 25.



valamint az érintett szolgáltatók és hatóságok feladatait. Értékeli a rendelet alkalmazásához szükséges feltételeket, összevetve azokat a jelenlegi hazai viszonyokkal. Végezetül felhívja a figyelmet olyan feladatokra, amelyek teljesítése szükséges a rendeletben foglaltak végrehajtásához.

Megállapítások: A jövőben bevezetendő adatkérési lehetőség várhatóan egyszerűsíti, gyorsítja és hatékonyabbá teszi a bűncselekmények nyomozását. Ugyanakkor több kérdés is felmerül, amelyek megválaszolása befolyásolja majd a rendelet hazai alkalmazását. Ezek közé tartozik a sürgős esetben történő adatkérésre való jogosultság és a nyomozó hatóságnak nem minősülő szervek adatkérési lehetősége.

Érték: A tanulmány – mely részletesen bemutatja az alkalmazásra váró új szabályozást – hasznos segédlet lehet a jogalkotók és jogalkalmazók számára, mind a felkészülés, mind a későbbi alkalmazás időszakában.

Kulcsszavak: adatmegőrzés, határon átnyúló adatkérés, elektronikus bizonyíték, kiberbűncselekmény

Abstract

Aim: In our increasingly digital lives, the use of electronic data as evidence has become indispensable in the detection and proof of crimes. This is especially true for crimes committed in or related to cyberspace, which have become increasingly prevalent in recent years. At the same time, the protection of private life requires that data processing be time-limited, necessitating rapid action by judicial authorities to obtain such data. Cross-border acquisition of evidence is even more challenging, as the methods used so far have proven to be slow and cumbersome, often resulting in data loss.

In 2023, the EU adopted a legislative package aimed at simplifying the cross-border acquisition of electronic evidence. The regulation, which will apply from August 18, 2026, and the accompanying directive intended to support its implementation, will reduce the time frame for e-evidence requests to 10 days. However, this requires the establishment of the necessary legal and procedural framework. This study presents the legislative package and outlines the tasks to be carried out to ensure effective preparation.

Methodology: The author examined the cross-border acquisition of electronic evidence and the key points of the new regulation based on domestic and international legal norms and practical experience. The study describes the opportunities provided by the currently applicable legislation and presents in detail the new regulatory environment created by the regulation. It covers the decisions mandating the preservation and disclosure of data, the scope of the data involved,

as well as the responsibilities of the relevant service providers and authorities. It also evaluates the conditions necessary for the implementation of the regulation, comparing them to the current domestic situation. Finally, it highlights tasks that must be completed for the effective implementation of the regulation.

Findings: The forthcoming data request mechanism is expected to simplify, accelerate, and enhance the efficiency of criminal investigations. However, several questions arise that will influence the domestic application of the regulation. These include the right to request data in urgent cases and the possibility for bodies that are not classified as investigative authorities to make such requests.

Value: This study, which provides a detailed overview of the new regulation to be implemented, can serve as a useful guide for legislators and legal practitioners, both during the preparation phase and throughout the subsequent application period.

Keywords: data disclosure, cross-border information exchange, electronic evidence, cyber-crime

Bevezetés

Az elmúlt évtizedekben soha nem látott módon változtak a köznyugalmat zavaró, fenyegető cselekmények. A múlt század végén a szervezett bűnözés és a terrorizmus által kiváltott erőszakhullámok, az ezredfordulót követően a politikai, gazdasági és környezeti válságövezetekből menekülő emberek milliói, majd legújabban az információs térben jelentkező veszélyek alakították biztonságérzetünket. A bűncselekmények kibertérbe tolódása, a digitalizált kommunikáció, az IoT-eszközök¹ térnyerése vagy a virtuális pénzügyi tranzakciók a bűnügyi nyomozás és bizonyítás rendszerét is megváltoztatták. Miközben ebben a digitális korszakban az elektronikus bizonyítékok szerepe egyre jelentősebb, addig a nyomozások során történő beszerzésük – különösen, ha erre határon átnyúló eljárások keretében kerülne sor – egyre bizonytalanabbá és nehezebbé válik.

A klasszikus nemzetközi bűnügyi együttműködési formák csak korlátozottan képesek az elektronikus bizonyítékok határon átnyúló beszerzésére, ami az adatmegőrzés jogi és időbeli korlátai miatt az adatok elvesztéséhez vezethet.

Az Európai Unió (a továbbiakban: EU) ezt felismerve 2023 nyarán egy normacsomagot fogadott el, mely alkalmas a tagállamok igazságügyi hatáságai és

1 Internet of things (dolgok internete): olyan hálózatban összekapcsolt fizikai eszközök, járművek, készülékek hálózata, amelyek érzékelőkkel, szoftverekkel és más technológiákkal kiegészítve lehetővé teszik az adatok gyűjtését és továbbítását, a felhasználók tájékoztatását vagy egyes műveletek automatizálását. Forrás: <https://www.ibm.com/think/topics/internet-of-things>

az EU-ban elérhető szolgáltatók közötti közvetlen, gyors és teljes bizonyítóerővel rendelkező adatcseréjére. A csomagnak két pillére van:

- az Európai Parlament és a Tanács által 2023. július 12-én elfogadott, a büntetőeljárás során az elektronikus bizonyítékokkal kapcsolatban, valamint a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából kibocsátott, közlésre kötelező európai határozatokról és megőrzésre kötelező európai határozatokról szóló, 2023/1543 rendelet (a továbbiakban: Rendelet), mely 2026. augusztus 18-án lép hatályba;
- ennek végrehajthatóságát támogató, az Európai Parlament és a Tanács által 2023. július 12-én elfogadott, a büntetőeljárásban az elektronikus bizonyítékok gyűjtése céljából a kijelölt telephelyek kijelöléséről és a jogi képviselők kinevezéséről szóló harmonizált szabályok meghatározásáról szóló 2023/1544 (EU) irányelv (a továbbiakban: Irányelv), amit a tagállamoknak 2026. február 18-ig kell a nemzeti jogba átültetni.

A Rendelet hatékony eszköz lehet az igazságügyi szervek kezében, de annak végrehajtásához a hátralévő közel egy évben több feltételt is meg kell teremteni. Tanulmányomban a normacsomag által nyújtott lehetőségeket és a működéséhez szükséges feltételrendszert kívánom bemutatni.

Az elektronikus adat fogalma, adatmegőrzés szabályozása, az adatvesztés veszélye

A bűncselekmények felderítésének, bizonyításának egyik alapeleme az adat. Egy emberölés esetében például az áldozat által utoljára hívott telefonszám, a helyszínről elmenekülő gépkocsi rendszáma, vagy a tanúk által a tettesről adott személyleírás mind-mind a nyomozást segítő adat, amelyről később derül ki, hogy valójában releváns vagy sem, azaz, hogy bizonyítékká válhat-e. Az adatok beszerzéséhez fel kell kutatni azok forrásait, melyek közül az objektívebb kategóriába tartoznak az elektronikus adatokat tároló rendszerek, adatbázisok. Míg a tanúk felkutatása és kihallgatása jellemzően szubjektív adatokat eredményez (maga az észlelés sem tökéletes, később az emlékek is torzulnak, végül a hatóság általi megismerésük, azaz a kihallgatás is nagyban függ az abban részt vevő személyektől), addig az elektronikus adatok mindvégig objektívek maradnak. Egy telefon híváslistája független az azt megkérő személytől és a lekérdezés időpontjától, az mindvégig változatlan marad. Az már egy másik kérdés, hogy ki, milyen új ismereteket, következtetéseket tud megállapítani ezekből az adatokból a feldolgozás, elemzés eredményeként.

Az elektronikus adat a büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: Be.) 205. §-a szerint *„a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja”*, amit eltérő rendelkezés hiányában tárgyi bizonyítási eszköznek kell tekinteni.

Az elektronikus adatok közös tulajdonsága, hogy fizikailag nem léteznek, nem „foghatók kézbe”. Megőrzésük, tárolásuk vagy továbbításuk csak valamilyen eszköz igénybevételel történhet (Wang, 2022). Ebből eredően vizsgálatuk sem történhet közvetlenül, ehhez valamilyen módon láthatóvá, megismerhetővé kell tenni azokat.

Digitalizált életünk egyre több, a bűnügyi nyomozásban felhasználható elektronikus adatot termel, melyek egy része bizonyítékként is felhasználható. A mobiltelefonok adatai (előfizetői adatok, hívások adatai, földrajzi adatok) mellett az internethasználatlal összefüggő adatok (IP-címek, doménnevek, feljelentkezések adatai, forgalmi adatok), vagy az IoT-k technikai adatai mind-mind relevánsak lehetnek egy bűncselekmény felderítése vagy nyomozása során. Nyitra Endre ezt így fogalmazza meg: *„Az adat vonatkozásában egyre gyakrabban lehet hallani azt, hogy ez a 21. század olaja, a gazdaság egyik mozgatórugója. Így van ez a rendészet területén is, hiszen adat, információ nélkül nehezen tudjuk megismerni a múltbeli, a jelenben zajló vagy a jövőben elkövetni kívánt releváns eseményt. Az adat (információ) az e-nyomozási folyamatok alapját is képezi.”* (Nyitrai, 2025).

Az információ felértékelődésével a mindennapi életünkben egyre nagyobb szerepet tölt be a kommunikáció és a hírközlés. Emiatt az adatok jelentős része is ezekhez a szolgáltatásokhoz kapcsolódva keletkezik. Az új szabályozás is ezt a változást tükrözi.

A pénzügyi szolgáltatások – úgymint banki, hitelezési, biztosítási és viszontbiztosítási, foglalkozási vagy magánnyugdíj, értékpapír, befektetési alapokkal kapcsolatos, fizetési és befektetési tanácsadás jellegű szolgáltatások – nyújtása során keletkező elektronikus adatok megőrzésére, kezelésére és átadására külön szabályok vonatkoznak. A tanulmány ezért ezeket nem érinti, mint ahogy a bemutatásra kerülő új szabályozás sem vonatkozik ezekre.

Másik oldalról viszont pont az adatok túltermelődése nehezíti a lényeges adatok felismerését és kiválasztását, mivel sokszor egyetlen entitást (például egy hívószámot) kell tüként megtalálni a tíz- vagy százazres adatsorból álló szénakazalban. Ezért a releváns adatok elvesztésének megakadályozása érdekében a hatóságok inkább szélesebb körben szerzik be az adatokat, melyből a nyomozás során lehetőségük lesz kiválasztani a valóban lényegeseket. Ez a folyamat

hatalmas méretű adatbázisok keletkezését és adatok konkrét cél nélküli kezelését eredményezi.

A velünk kapcsolatban elérhető adatok mennyiségének és típusainak folyamatos bővülése a privát létünk sérülékenyebbé válását eredményezte. Ezért, a magánszféra védelme érdekében korlátok közé kellett szorítani ezeknek az adatoknak a beszerzését, tárolását, leginkább pedig visszaszorítani a konkrét cél nélküli, készletező adatkezelést.

Az elektronikus hírközlési adatvédelmi irányelv (2002/58/EK irányelv) és annak 2006-os módosítása (2006/24/EK irányelv) szabályozta az adatok megőrzési idejét, és fél évtől két évig terjedő időtartamban állapították meg. Az irányelv rendelkezéseit a hírközlési törvény ültette át a hazai jogba, és ennek értelmében a szolgáltatók adatmegőrzési kötelezettsége 2008. március 15-től a megvalósult hívások esetében egy évre, míg a sikertelen hívások esetében fél évre módosult [2003. évi C. tv. 159/A. §. (3) bekezdés].

Az EU Bírósága 2014-ben az uniós joggal ellentétesnek nyilvánította a 2006-os módosító irányelvet, mivel álláspontja szerint az általános jellegű adatmegőrzés sérti a magánélet tiszteletben tartásához és a személyes adatok védelméhez fűződő alapvető jogokat ([URL1](#)). A döntés hatására volt ország, ahol megszüntették az adatmegőrzést (Ausztria, Hollandia, Románia), volt, ahol az erre vonatkozó törvény végrehajtását felfüggesztették (például Németország), és volt olyan, ahol változatlanul hagyták a szabályozást, mint ahogyan Magyarországon is. A tagállamok többségében az adatokat továbbra is 6–12 hónapig köteles a szolgáltató megőrizni, és törvényben meghatározott célból az arra feljogosított hatóságnak átadni.

Az jól látszik, hogy a jelen állapot eléggé kaotikus, miután a megőrzési időt meghatározó irányelv megsemmisítése megkérdőjelezi az adatmegőrzés jogszerűségét is, ugyanakkor a terrorizmus fenyegetése, illetve a bűnözés súlypontjának kibertérbe történő áttolódása nélkülözhetetlenné teszi az elektronikus adatok rendelkezésre állását. Több ország a GDPR (2016/679 EU rendelet) konkrét tiltásának hiányára hivatkozva hagyta meg az adatmegőrzés lehetőségét, de ehhez egy felhatalmazás lenne a valódi megoldás. Az EU ugyan 2017-ben megkezdte az elektronikus hírközlési adatvédelmi irányelv kiváltását az úgy nevezett E-privacy rendelet javaslatának megfogalmazásával ([URL2](#)), de az a jogalkotási folyamat 2021-ben leállt. Végül az Európai Bizottság a 2025-ös munkatervében a közös megállapodás esélytelensége miatt vissza is vonta ([URL3](#)), és a több éves munka végeredménye csak egy megszövegezett javaslat maradt. A hírek szerint 2025 nyarán egy újabb szabályozás előkészítése kezdődik majd el az EU-ban, de egy konkrét szabályozás hatályba lépése várhatóan még hosszú időt vesz igénybe.

A jelenlegi helyzetben egy-egy bűncselekménnyel összefüggő elektronikus adat – a pénzügyi szolgáltatások során keletkező adatokat ide nem értve – korlátozott ideig, általában egy évig áll rendelkezésre. Ez idő alatt kell ezeket az adatokat kezelő szolgáltatótól megszerezni, függetlenül attól, hogy az az eljáró hatósággal azonos országban, egy EU-n belüli másik tagállamban, vagy esetleg azon kívüli (harmadik) ország területén működik. Az adatkérések hatékonyságát tovább nehezíti, hogy gyakran csak több lépcsőben lehet a valóban releváns adathoz eljutni, ami akár más-más szolgáltató, más-más országban történő, egymás utáni megkeresését jelenti. Az EU felmérése szerint a tagállamokban folytatott nyomozások 85%-ában bizonyítékká válik valamilyen elektronikus adat, amelyek közel fele csak nemzetközi együttműködés keretében szerezhető be ([URL4](#)).

Amennyiben egy releváns adatot a megőrzési időn belül nem sikerül megkérni, úgy az az adat végérvényesen elveszik, és a felderítés vagy bizonyítás során már nem számolhatunk vele. Emiatt különösen fontos az adatkérések mielőbbi célba juttatása, és a szolgáltatók válaszadási hajlandóságának fokozása.

A jelenlegi helyzetben egy tagállami hatóság egy másik állam területén lévő szolgáltatótól három módon tudja az adatokat beszerezni:

- Az EU-n kívüli állam területén lévő szolgáltató esetén a legbiztosabb – de időben leghosszabban megvalósuló – módja az adatkérésnek a bűnügyi jogsegély, melynek alapja a nemzetközi bűnügyi jogsegélyről szóló törvény (1996. évi XXXVIII. törvény).
- Egy másik EU-tagállam területén lévő szolgáltató esetén alkalmazható a tagállamok közötti, kölcsönös elismerés elvén alapuló egyszerűsített bűnügyi együttműködés (2005. évi CXVI. törvény), amit az EU Tanácsának a közös nyomozó csoportról (Joint Investigation Team, JIT) szóló 2002/465/IB. kerethatározata, majd az Európai Parlament és a Tanács 2014/41/EU számú irányelve az európai nyomozási határozat (ENYH) jogintézményével tovább egyszerűsített. Ezek az együttműködési formák ugyan egyszerűsítettek a bizonyítékok határon átnyúló gyorsabb beszerzését, de az elektronikus bizonyítékok esetében még mindig körülményesek és nehézkesek maradtak.
- Egyes esetekben a szolgáltatók – egyéb tilalom hiányában – a más ország eljáró hatóságától közvetlenül hozzájuk érkezett megkeresést saját belátásuk szerint megválaszolják. Ez a fajta önkéntes teljesítés hasznos és gyors, de teljes mértékben a szolgáltató hozzáállásától függ, ami miatt nagy a bizonytalansági faktor benne.

Az elektronikus bizonyítékok nemzetközi együttműködés keretében történő beszerzését az elhúzódó eljárások mellett tovább bonyolítja a megőrzésre vonatkozó eltérő jogi szabályozás is, hiszen van olyan tagállam, ahol az adatok

egyáltalán nem kerülnek megőrzésre. Ezekben az esetekben a megkeresések eleve eredménytelenek, hiszen nem létező adatokra vonatkoznak.

A jelenlegi helyzetet a Rendelet így foglalja össze: „A 2014/41/EU európai parlamenti és tanácsi irányelv lehetővé teszi, hogy ENYH-t bocsássonak ki bizonyítékoknak egy másik tagállamban történő gyűjtése céljából. Ezen túlmenően a Tanács által az Európai Unióról szóló szerződés 34. cikkének megfelelően létrehozott, az Európai Unió tagállamai közötti kölcsönös büntügyi jogsegélyről szóló egyezmény [...] szintén lehetőséget biztosít arra, hogy egy másik tagállamtól bizonyítékot kérjenek. Előfordulhat ugyanakkor, hogy az ENYH-t létrehozó 2014/41/EU irányelvben és a kölcsönös büntügyi jogsegélyről szóló egyezményben megadott eljárások és határidők nem megfelelőek elektronikus bizonyítékok esetén, amelyek volatilisabb természetűek, továbbá könnyebben és gyorsabban törölhetők. Az elektronikus bizonyítékok beszerzése az igazságügyi együttműködés csatornáinak igénybevételeivel gyakran hosszú ideig tart, ami olyan helyzeteket eredményezhet, amelyekben a későbbi nyomok már nem elérhetők. Ezenfelül nincs harmonizált jogi kerete a szolgáltatókkal való együttműködésnek, noha egyes harmadik országbeli szolgáltatók elfogadják a tartalmi adatoktól eltérő adatokra irányuló közvetlen megkereséseket az alkalmazandó nemzeti joguk által megengedett mértékben. Ennek következményeként a tagállamok egyre inkább a szolgáltatókkal kialakított közvetlen önkéntes együttműködési csatornákra támaszkodnak, ha ilyen rendelkezésre áll, és különböző nemzeti eszközöket, feltételeket és eljárásokat alkalmaznak.” (Rendelet 8. pont).

A Rendelet tartalma

Az elektronikus bizonyítékok határon átnyúló beszerzésének nehézségeit felismerve az EU 2017-ben egy nyilvános konzultációt kezdett, melyre a tagállamok többsége érdemi állásfoglalással reagált. Ezek alapján 2019-ben kétirányú előkészítő munkáról született döntés. Az egyik az USA-val folytatandó tárgyalásokat ([URL5](#)), a másik a 2001-es Budapesti Egyezmény² második kiegészítő jegyzőkönyvének a megalkotását tűzte ki célul. Míg az USA-val a tárgyalások még mindig zajlanak, addig a kiegészítő jegyzőkönyv elkészült, és azt 2021. november 17-én az Európa Tanács Miniszteri Bizottsága el is fogadta ([URL6](#)). A kiegészítő jegyzőkönyv eredményeként született meg 2023. július 12-én a Rendelet, és az annak végrehajtását támogató Irányelv.

2 A Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezmény (Convention on cybercrime), amit Magyarországon a 2004. évi LXXIX. törvény hirdetett ki.

A Rendelet két lényeges – az alábbiakban részletesen bemutatott – eljárási keretet szabályoz. Az egyik alapján a Rendelet hatálya alá tartozó szolgáltató kötelezhető bizonyos elektronikus adatok megőrzésére, míg a másik alapján pedig kötelezhető ezeknek az adatoknak az átadására. A Rendelet normál esetben tíz napos válaszadási határidőt ír elő, mely valóban alkalmas lehet a hatékony bizonyítékszerzésre. Az így beszerzett bizonyítékot vagy egy konkrét bűncselekmény miatt folytatott nyomozásban lehet felhasználni, vagy pedig egy már kiszabott, szabadságelvonással járó büntetés foganatosítása érdekében. Az új szabályozás nem érinti sem a pénzügyi tevékenységgel összefüggő adatokat, sem pedig a tagállamon belüli adatkérést. Utóbbi esetén egy eljáró hatóság továbbra is az adott állam jogrendje szerint kérheti az adatokat az országa területén letelepedett vagy képvisellel rendelkező szolgáltatótól.

A megkérhető adatok köre

A Rendelet az elektronikus bizonyítékok körébe a 2.2 pontban jelzett részletezett szolgáltatások nyújtása során keletkezett releváns adatokat sorolja, és három csoportba – előfizetői, forgalmi és tartalmi adatokra – osztja. Az előfizetői adatokkal egy elbírálás alá esnek azok a forgalmi adatok is, melyeket kizárólag a felhasználó személy azonosítása céljából kérnek meg.

Az adatok közlésére vagy megőrzésére kötelezés csak olyan adatokra irányulhat, melyeket a szolgáltató a határozat kézhezvételkor a rendszerében tárol. A határozatok nem írhatnak elő általános megőrzési kötelezettséget (azaz nem teszi lehetővé a készletező adatgyűjtést), és nem vonatkozhatnak a határozat kézhezvételét követően tárolásra kerülő adatok kifürkészésére vagy beszerzésére. A szolgáltató mentesül az alól is, hogy a titkosított formában tárolt adatokat vissza kelljen fejtenie (Rendelet 19–20. pont). Ez jelentős eltérés a hazai szabályozástól, hisz a Be. 264. § (3) bekezdése előírja a titkosított vagy más módon megismerhetetlenné tett adatok eredeti állapotba történő visszaállítása kötelezettségét.

A Rendelet annyiban korlátozza még a megkérhető adatok körét, hogy a határozatok csak az Európai Unióban nyújtott szolgáltatásokkal összefüggésben keletkezett adatokra bocsátható ki. Ebből adódóan egy EU-ban letelepedett külföldi szolgáltatótól az EU-n kívül nyújtott szolgáltatásával kapcsolatban továbbra is vagy nemzetközi bűnügyi jogsegély, vagy az önkéntes teljesítés alapján kérhető adat. A megkérhető adatok típusait a tanúsítványok részletesen felsorolják.

Az előfizetői adatok köre és a kizárólag a felhasználó azonosítását szolgáló adatok

Az előfizetői adatok köre eléggé pontosan körülírható, ebbe tartoznak az ügyfél által szolgáltatás megrendelésekor megadott személyes és kapcsolattartási adatok, illetve az igénybe vett szolgáltatás adatai:

- előfizető vagy ügyfél neve, születési ideje, postai vagy földrajzi címe, számlázási és fizetési adatok, elérhetőségei (telefonszám, e-mail cím);
- a szolgáltatás kezdete, típusa, tartalma; valamint
- a szerződés és az ahhoz bemutatott okmányok másolatai, technikai adatok (például PUK kód).

Vannak azonban olyan adatok, melyek egyaránt alkalmasak a szolgáltatást igénybe vevő személy azonosítására és a további szokások, kapcsolatok felderítésére is. Ilyenek lehetnek például az IP-címek, más azonosítókkal való hozzáférések, esetleg az ezekhez kapcsolódó további olyan adatok, mint például a forráspontok és az időbélyegzők.

A Rendelet ezekben az esetekben – bár ugyanarról az adatról van szó – különbséget tesz a felhasználás célja, és ezáltal az alapvető jogokra gyakorolt hatásuk alapján. Amennyiben az adatokra kizárólag az adott szolgáltatást használó személy azonosítása érdekében van szükség, úgy egy elbírálás alá esik az előfizetői adatokkal, és előzetes ügyészi hozzájárulással is kibocsátható a határozat. Egyéb esetben ezek az adatok a forgalmi adatok körébe tartoznak, és már előzetes bírói hozzájárulást igényel a beszerzésük.

A forgalmi adatok köre

A forgalmi adatok – az előző pontban szereplő adatok kivételével – az adott szolgáltatónál keletkező, vagy a rendszerükben kezelt olyan technikai információk, amelyek egy adott szolgáltatás nyújtásával kapcsolatban keletkezhetnek. Ilyenek például:

- ki küldte, vagy ki kapta az üzenetet,
- a használt eszköz azonosítója és helye,
- a kapcsolat időpontja, időtartama, mérete (adatforgalma), helyszíne,
- a használt technikai beállítások (például protokoll, tömörítés),
- internethasználattal kapcsolatos adatok (IP-címek, naplófájlok).

A tartalmi adatok köre

A tartalmi adatok körét a Rendelet értelmező rendelkezése nem egy taxatív felsorolással határozza meg, hanem gyakorlatilag ide tartozik minden digitális forgalmú adat, ami nem minősül előfizetői vagy forgalmi adatnak. A tanúsítványok ebben az esetben is segítenek, és a nyomtatványon felkínálnak pár kiválasztható kategóriát, mint például a „*mailbox dump, a felhasználó által előállított online tárolási dump, oldaldump, üzenetek naplója, hangüzenet-dump, szervertartalom, készülék backup, kapcsolatok*” adatokat.

Az érintett szolgáltatók

A Rendelet megfogalmazása szerint érintett szolgáltató bármely természetes vagy jogi személy, aki vagy amely – a pénzügyi szolgáltatások kivételével – a következő szolgáltatáskategóriák közül egyet vagy többet nyújt az EU egy vagy több tagállamában:

- elektronikus hírközlési szolgáltatás;
- internetes doménnév- és IP-szám szolgáltatások (például IP-címek kiosztása, doménnév-nyilvántartási szolgáltatások, doménnév-nyilvántartói szolgáltatások és doménnevekhez kapcsolódó titkosítási és proxyszolgáltatások);
- az információs társadalom bármely – általában térítés ellenében, távolról, elektronikus úton és a szolgáltatást igénybe vevő egyéni kérelmére nyújtott – szolgáltatása, ami lehető teszi:
 - a) felhasználóik számára az egymással való kommunikációt, vagy
 - b) adatok tárolását vagy más módon történő kezelését azon felhasználók nevében, akiknek a szolgáltatást nyújtják, feltéve, hogy az adattárolás meghatározó eleme a felhasználó részére nyújtott szolgáltatásnak (Rendelet 3. cikk 3. pontja).

Az érintett szolgáltató meghatározásánál fontos szempont lesz, hogy milyen jelentéssel bír a „*szolgáltatást nyújt az EU területén*” meghatározás. Az indokolás alapján több szempontot is vizsgálni kell majd az érintett szolgáltatói szerep megállapításához. Így nem tartozik majd a Rendelet hatálya alá, aki nem biztosítja felhasználói számára az egymás közötti kommunikációt, vagy nem nyújt lehetőséget adatok tárolására, kezelésére, illetve az adattárolás nem lesz meghatározó eleme a szolgáltatásnak (Rendelet 27. pont). Ugyanígy egy online interfész pusztá elérési lehetősége (például egy szolgáltató honlapjának vagy e-mail címének a hozzáférhetősége) önmagában még nem eredményezi egyértelműen az érintettséget (Rendelet 29. pont).

Ugyancsak fontos vizsgálandó körülmény lesz ebben a témakörben, hogy van-e a szolgáltatónak érdemi kapcsolata az EU-val. A Rendelet szerint ez a kapcsolat fennáll, ha a szolgáltató az EU-ban telephellyel rendelkezik. Ennek hiányában az érdemi kapcsolatot megalapozhatja egy vagy több tagállamban található jelentős számú felhasználó, továbbá az egy vagy több tagállamot célzó tevékenység megléte (Rendelet 30. pont).

Biztos, hogy ezek a kevésbé konkrét meghatározások az egyes tagállamokban eltérő gyakorlatot eredményeznek majd, de azért a nyomozásokban felhasználásra kerülő elektronikus bizonyítékok többsége egyértelműen olyan szervezetektől származik, melyek kategorikusan besorolhatók az érintett szolgáltatói körbe.

A közlésre kötelező európai határozat és tanúsítvány (KKEHT) és a megőrzésre kötelező európai határozat és tanúsítvány (MKEHT)

A határozatoknak a szolgáltató (és szükség esetén a végrehajtó hatóság), valamint a kibocsátó és hitelesítő hatóság és ügyszámaiknak a megnevezése mellett tartalmazniuk kell az érintett felhasználó és a megőrzésre kért adatok azonosítására alkalmas adatokat (személyes adatok, egyedi technikai azonosítók), a megőrzésre kért adatok Rendelet szerinti besorolását (előfizetői, felhasználó azonosítását szolgáló, forgalmi vagy tartalmi), a megőrizni kért adatok időtartományát, a büntetőjogi hivatkozást és a megőrzés szükségessége és arányossága feltételeinek meglétét igazoló indokolást.

A szolgáltató által kezelt releváns elektronikus adatok megőrzésére kötelező határozatot – ami megtiltja az adatok eltávolítását, törlését vagy módosítását – csak az adatok átadására irányuló kölcsönös jogsegély, ENYH vagy közlésre kötelező európai határozat érdekében lehet kibocsátani. A megőrzésre irányuló határozat csak azokra az adatokra vonatkozhat, melyeket a szolgáltató a kézhezvétel időpontjában tárolt, és nem rendelkezhet később keletkező adatok megőrzéséről.

A közlésre kötelező európai határozatot a Rendelet I. melléklete szerinti „*közlésre kötelező európai határozat tanúsítvány*” (KKEHT) nyomtatvány, míg a megőrzésre kötelező európai határozatot a Rendelet II. melléklete szerinti „*megőrzésre kötelező európai határozat tanúsítvány*” (MKEHT) nyomtatvány megküldésével kell közölni. A tanúsítványokat vagy az EU, vagy a címzett szolgáltató telephelye szerinti tagállam valamely hivatalos nyelvén kell megküldeni. A fordítási költségek csökkentése, illetve a kapcsolattartás egyszerűsítése érdekében a Rendelet szorgalmazza az tanúsítványok formanyomtatványainak előre történő lefordítását és ezek alkalmazását.

Az MKEHT és a KKEHT kibocsátásának feltételei

A határozatokat csak arra jogosult kibocsátó hatóság, kizárólag a Rendeletben megállapított ügyekben és az előírt előzetes hozzájárulás megléte esetén terjesztheti elő. Ebből adódóan ennek a három feltételnek a konjunktív teljesülése szükséges.

A kibocsátásra felhatalmazott hatóságok

A Rendelet szerinti kibocsátó hatóságok:

- az adott ügyben hatáskörrel rendelkező bíró, bíróság, nyomozási bíró vagy ügyész; vagy
- ügyész vagy bíró előzetes hozzájárulásával a kibocsátó állam belső joga szerint az adott ügyben bizonyítékgyűjtés elrendelésére hatáskörrel rendelkező, nyomozó hatósággént eljáró illetékes hatóság [Rendelet 4. cikk (1) bekezdés].

Magyarországon a Be. szerint mind a Nemzeti Védelmi Szolgálat, mind a Terrorelhárítási Központ (TEK) jogosult előkészítő eljárásra, de nem minősülnek nyomozó hatóságnak. Kérdés, hogy ezek a szervezetek vajon megfelelnek-e a Rendelet szerinti kibocsátó hatóság kritériumainak. Ha a hangsúly a nyomozó hatóságon lesz, akkor nem. Azonban, ha elegendő a bizonyítékgyűjtés elrendelésére való jogosultság, akkor igen. Szerintem ez is egy olyan kérdés, melyet érdemes lenne előzetesen tisztázni. Különösen azért is, mert a határozatok kibocsátásának alapjául szolgáló bűncselekmények egy része kimondottan a terrorizmussal összefüggő, így a TEK kiemelten érdekelt lehet az adatkérésekben.

A bűncselekménnyel szemben támasztott követelmények

A Rendelet a kért intézkedés típusától és az egyes adatköröktől függően eltérő feltételeket állapít meg az eljárás alapjául szolgáló bűncselekménnyel, vagy a végrehajtásra váró ítélettel szemben.

Megőrzésre kötelező határozat kibocsátására – amennyiben a rá vonatkozó nemzeti jog szerint a kibocsátó hatóság azt egy hasonló belföldi ügyben, azonos feltételek mellett is kibocsáthatná – bármilyen bűncselekmény vonatkozásában, vagy legalább négy hónapos, nem a vádlott távollétében kiszabott szabadságvesztés-büntetés vagy szabadságelvonással járó intézkedés esetén van lehetőség. Megőrzés esetén a Rendelet nem tesz különbséget az egyes adatkörök között.

Közlésre kötelezés esetén az előfizetői adatok és kizárólag a használó azonosítását szolgáló adatok megkérésre bármilyen bűncselekmény vonatkozásában vagy legalább négy hónapos, nem a vádlott távollétében kiszabott szabadságvesztés-büntetés vagy szabadságelvonással járó intézkedés esetén van lehetőség.

Az előzőbe nem tartozó fogalmi és tartami adatok már szenzitívebbek, így a Rendelet szigorúbb feltételekhez köti a megismerhetőségüket, azaz a közlésre kötelezést. Ezek az alábbi bűncselekmények miatt indult eljárásban, vagy azok miatt kiszabott ítéletek esetében kérhetők:

- olyan bűncselekmény esetén, melynek büntetési tételének felső határa legalább három év;
- részben vagy egészben információs rendszer felhasználásával elkövetett alábbi bűncselekmények:
 - a) információs rendszerekkel kapcsolatos csalás, materiális és immateriális készpénz-helyettesítő fizetési eszközök csalárd felhasználásával kapcsolatos bűncselekmények és a készpénz-helyettesítő fizetési eszközök csalárd felhasználása [(EU) 2019/713 irányelv 3–8. cikk];
 - b) szexuális bántalmazással kapcsolatos bűncselekmények, szexuális kizsákmányolással kapcsolatos bűncselekmények, gyermekpornográfiával kapcsolatos bűncselekmények, gyermekkel való, szexuális céllal történő kapcsolatfelvétel bűncselekménye [(EU) 2011/92 irányelv 3–7. cikk];
 - c) információs rendszerekhez való jogellenes hozzáférést, rendszert érintő jogellenes beavatkozást, adatot érintő jogellenes beavatkozást, jogellenes adatszerzést megvalósító bűncselekmény [(EU) 2013/40 irányelv 3–8. cikk];
- terrorista bűncselekmények, terrorista csoporthoz kapcsolódó bűncselekmények, terrorista bűncselekmény elkövetésére való nyilvános uszítás, terroristák toborzása, terrorista kiképzésben részesítés, terrorista kiképzésben való részvétel, terrorizmus céljából való utazás, terrorizmus céljából való utazás szervezése vagy egyéb módon történő elősegítése, a terrorizmus finanszírozása, terrorista tevékenységekhez kapcsolódó egyéb bűncselekmények [(EU) 2017/541. irányelv 4–12. és 14. cikk];
- a fenti bűncselekmények miatt kiszabott, legalább négy hónapos, nem a vádlott távollétében kiszabott szabadságvesztés-büntetés vagy szabadságelvonnással járó intézkedés végrehajtása érdekében, amennyiben az elítélt szó-késben van [Rendelet 5. cikk (4) bekezdés].

A bűncselekmények esetében a megőrzésre és közlésre kötelezés lehetősége kiterjed mind a bűnsegedekre és felbujtókra, mint ahogyan a kísérleti szakra is.

Az előzetes igazságügyi hitelesítés

Mind a megőrzésre, mind a közlésre kötelező határozatok kibocsátásához igazságügyi hatóság előzetes hitelesítését (jóváhagyását) követeli meg a Rendelet.

Az előfizetői és kizárólag a használó azonosítását szolgáló forgalmi adatok közlésére, vagy bármilyen típusú adat megőrzésére kötelező határozatot legalább ügyészi hozzájárulással lehet kibocsátani.

Az előzőkbe nem tartozó forgalmi és tartalmi adatok közléséhez bírósági felülvizsgálat (bírói, nyomozó bírói hozzájárulás) szükséges (Rendelet 36. pont), és ez független a kibocsátó vagy a végrehajtó hatóság tagállamában érvényes engedélyezési szintektől. Így attól függetlenül, hogy Magyarországon az elektronikus hírközlési szolgáltatás során keletkező forgalmi adatok (például egy mobiltelefon híváslistája) büntetőeljárásban történő beszerzése nem kötött bírói engedélyhez, a Rendelet szerinti beszerzésükhöz már szükség lesz hozzá.

Az előzetes hitelesítések körében két sürgősségi kivétel van az alábbi feltételek egyidejű teljesülése esetén:

- vagy előfizetői (ideértve a tényleges használó megállapítást célzó forgalmi) adatok közlésére, vagy bármilyen típusú adat megőrzésére irányul a kért intézkedés;
- a kért intézkedésre igazoltan sürgős esetben kerül sor;
- az igazságügyi hatósági (ügyészi) előzetes hitelesítés (hozzájárulás) az időben nem szerezhető be;
- a kibocsátó hatóság hasonló ügyben a rá vonatkozó nemzeti jog alapján előzetes ügyészi engedély nélkül jogosult ilyen adatok beszerzésére (Rendelet 37. pont).

Hazánkban a Be. 262. § (1) bekezdés c) pontja szerint az elektronikus hírközlési szolgáltatóktól az adatkérés – mind az előfizetői, mind a forgalmi és tartalmi adatok esetében – alapvetően ügyészi engedélyhez kötött, de az előzetes engedélyezéssel járó késedelem veszélye esetén e nélkül is kérhető. Ebben az esetben az ügyészség engedélyét utólag kell beszerezni.

Felmerülhet a kérdés, hogy ez a szabályozás vajon megfelel-e a Rendelet kritériumának, és a magyar hatóságok sürgős esetekben kérhetnek-e majd előzetes ügyészi engedély nélkül előfizetői adatokat külföldi szolgáltatótól? A kérdést két oldalról lehet megközelíteni.

Az első megközelítés szerint az a lényeg, hogy a Be. alapján az adatok nem ügyészi engedély nélkül szerezhetők be, hanem az, hogy sürgős esetben a beszerzéshez elegendő az ügyész utólagos engedélye, de az semmiképp sem mellőzhető. Így a hazai kibocsátó hatóság – a nemzeti jog szerint – ügyészi hozzájárulás nélkül nem rendelkezik felhatalmazással ilyen adatok beszerzésére.

A második megközelítésnél szó szerint olvassuk a Rendelet szövegét, miszerint: „...az illetékes hatóságok kivételesen kibocsáthatnak közlésre kötelező európai határozatot [...] vagy megőrzésre kötelező európai határozatot az érintett

határozat előzetes hitelesítése nélkül, amennyiben a hitelesítés nem szerezhető be időben, és ha az említett hatóságok hasonló belföldi ügyben előzetes hitelesítés nélkül is kibocsáthatnak határozatot” (Rendelet 4 cikk (5) bekezdés).

Ebben az esetben az előzetes hitelesítés nélküli jogosultság a fő kérdés, ami viszont teljesül hazánkban. Mivel a Rendelet is megköveteli a 48 órán belüli utólagos ügyési hitelesítést, úgy gondolom, hogy biztosított az igazságügyi kontroll és ezáltal érvényesülnek az alapvető jogok. Álláspontom szerint a hazai kibocsátó hatóságok ezek alapján jogosultak lesznek élni ezzel a felhatalmazással.

Határidők

A KKEHT alapján az érintett szolgáltató alapesetben 10 napon belül lesz köteles választ adni a megkeresésre [Rendelet 10. cikk (2) bekezdés], amit sürgős esetben nyolc órán belül kell teljesítenie [Rendelet 10. cikk (4) bekezdés]. A Rendelet a sürgős esetek körébe sorolja a személyek életét, testi épségét vagy biztonságát közvetlenül fenyegető veszélyhelyzeteket, illetve a kritikus infrastruktúra megzavarásából vagy megsemmisítéséből eredő közvetlen veszélyhelyzeteket (Rendelet 3. cikk 18. pont).

Egyes esetekben a kibocsátó hatóság a szolgáltatóval párhuzamosan a végrehajtó hatóságot is köteles értesíteni (Rendelet 8. cikk), aki ebben az esetben megvizsgálja a határozat teljesíthetőségét. Erre is tíz nap áll rendelkezésére, mely felfüggeszti a megkeresett szolgáltató rendelkezésére álló tíz napos határidőt [Rendelet 8. cikk (4) bekezdés], így szélsőséges esetben a teljesítésre húsz napot kell várni.

Ugyanez az adatszolgáltatás az ENYH esetében jellemzően 2–3 hónapos, míg nemzetközi bűnügyi jogsegély esetében akár tíz hónapos teljesítési idővel történik, továbbá nincs jogszabályban rögzített rövidített határidő a sürgős helyzetekre.

A megőrzésre kötelezés esetén a szolgáltatónak a MKEHT kézhezvételekor rendelkezésére álló adatokat hatvan napig kell változatlanul megőriznie. Ez idő alatt a kibocsátó hatóságnak igazolnia kell, hogy a KKEHT kibocsátásra került. Indokolt esetben a hatvan napos megőrzési határidő egy alkalommal harminc nappal meghosszabbítható, melyhez a kibocsátó hatóságnak a Rendelet VI. mellékletének szerinti nyomtatványt kell kitöltenie.

Az MKEHT és a KKEHT továbbítása

Mind a MKEHT-t, mind a KKEHT-t elsősorban az adatkezelőként eljáró szolgáltatónak, és a 8. cikkben előírt kötelező értesítés eseteiben a végrehajtó hatóság részére kell megküldeni. Amennyiben az adatkezelőként eljáró szolgáltatót

nem lehetett azonosítani, vagy értesítése a nyomozás érdekét veszélyeztetné, a tanúsítványok az adatfeldolgozóknak is kézbesíthetők. Ezzel a jogalkotó kizárta annak a kényszerét, hogy egy összetett, többszereplős folyamatban a kibocsátó hatóságnak kelljen – a szerződések részletes jogi értelmezésével – megállapítani az egyes szerepköröket.

A szolgáltatók és a kibocsátó hatóságok, valamint a kibocsátó és végrehajtó hatóságok közötti írásbeli kommunikáció, illetve a válaszok és adatok megküldése egy biztonságos és megbízható decentralizált informatikai rendszeren keresztül történik [Rendelet 19. cikk (1) bekezdés].

A tanúsítványok címzettnek történő megküldése mellett a kibocsátó hatóságot az adatkéréssel, megőrzéssel érintett személyek 13. cikk szerinti értesítése is terheli még.

A jogorvoslati lehetőségek

Az adatkérésről fő szabályként tájékoztatni kell az érintett célszemélyt, mely alól a Rendelet kivételt engedélyez a nemzeti jog rendelkezésével összhangban [Rendelet 13. cikk (1) és (2) bekezdés].

A tájékoztatásnak azonban nemcsak az adatkérésről vagy megőrzésről kell szólnia, hanem a jogorvoslati lehetőségekre is ki kell terjednie. A jogorvoslati lehetőséget, mely az intézkedés jogszerűségének vitatását is magába foglalja, a kibocsátó állam bírósága előtt lehet gyakorolni, a nemzeti jog erre vonatkozó szabályainak figyelembevételével.

A hazai jogalkalmazásban az adatkéréssel kapcsolatban nem terheli semmilyen értesítési kötelezettség a felderítő vagy nyomozó szerveket, sőt a nyomozás érdekében az adatszolgáltató ezen irányú kötelezettségének a teljesítése is korlátozható [Be. 264. § (7) és (8) bekezdés].

A büntetőeljárásban egyedül a bírói engedélyhez kötött leplezett eszközökkel kapcsolatos értesítési kötelezettség gyakorlati érvényesülését lehet vizsgálni, mely jellegét tekintve sokban hasonlít az érintett tájékoztatása nélküli adatkéréshez. Mindkét intézkedés beavatkozás a magánszférába, és mindkét eljárás esetén lehetőség van az érintett értesítésének mellőzésére [Be. 251. § (1) bekezdése].

A tapasztalat azt mutatja, hogy a leplezett eszközök esetében az értesítés mellőzését engedélyező kivételes szabály a felderítő vagy nyomozó szerv diszkrecionális döntésén alapuló általános gyakorlattá vált.

A jogorvoslati lehetőségek hazai szabályozását az Emberi Jogok Európai Bírósága (EJEB) több ítéletben, így többek között a Vissy-Szabó kontra Magyarország ügy ítéletének 86. szakaszában is kritizálta ([URL7](#)). Ennek alapján az

elektronikus adatok beszerzésével kapcsolatban is olyan értesítési szabályokat kellene kialakítani, mely megfelelően garantálja hatékony jogorvoslathoz fűződő alapvető jog érvényesülését. Az 1. számú táblázat az előzőekben részletezett feltételeket összegzi.

1. számú táblázat
A feltételek összesítése

Kritériumok	Kért intézkedés	Adattípus		
		Előfizetői	Forgalmi	Tartalmi
Minimum hitelesítési szint	Megőrzés	Ügyész		
	Közlés	Ügyész	Bíró	Bíró
Bűncselekmény	Megőrzés	Bármilyen bűncselekmény		
	Közlés	Bármilyen bűncselekmény	Minimum 3 év felső határ vagy a Rendeletben nevesített bűncselekmény	
Kiszabott ítélet	Megőrzés	Minimum 4 hónapos szabadságvesztés		
	Közlés	Minimum 4 hónapos szabadságvesztés	Minimum 3 év felső határos vagy a rendeletben nevesített bűncselekmény ügyében hozták	
Végrehajtó hatóság értesítése	Megőrzés	Nem kell		
	Közlés	Nem kell	Szükséges	Szükséges
Sürgősségi kivétel	Megőrzés	Van		
	Közlés	Van	Nincs	Nincs

Forrás. A szerző saját szerkesztése a Rendelet alapján.

Az Irányelv

Az Irányelv a Rendelet végrehajthatósága érdekében kötelezi az EU területén, a Rendelet szerinti szolgáltatást nyújtó természetes vagy jogi személyeket, hogy valamely tagállamban lehetséges címettként jelöljenek ki egy telephelyet vagy egy jogi képviselőt. Az Irányelv nem vonatkozik olyan szolgáltatókra, melyek egyetlen tagállam területén telepednek le, és kizárólag ide korlátozva nyújtanak szolgáltatást.

A szolgáltatók mellett a tagállamokra is feladatokat ró, így ki kell dolgozniuk a bejelentési kötelezettségeket elmulasztó szolgáltatókkal szemben egy kellően hatékony, arányos és visszatartó erejű szankciórendszert is.

Az Irányelv alapján egy központi hatóságot is ki kell jelölni, melynek feladata lesz ezeknek az adatoknak a nyilvántartása és hozzáférhető tétele, kiegészítve többek között az adott szolgáltató által elfogadott nyelv megjelölésével is (Irányelv 4. és 6. cikk).

Felkészülés a hatálybalépésre

A Rendelet hatálybalépésére ki kell alakítani azt a környezetet, mely egyformán alkalmas lesz a határozatok fogadására és továbbítására is. Ehhez meg kell teremteni az Irányelv által elvárt jogi környezetet, majd a Rendelet végrehajtásához meg kell teremteni a szervezeti és adminisztratív rendszert. Ehhez az alábbiakat kell megvalósítani.

A végrehajtó és a központi hatóság kijelölése

A határozatok teljesítésével összefüggésben a Rendelet értelmében tagállamomként ki kell jelölni egy végrehajtó hatóságot (enforcing authority), amely jogosult az KKEHT és MKEHT átvételére, az ezzel kapcsolatos értesítések fogadására. Az Irányelv alapján pedig egy központi hatóságot (central authority) kell kijelölni a telephelyek és jogi képviselők nyilvántartása érdekében.

A végrehajtó hatóság szerepe túlmutat egy adminisztratív közvetítő tevékenységen. A közlésre kötelező határozatok közül a kibocsátó hatóságnak – az érintett szolgáltató mellett – a végrehajtó hatóságot is köteles értesítenie, amennyiben forgalmi vagy tartalmi adatok közlését kéri. A kötelező értesítés alól kivételt képez a kizárólag a használó megállapítását célzó forgalmi adatok közlésére irányuló határozat, illetve, ha az eljárás alapjául szolgáló bűncselekményt a kibocsátó államban követték el, vagy az adatkéréssel érintett személy lakóhelye a kibocsátó államban található [Rendelet 8. cikk (1) és (2) bekezdése].

A végrehajtó hatóság a hozzá beérkezett határozatokat tíz napon – sürgős esetben 96 órán – belül értékeli, mely során a kérelmet vagy teljesíthetőnek ítéli meg, vagy annak teljesítésével kapcsolatban akadályt állapít meg.

Amennyiben a Rendelet 12. cikk (1) bekezdés a)-d) pontjában nevesített akadályt (mentesség vagy kiváltságok fennállása, a teljesítés nyilvánvalóan alapvető jog megsértésével járna, a teljesítés ellentétes lenne kétszeres eljárás alá vonás és a kétszeres büntetés tilalmával, az eljárás alapjául szolgáló cselekmény a végrehajtó állam joga szerint nem bűncselekmény) állapít meg, úgy erről a lehető leghamarabb, de legkésőbb az értesítés kézhezvételétől számított tíz napon – sürgős esetben 96 órán – belül értesíti a címzett szolgáltatót és a kibocsátó hatóságot.

A Rendelet külön említi az alábbi körülményeket, melyek megtagadási okok lehetnek:

- ha az adatszolgáltatás kérése valaki neme, faji vagy etnikai származása, vallása, szexuális irányultsága vagy nemi identitása, állampolgársága, nyelve vagy politikai véleménye miatt indított eljárásban, vagy emiatt kiszabott büntetés végrehajtása érdekében történt (Rendelet 11. pont);

- ha a kért adatokat a végrehajtó állam joga alapján biztosított mentességek vagy kiváltságok védik; vagy
- azokra a sajtószabadság vagy az egyéb médiában való véleménynyilvánítás szabadsága tekintetében speciális korlátozó szabályok vonatkoznak (Rendelet 63. pont).

Amennyiben nem látja akadályát a határozat teljesítésének, úgy erről nem köteles külön értesítést küldeni, de nem is tiltott a címzett szolgáltató erről történő értesítése sem.

A címzett szolgáltató a válaszdásra vagy a végrehajtó hatóság teljesíthetőségéről kapott értesítése, vagy ennek hiányában az arra nyitva álló tíz napos határidő értesítés nélküli letelte után kötelezett. A válaszdásra rendelkezésére álló tíz napos határidő ekkor indul el [Rendelet 8. cikk (4) bekezdés].

A fentiek alapján a nemzeti végrehajtó hatóságnak folyamatosan kell majd a 25 tagállamból fogadnia és értékelnie a határozatokat, ezekről rövid határidőn belül (tíz nap, vagy sürgős esetben 96 óra) döntést hozni, melyeket megtagadás esetén a hazai szolgáltatók és a kibocsátó hatóságok felé közölni is kell. Valószínűleg erre a Nemzetközi Bűnügyi Együttműködési Központ lenne alkalmas. Kérdés, hogy ez milyen leterheltséggel jár, illetve milyen technikai és humán erőforrást igényel.

Az Irányelv értelmében a tagállami központi hatóság tartja majd nyilván az országában letelepedett kijelölt telephelyek és az ott lakóhellyel vagy székhellyel rendelkező jogi képviselők kapcsolattartási adatait, illetve az ezekben bekövetkezett változásokat, több kijelölt telephely vagy képviselő esetén a területi illetékességeket, valamint a megkeresésekben alkalmazható nyelveket. A nyilvánartás adataihoz egy EU szinten kialakított koordinációs és együttműködés keretében folyamatos hozzáférést kell biztosítani a többi központi hatóság és a Bizottság részére [Irányelv 4. cikk (1) bekezdés és 6. cikk (3)–(4) bekezdés].

A két norma a hatóságok tekintetében nem utal egymásra, és nem derül ki, hogy a jogalkotó szándéka szerint a két hatóság – a Rendelet szerinti végrehajtó és az Irányelv szerinti központi – feladatait azonos szervezetnek kell-e ellátnia. Azonban a két norma egymásra épülése, az erre vonatkozó egyértelmű tilalom hiánya és a feladatok összefüggése miatt célszerű lenne egy közös hatóság kijelölése.

Az előzetes hitelesítés (engedélyeztetés)

A hazai szabályozástól eltérően a Rendelet alapján minden határozat – akár előfizető vagy a tényleges használói adatok megállapítására, akár forgalmi vagy

tartalmi adatokra vonatkozik – előzetes hitelesítésére lesz szükség. A Rendelet lehetővé teszi a szükséges adatok rövid határidőn belüli beszerzését egy külföldi telephellyel rendelkező szolgáltatótól, de ehhez első lépésként az idegen nyelvű határozatot előzetesen hitelesíteni kell ügyésszel vagy bíróval. A Rendelet szellemisége és küldetése alapján olyan hitelesítési (engedélyeztetési) eljárást kell kialakítani és a Be.-ben is megjeleníteni, mely ugyanilyen rövid idő alatt lehetővé teszi a határozatok kibocsátását. Az ügyészi hitelesítés feltehetően az adott nyomozás felügyeletét ellátó ügyész, míg a bírói hitelesítés az illetékes nyomozási bíró hatáskörébe tartozik majd. Erre azonban fel kell készíteni a helyi és területi végrehajtó szervekhez rendelt ügyészi és bírói szervezeteket is, hogy ez előzetes hitelesítés nem vegyen hosszabb időt igénybe, mint maga a külföldi adatszolgáltatás.

Kérdésként merülhet fel például, hogy a Rendelet 9. cikk (4) bekezdése alapján több nyelven – az EU vagy a végrehajtó állam hivatalos nyelvein – is kibocsátható határozat nyelvét ki határozza meg? A kibocsátó hatóság, a hitelesítő ügyész vagy bíró? Kell-e majd előzetesen egyeztetni erről, vagy lesz preferált nyelv? Elegendő lesz-e az eljáró hatóság tagjának nyelvtudása, vagy hiteles fordítást kell alkalmazni, és ha igen, ennek a költsége kit terhel majd? Ezek olyan gyakorlati kérdések, melyekkel a Rendelet értelemszerűen nem foglalkozik, de a hazai viszonyok között döntést igényelnek.

Kommunikációs csatorna kiépítése

A Rendelet V. fejezete szerint az írásbeli kommunikációt egy erre dedikált, decentralizált kommunikációs rendszeren keresztül kell lebonyolítani. Ehhez nemzeti szinten úgy kell biztosítani a hozzáférést az adott államban letelepedett szolgáltatóknak és jogi képviselőknek, hogy az ne jelentsen aránytalan anyagi terhet. Ennek érdekében az elektronikus végponti hozzáférési eszközök helyett lehetőség lesz a Bizottság által kifejlesztett, webalapú interfész igénybevételére is, ami szintén biztosítja az elvárt biztonságos adatáramlást. A szolgáltatók mellett a tagállamok számára is lehetőség lesz a nemzeti informatikai rendszer helyett a Bizottság által fejlesztett szoftver használatára. A kommunikációs csatornán az adatok továbbítása mellett biztosítani kell azt is, hogy nemzeti szinten statisztikai adatokat lehessen gyűjteni.

A decentralizált informatikai rendszerrel kapcsolatos elvárásokat a Rendelet 68., 81–92. pontjai, a 3. cikk 20. pontja, valamint a 19–23. cikke részletezi, melyek kötelező alkalmazása a 25. cikk szerinti végrehajtási jogi aktusok elfogadását követő év elteltével lesz kötelező.

Jogalkotás

A Rendelet alkalmazása ugyan nem igényel külön jogalkotást, de az előzőekben említett okok miatt a Be.-t módosítani kell az előzetes hitelesítés érdekében az ügyész és a nyomozási bíró feladatkörét illetően, valamint biztosítani kell a hatékony jogorvoslat lehetőségét. Ezeken túl a végrehajtó és a központi hatóságot hazánkban is ki kell jelölni, valamint ezek működését szabályozni kell.

Az Irányelv nemzeti jogba történő átültetésére 2026. február 18-ig van határidő. Ehhez meg kell alkotni a telephelyek és jogi képviselők bejelentési kötelezettségeit, valamint a velük szemben alkalmazható szankciókat tartalmazó jogi normákat [Irányelv 7. cikk (1) bekezdés].

A jogalkotás területén külön kihívásként jelentkezik azon kettős szankciórendszer kialakítása, mely egyrészt a kibocsátó hatóságok adatmegőrzési vagy átadási kéréseinek – a Rendelet biztosította lehetőségeken kívüli – nem teljesítése esetén, másrészt pedig az Irányelv szerinti bejelentési és adatszolgáltatás kötelezettség elmulasztása esetén szabható majd ki a szolgáltatóra. Ezeknek arányosnak, hatékonyak és kellően elrettentőnek kell lenniük. Az Irányelv megsértése esetén kiszabható szankciók szabályozásáról 2026. február 18-ig kell értesíteni a Bizottságot (Irányelv 5. cikk).

Összefoglalás

Az EU felismerte, hogy az elektronikus bizonyítékok szerepe a bűncselekmények felderítése és bizonyítása területén egye nagyobb szerepet tölt be. Ezeknek az adatoknak a határon átnyúló beszerzése a hagyományos nemzetközi bünygyi együttműködési csatornákon nehézkes és lassú, ami gyakran adatvesztést eredményez.

Az adatok beszerzésének egyszerűsítése érdekében kiadott Rendelet és Irányelv olyan jogi eszköz az igazságügyi hatóságok kezében, mely valóban képes segíteni a bünygyi nyomozást.

Az elektronikus adatok megőrzésének területén érzékelhető szabályozási anomáliák és a tagállamok eltérő szabályozásai ugyanakkor egy összetett eljárási rendet eredményezett, melynek gyakorlati végrehajtása kihívásokat hordoz magában.

A Rendelet hatályba lépését követően három év állt a tagállamok rendelkezésre a szervezeti, jogi és technikai feltételek megteremtésére, melynek 2/3-a eltelt. A hazai előkészületekről nem sok információ került nyilvánosságra, de a feladatok nagy része valószínűleg a hátralévő egy évre koncentrálódik.

Felhasznált irodalom

- Nyitrai E. (2025). *A digitális adatok és a modern technikai eszközök jelentősége a kriminalisztikában: A deepfake és a fake news jelenségek*. Ludovika Egyetemi Kiadó. https://doi.org/10.36250/01198_00
- Wang, R. L. (2022). Information is non-physical: The rules connecting representation and meaning do not obey the laws of physics. *Journal of Information Science*, 51(2), 455–462. <https://doi.org/10.1177/01655515221141040>

A cikkben szereplő online hivatkozások

- URL1: Az Európai Unió Bíróságának 54/14. számú sajtóközleménye a digitális adatkezeléssel és uniós jogértelmezéssel összefüggésben. <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054hu.pdf>
- URL2: Az Európai Bizottság rendelet-javaslat a elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről (ePrivacy Regulation). <https://eur-lex.europa.eu/legal-content/HU/TEXT/HTML/?uri=CELEX:52017PC0010&from=HU>
- URL3: Overview and professional analysis of the European ePrivacy Regulation provided by Cyber Risk GmbH. <https://www.european-eprivacy-regulation.com/>
- URL4: EUR-Lex summary page on electronic evidence in criminal proceedings within the European Union. <https://eur-lex.europa.eu/HU/legal-content/summary/electronic-evidence-in-criminal-proceedings.html>
- URL5: Council Decision authorising negotiations between the European Union and the United States on cross-border access to electronic evidence in criminal matters. <https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/en/pdf>
- URL6: Második kiegészítő jegyzőkönyv a Számítástechnikai Bűnözésről szóló Egyezményhez az elektronikus bizonyítékok átadásáról és a megerősített együttműködésről. [https://eur-lex.europa.eu/legal-content/HU/TEXT/PDF/?uri=CELEX:22023A0228\(01\)](https://eur-lex.europa.eu/legal-content/HU/TEXT/PDF/?uri=CELEX:22023A0228(01))
- URL7: Judgment of the European Court of Human Rights in the case of Szabó and Vissy v. Hungary concerning secret surveillance measures. [https://hudoc.echr.coe.int/fre#%7B%22itemid%22:\[%22001-160020%22%22%7D](https://hudoc.echr.coe.int/fre#%7B%22itemid%22:[%22001-160020%22%22%7D)

Alkalmazott jogforrások

Törvények

1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről
2003. évi C. törvény az elektronikus hírközlésről
2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

2005. évi CXVI. törvény az Európai Unió tagállamai közötti kölcsönös bűnügyi jogsegélyről szóló, 2000. május 29-én kelt egyezmény és az egyezmény 2001. október 16-án kelt kiegészítő jegyzőkönyve kihirdetéséről

2007. évi CLXXIV. törvény az elektronikus hírközlésről szóló 2003. évi C. törvény módosításáról

2017. évi XC. törvény a büntetőeljárásról

Nemzetközi normák

A Számítástechnikai Bűnözésről szóló Egyezményhez csatolt második kiegészítő jegyzőkönyv a megerősített együttműködésről és az elektronikus bizonyítékok átadásáról. [https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:20203A0228\(01\)](https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:20203A0228(01))

A Tanács kerethatározata (2002. június 13.) a közös nyomozócsoportokról (2002/465/IB) <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32002F0465>

Az Európai Parlament és a Tanács (EU) 2011/92 irányelve (2011. december 13.) a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról. <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32011L0093>

Az Európai Parlament és a Tanács (EU) 2013/40 irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040&from=DA>

Az Európai Parlament és a Tanács (EU) 2017/541. irányelve (2017. március 15.) a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról. <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32017L0541>

Az Európai Parlament és a Tanács (EU) 2019/713 irányelve (2019. április 17.) a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról. <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019L0713>

Az Európai Parlament és a Tanács (EU) 2023/1543 rendelete (2023. július 12.) a büntetőeljárás során az elektronikus bizonyítékokkal kapcsolatban, valamint a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából kibocsátott, közzésre kötelező európai határozatokról és megőrzésre kötelező európai határozatokról. <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32023R1543>

Az Európai Parlament és a Tanács (EU) 2023/1544 irányelve (2023. július 12.) a büntetőeljárásban az elektronikus bizonyítékok gyűjtése céljából a kijelölt telephelyek kijelöléséről és a jogi képviselők kinevezéséről szóló harmonizált szabályok meghatározásáról. <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32023L1544>

Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről. <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32002L0058>

Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról. <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32006L0024>

Az Európai Parlament és a Tanács 2014/41/EU irányelve (2014. április 3.) a büntetőügyekben kibocsátott európai nyomozási határozatról. <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32014L0041>

Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR) <https://net.jogtar.hu/jogszabaly?docid=a1600679.eup>

Egyezmény a Tanács által az Európai Unióról szóló szerződés 34. cikkének megfelelően létrehozott, az Európai Unió tagállamai közötti kölcsönös bűnügyi jogsegélyről (2000/C 197/01) [https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:42000A0712\(01\)](https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:42000A0712(01))

Számtástechnikai Bűnözésről Szóló Egyezmény. (Budapest, 2001.11.23.) <https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf>

A cikk APA szabály szerinti hivatkozása

Csizner Z. (2026). Elektronikus bizonyítékok az időprésben. *Belügyi Szemle*, 74(1), 35–59. <https://doi.org/10.38146/BSZ-AJIA.2026.v74.i1.pp35-59>

Nyilatkozatok

Összeférhetetlenség

A szerző nem jelentett összeférhetetlenséget.

Finanszírozás

A szerző nem kapott pénzügyi támogatást a kutatáshoz, a szerzőséghez és/vagy a cikk publikálásához.

Etikai nyilatkozat

Jelen cikkhez nem kapcsolódik adatkészlet.

Nyílt hozzáférésről szóló tájékoztatás

Jelen cikk nyílt hozzáférésű (Open Access) közlemény, amely a Creative Commons Nevezd meg! – Ne add el! – Ne változtasd! 4.0 Nemzetközi licenc (CC BY-NC-ND 4.0) feltételei szerint kerül publikálásra: <https://creativecommons.org/licenses/by-nc-nd/4.0/>. A licenc alapján a közlemény változtatás nélkül és nem kereskedelmi célra bármely médiumban szabadon felhasználható, megosztható és újraközölhető, feltéve, hogy a felhasználó megfelelő hivatkozással feltünteti az eredeti szerző(ke)t és a közlés helyét, valamint megadja a licenc linkjét.

Származékos mű készítése (pl. átdolgozás, adaptáció, fordítás) és kereskedelmi felhasználás nem engedélyezett.

Levelező szerző

A cikk levelező szerzője Csizner Zoltán, aki a csizner.zoltan2@uni-nke.hu e-mail címen érhető el.