AN OVERVIEW ON THE DIFFERENT APPROACHES TO REGULATE IOT PERMANENT ROAMING

AZ IOT TARTÓS BARANGOLÁS SZABÁLYOZÁSÁNAK ELTÉRŐ MEGKÖZELÍTÉSEINEK ÁTTEKINTÉSE

MIKLÓS Gellért [1]

Abstract

The aim of this paper is to present the different approaches to regulate the permanent roaming of IoT devices and the data security and economic aspects of such regulations. The topicality of the subject is provided by the increasing proliferation of IoT devices, the progress made in the field of connectivity, the deployment of next-generation mobile networks (5G) and the emergence of new applications based on them. IoT devices are able to connect to networks and communicate with other IoT devices using a variety of technologies. One way to do this is to connect to a mobile network. In the event that an IoT device is connected to a public mobile network in another state other than its public home network for a specified period of time, it is considered to be permanent roaming. The regulation of this phenomenon is evolving dynamically in the world along different concepts. Some states allow, while others prohibit or restrict permanent roaming, while there are states where the issue is currently completely unregulated. With the proliferation of IoT devices and the emergence of differing regulatory regimes, it is expected that more and more countries will regulate permanent roaming.

Keywords

IoT, permanent roaming, EU, data security, telecommunications

Absztrakt

Jelen írás célja bemutatni a cellás IoT eszközök tartós barangolására vonatkozó eltérő szabályozásokat és azok adatbiztonsági, gazdasági vonatkozásait. A téma aktualitását az IoT eszközök egyre növekvő ütemű elterjedése, a csatlakoztathatóság terén elért fejlődés és az újgenerációs mobilhálózatok (5G) telepítése, valamint az erre épülő új alkalmazási területek megjelenése szolgáltatja. Az IoT eszközök különböző technológiák alkalmazásával képesek kapcsolódni hálózatokhoz és kommunikálni más IoT eszközökkel. Ennek egyik módja a mobilhálózathoz való csatlakozás. Abban az esetben, amennyiben egy IoT eszköz a nyilvános hazai hálózatától eltérő, más államban található nyilvános mobilhírközlő hálózathoz meghatározott időtartamnál tovább csatlakozik, tartós barangolásról beszélünk. Ennek a jelenségnek a szabályozása eltérő koncepciók mentén dinamikusan fejlődik a világban. Bizonyos államok engedélyezik, más államok tiltják, vagy korlátozzák a tartós barangolást, azonban léteznek olyan államok is, ahol a kérdés jelenleg teljesen szabályozatlan. Az IoT eszközök terjedésével és az eltérő szabályozási rendszerek kialakulásával várható, hogy egyre több országban kerül majd szabályozásra a tartós barangolás.

Kulcsszavak

IoT, tartós barangolás, EU, adatbiztonság, telekommunikáció

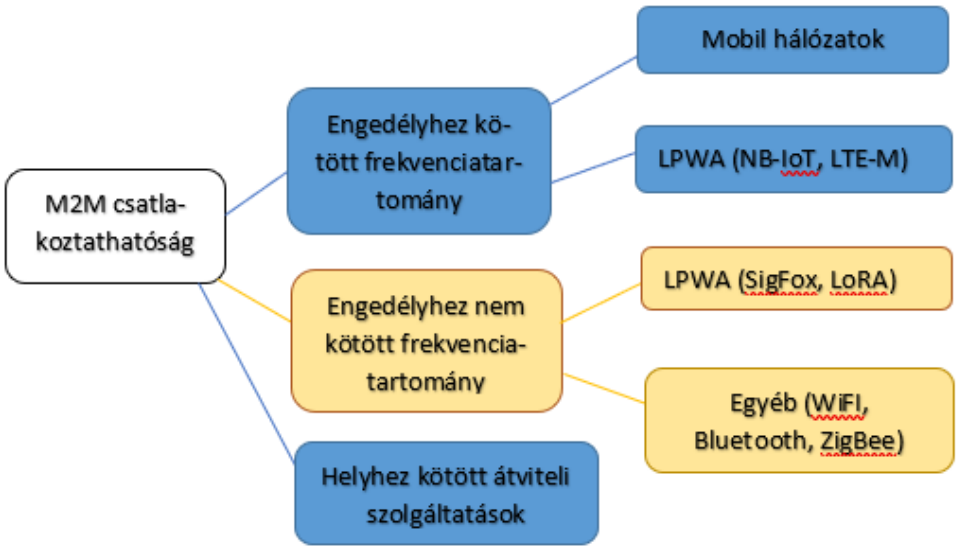
[1] gellert.miklos@gmail.com | ORCID: 0000-0002-3757-6834 | PhD Student, Óbuda University Doctoral School for Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Az IoT eszközök egyre gyorsuló elterjedése a gazdaság szinte minden ágazatában érezteti hatását. Az okos eszközök iránti növekvő igény ösztönzőleg hatott kapcsolódás, a hardware és software fejlesztés terén is. A szabályozás azonban nem tartotta a lépést ezzel a gyors ütemű fejlődéssel, amely jelentős kihívás elé állítja a szabályozó hatóságokat. A szabályozó hatóságok látókörében még mindig az ember és ember közötti kommunikáció a domináns, így a szabályozás logikája is arra épül fel. A frekvenciasávok felosztása, kiosztása és hasznosítása, az eszközök és technológiák szabványosítása, az gépek közötti kommunikáció számára elkülönített számtartományok szabályozása vagy az IoT eszközök biztonsága csak néhány olyan kérdés melyekkel a szabályozó hatóságok az elmúlt évtized során szembesülni kényszerültek. Jelen írás célja bemutatni a cellás IoT eszközök tartós barangolásával kapcsolatos eltérő szabályozási megközelítéseket.

Az IoT eszközök csatlakoztathatósága

Az IoT eszközök – definíciójukból adódóan – más eszközökkel kommunikálnak, a kommunikációhoz szükséges jeleket pedig szabványosított technológia alkalmazásával, valamely hálózathoz történő csatlakozás útján továbbítják. Az eszközök között létrejövő kapcsolódás megvalósulhat engedélyhez kötött frekvencia használatára alapuló technológia által, vagy engedély nélkül használható frekvencia alkalmazásával is. Az előbbire példa az elektronikus hírközlési szolgáltatások nyújtása során alkalmazott mobil hálózatok (2G, 3G, 4G, 5G), vagy az engedélyköteles frekvenciatartományban működő LPWAN (Low Power Wide Area Network) megoldások, mint a Narrowband-IoT vagy az LTE-M technológia. Az utóbbira példa az engedélyhez nem kötött frekvenciatartomány alkalmazására alapul LPWAN megoldások, mint a SigFox, vagy a Low Power Radio (LoRa) technológiák, valamint az egyéb, magánhálózati technológiák, mint a WiFi, Bluetooth és a ZigBee. [1]



1. Ábra: M2M csatlakoztathatóság fajtái, forrás: BEREC, Internet of Things indicators, 18. oldal

A különböző technológiáknak megvannak a maguk specifikációi, melyek meghatározzák annak alkalmazási területét is. Az LPWA technológiák, mint nevükből is adódik, olyan alkalmazási területeken használhatók fel leginkább, ahol fontos szempont az alacsony energiafogyasztás, valamint a nagy átviteli távolság alacsony átviteli sebesség mellett. Erre tipikus példa lehet a precíziós mezőgazdaságban (pl. talajnedvesség mérésére) vagy az okos városok kialakítása során (pl. parkolóhely állapotának jelzésére) alkalmazott szenzorok. Ezek a szenzorok ugyanis jellemzően kisméretű adatcsomagokat továbbítanak, azonban fontos a minél hosszabb élettartam és a

Vannak azonban olyan alkalmazási területek, amelyek esetén az LPWA megoldások nem megfelelőek, mert például nem tudják biztosítani a szükséges adatátviteli sebességet, az alacsony késleltetést vagy az elvárt megbízhatóságot. Ezekben az esetekben megoldást jelenthet a cellás IoT (angolul cellular IoT). További előnye a cellás IoT megoldásoknak, hogy a világ szinte összes országában ki van már építve a mobilhírközlő hálózat, így az IoT szolgáltatók részéről nem szükséges külön infrastrukturális beruházás az okos eszközök működtetéséhez. A legújabb, ötödik generációs mobilhálózatok minden korábbinál nagyobb adatátviteli sebességet tesznek elérhetővé az IoT eszközök és alkalmazások számára, megvalósíthatóvá téve az olyan nagymennyiségű adat gyors átvitelére épülő alkalmazásokat, mint például az önvezető autózás vagy a robotsebészet.

Tartós barangolás

Az elektronikus hírközlő hálózatok működésében és az elektronikus hírközlési szolgáltatások nyújtásában az azonosítók biztosítják a hálózatok, szolgáltatási rendszerek és különösen az előfizetők megkülönböztetését. A legismertebb ilyen azonosító a telefonszám, amellyel a világméretű telefonhálózat minden végpontja egyértelműen azonosítható és a hálózat bármely végpontjáról felhívható, elérhető.[2] A Nemzetközi Távközlési Egyesület (angolul International Telecommunication Union) által kibocsájtott nemzetközi számozási terv (ITU-T E.164 Ajánlás) szabja meg a telefonszámok felépítését és az egyes országok országkódját. Ez Magyarország esetében a +36-os kód. A nemzeti számozási terv kialakítása állami hatáskör, melyet Magyarországon jelenleg a 14/2020. (XII. 15.) NMHH rendelet szabályoz. Az elektronikus hírközlési azonosítók, ideértve a telefonszámokat is, hasonlóan a frekvenciatartományokhoz az állam tulajdonát képező korlátos erőforrásnak minősülnek. Ezekkel a korlátos erőforrásokkal való gazdálkodás jellemzően az államok nemzeti szabályozó hatóságának feladatkörébe tartoznak. Magyarországon erre a gazdálkodási és felügyeleti tevékenységre kijelölt hatóság a Nemzeti Média- és Hírközlési Hatóság (a továbbiakban: NMHH).

A hatályos magyar nemzeti számozási terv külön számtartományt tartalmaz a gépek közötti szolgáltatások (M2M számok) nyújtására, ehhez a 71-es kódot rendeli.[2] A 71-es kód alatt nyújtott gépek közötti szolgáltatás olyan kommunikációt tesz lehetővé a végberendezések vagy alkalmazások között az elektronikus hírközlő hálózaton, ahol az információt legfeljebb csekély emberi beavatkozással továbbítják. [8] Tekintettel arra, hogy a számtartomány elsősorban a gépek közötti kommunikációt szolgálja, ezért hangkommunikáció, il-

[2] 1. Melléklet 2.7.

letve üzenetküldés csak korlátozott jelleggel, az IoT eszközök és alkalmazások között létesíthető. A nemzeti számozási terv külön számtartományt rendel az Európai Unión belüli extraterritoriális használatra.

A hatóság az azonosítók használatára az elektronikus hírközlési szolgáltatókról vezetett nyilvántartásába bejegyzett hírközlési szolgáltatót jelölhet ki. A szolgáltató a kijelölés érdekében kérelmet nyújt be a hatósághoz, a hatóság pedig a számmező kijelölési határozatában a kérelemben meghatározott alkalmazás jellegétől függő számhasználati feltételeket állapíthat meg. Az NMHH egy adott M2M alkalmazás részére a számokat különböző nagyságú számmezőkben jelöli ki és adja át a szolgáltatók részére.

A gyakorlatban ez azt jelenti, hogy amennyiben egy vállalkozás cellás IoT eszközöket kíván forgalomba hozni Magyarország területén és ehhez a nemzeti számozási tervben meghatározott M2M számot kíván felhasználni, úgy a hírközlési szolgáltató a vállalkozást megállapodásuk alapján létrejövő számhasználati jogviszony keretében feljogosítja az M2M számok használatára. Az IoT eszközök azonosítása a beépített SIM-kártya (előfizetői azonosító modul) útján történik. Amennyiben az IoT eszközök az Európai Unión belüli extraterritoriális használatra is engedélyezett tartomány számaival kerültek azonosításra, úgy - amennyiben a tartós barangolás egyéb feltételei fennállnak – azok az IoT eszközök az Európai Unió bármely tagállamában korlátozás nélkül használhatók.

A szolgáltatók az azonosítók használatáért és lekötéséért, valamint az azonosítóengedélyezési eljárásokért díjat fizetnek az NMHH részére. Éppen ez az, ami az adatbiztonság és adatvédelem mellett az egyik leggyakrabban elhangzó érv a tartós barangolás korlátozása vagy tiltása érdekében. Tartós barangolás esetén ugyanis az történik, hogy a vállalkozás fizet egy adott ország szolgáltatója számára a számhasználati jogosultságért és az IoT eszközök kommunikációjához szükséges szolgáltatástért (pl. internet hozzáférés), a szolgáltató pedig az azonosítók használatáért díjat fizet a nemzeti szabályozó hatóság részére. Az IoT eszközök azonban végül tartósan más államban kerülnek telepítésre, használatra. A vállalkozás a célállamban is megszerezhette volna az IoT szolgáltatás nyújtásához szükséges azonosítókat, ez azonban valamely oknál fogva nem történt meg. Ilyen ok lehet a például a globális ügyintézés, hiszen egy globális szolgáltatótól beszerezni egy számos országban használható megoldást egyszerűbb és kisebb költséggel jár, mint minden országban helyi megoldást keresni. Ezért a célállam és az ott működő hírközlési szolgáltatók végeredményben bevételektől esnek el a tartós barangolás miatt.

A TARTÓS BARANGOLÁS SZABÁLYOZÁSA AZ EURÓPAI UNIÓBAN

Az Európai Unió az elmúlt évtizedekben jelentős erőfeszítéseket tett a távközlési szektor harmonizációjára és az egységes belső piac megteremtésére. Ennek részeként került sor a nyilvános mobilhírközlő hálózatok közötti barangolás szabályozására is. A következő tíz éves, 2031-ig terjedő időszakra az átdolgozott roaming végrehajtási rendelet (a továbbiakban: Roaming Rendelet) szabályai irányadók az Európai Unión belül. [9] A Roaming Rendelet alapján a tartós barangolás nincs tiltva, az kereskedelmi tárgyalások tárgyát képezi, és arról két szolgáltató szabadon köthet megállapodást a közöttük létrejövő nagykereskedelmi barangolási megállapodásban.

Ez azonban egyelőre csak lehetőség, de nem kötelezettség a hírközlési szolgáltatók számára. Az Európai Unión belül várhatóan egyre több szolgáltató fogja lehetővé tenni az IoT eszközök közötti kommunikáció esetén a hálózatán történő barangolást, hatékonyabbá

és versenyképesebbé téve ezáltal az IoT eszközök piacát.[3] A mobilhálózat-üzemeltető szolgáltatók a Roaming Rendelet alapján kötelesek referenciaajánlatot közzétenni, ami tartalmazza a nagykereskedelmi barangolási hozzáférésre vonatkozó általános feltételeket.[4] A szolgáltatók ebben a referencia ajánlatban feltételeket szabhatnak meg a tartós barangolás megakadályozása céljából.

A referenciaajánlat tartalmazhat rendelkezéseket arra az esetre, amennyiben feltételezhető, hogy más szolgáltató előfizetőnek jelentős része tartósan barangol a látogatott hálózaton. Ebben az esetben a látogatott hálózat üzemeltetője – a vonatkozó uniós és nemzeti adatvédelmi szabályok betartása mellett – információkéréssel fordulhat a másik szolgáltatóhoz annak objektív mutatók alapján történő megállapítása érdekében, hogy valóban tartós barangolásról van-e szó az adott előfizetők vonatkozásában.

Amennyiben az információkérés, a felszólítás és egyéb intézkedések sem vezettek eredményre, végső eszközként a referenciaajánlat lehetőséget biztosíthat a nagykereskedelmi barangolási megállapodás megszüntetésére, amennyiben objektív kritériumok alapján megállapításra került, hogy a másik szolgáltató előfizetőinek jelentős hányada tartós barangolást végez és erről tájékoztatásra került. A nagykereskedelmi barangolási megállapodás egyoldalú megszüntetésére tartós barangolásra hivatkozással, kizárólag a látogatott hálózatot üzemeltető szolgáltató nemzeti szabályozó hatóságának előzetes engedélye alapján kerülhet sor. A nemzeti szabályozó hatóság a kérelem kézhezvételét követő három hónapon belül dönt, a másik szolgáltató szabályozó hatóságával folytatott konzultációt követően. A hatóság a döntésről tájékoztatja továbbá az Európai Bizottságot is. Az eljárás során mindkét nemzeti szabályozó hatóság dönthet úgy, hogy felkéri az Európai Elektronikus Hírközlési Szabályozók Testületét (rövidítve BEREC), hogy egy hónapon belül hozzon állásfoglalást az alkalmazott intézkedések vonatkozásában.

A fenti, több lépcsős eljárás szabályaiból megállapítható, hogy az jogalkotó szándéka valóban az volt, hogy a nagykereskedelmi barangolási megállapodás felmondására a tartós barangolás következményeképp valóban csak végső megoldásként, a valóban visszaélésszerű helyzetek során kerülhessen sor. Az Unió számára a prioritás a belső piac fenntartása és a verseny, valamint az innováció elősegítése.

Az Európai Unióból történő adatok továbbítására, értve ez alatt az IoT eszközök által kezelt adatok továbbítását is, az Európai Unió általános adatvédelmi rendeletének rendelkezései irányadók. Amennyiben az IoT eszközök az adatokat harmadik országba, például Kínába vagy az Egyesül Államokba kívánják továbbítani, úgy az adattovábbításnak meg kell felelnie a személyes adatok harmadik országba történő továbbítására vonatkozó többletkövetelményeknek is, az Európai Unióban azonban nincs érvényben olyan adatlokalizációs követelmény amely megkövetelné az IoT szolgáltatóktól, hogy infrastruktúrájukat vagy az adatokat az Unió területén belül tárolják.

[3] Roaming Rendelet (21) Preambulumbekezdés

[4] Roaming Rendelet (16) Preambulumbekezdés és 3. cikk (5)

SZAÚD-ARÁBIA

Szaúd-Arábia mind gazdasági erejét, mind lakosságszámát tekintve az Arab-félsziget egyik meghatározó állama. Az ott végbemenő gazdasági folyamatok, a kialakított szabályozási keretrendszer hatással van a szomszédos országokra is. Igaz ez az IoT eszközökre és szolgáltatásokra vonatkozó szabályozásra is.

A szaúdi telekommunikációs szabályozó hatóság, a Communications and Information Technology Commission (rövidítve CITC) 2019-ben fogadta el az IoT Szabályozási Keretrendszert (angolul IoT Regulatory Framework, a továbbiakban: Keretrendszer) amelyben szabályozásra kerültek az IoT szolgáltatások nyújtásával összefüggő főbb kérdések, mint az engedélyköteles frekvenciatartományok, az azonosítóhasználat és a típusjóváhagyás. Ez a keretrendszer volt az első, amely kifejezetten az IoT szektort és az azzal kapcsolatos szolgáltatások nyújtását szabályozta, azzal a deklarált céllal, hogy Szaúd-Arábiát az IoT terén az Arab-félsziget és a világ egyik vezető országává tegye.

A Keretrendszer alapján IoT szolgáltatásokat Szaúd-Arábiában helyhez kötött vagy mobil hálózaton keresztül csak a CITC által megadott engedéllyel rendelkező telekommunikációs szolgáltató nyújthat. Engedély azonban csak az országban bejegyzett gazdasági társaság kérelmezhet, meghatározott feltételek teljesülése esetén. [3] Ez a gyakorlatban azt jelenti, hogy Szaúd-Arábiában csak a helyi hírközlési szolgáltatók nyújthatnak a mobilhírközlő hálózaton IoT szolgáltatást. Ehhez a szaúdi nemzeti számozási tervben kijelölt M2M azonosítókat kell használni. [3]

A fentieken túlmenően a Keretrendszer előírja az IoT szolgáltatók számára azt is, hogy az IoT szolgáltatások nyújtásához használt összes szervert és minden adatot az ország területén belül tároljanak, valamint biztosítsák a hatóság számára az adatok legalább 12 hónapig történő megtekintéséhez szükséges technikai képességeket.[5] Ez erős kontrollt biztosít az adatok felett mind a bűnüldöző szervek, mind a nemzetbiztonsági szolgálatok számára. Az adatlokalizációs követelményt a Keretrendszer megismétli a 8. pontban, amikor a szolgáltatók számára további követelményként előírja, hogy az IoT hálózat összes összetevőjét, eszközét és az adatok tárolására szolgáló szervereket Szaúd-Arábia területén kell üzemeltetni. A tartós barangolásra épülő globális megoldások tehát Szaúd-Arábiában nem engedélyezettek, a cellás IoT eszközök működéséhez helyi hírközlési szolgáltatók által nyújtott mobil hálózati hozzáférés szükséges.

A CITC 2022 márciusában nyilvános konzultációt kezdeményezett a szolgáltatók és iparági szereplők részvételével a Keretrendszer szabályainak felülvizsgálata érdekében. [4] A konzultáció továbbra is fenntartja az engedélyre, valamint a szaúdi M2M számok használatára vonatkozó kötelezettséget, nem tartalmazza azonban az adatlokalizációra vonatkozó korábbi előírást. Ez azonban nem feltétlenül jelenti azt, hogy amennyiben a konzultációban megfogalmazott szabályok elfogadásra kerülnek, úgy abban az esetben már nem szükséges a szerverek és adatközpontok országon belüli fenntartása. 2021 szeptemberében elfogadásra került a személyes adatok védelméről szóló törvény (angolul Personal Data Protection Law vagy röviden PDPL), amely rögzíti, hogy tilos személyes adatot tárolni, vagy kezelni Szaúd-Arábia területén kívül a felhasználó kifejezett engedélye vagy az adatvédelmi hatóság írásos engedélye nélkül, amely engedélyt a hatóság esetről esetre vizsgálva állít ki.

[5] IoT Szabályozási Keretrendszer 7. pont

A fenti szabályokból látható, hogy a szaúdi szabályozás szigorúan tiltja a tartós barangolást, elzárva a globális hírközlési szolgáltatókat a szaúdi piachoz való hozzáféréstől, versenyelőnybe hozva a helyi szolgáltatókat. Ezen túlmenően az adatlokalizációs és adatmegőrzési kötelezettségek útján erős kontrollt biztosít a hatóságok számára az IoT szolgáltatások nyújtása során keletkező adatok felett.

TÖRÖKORSZÁG

Törökország telekommunikációs szabályozó hatósága, az Információs és Kommunikációs Technológiai Hatóság (angolul Information and Communication Technologies Authority, rövidítve a továbbiakban: ICTA) az IoT szektorra két jelentős hatású határozatot tett közzé a közelmúltban, az egyiket 2018 elején, a másikat 2019 elején. Az első döntés a járművekben nyújtott e-Call szolgáltatások szabályaira vonatkozott, míg az utóbbi a távoli konfigurációra alkalmas e-SIM technológiákra vonatkozott. A második döntés előírta az IoT szolgáltatók számára, hogy szolgáltatásukat csak helyi SIM kártyák útján nyújthatják, vagy olyan távoli konfigurációra (angolul over-the-air, OTA) alkalmas SIM technológiát kell alkalmazni, amely lehetővé teszi a helyi szolgáltatók profiljára történő átállást. [5] A tartós barangolást az ICTA fenti eSIM döntése, valamint az elektronikus kommunikációról szóló 5809 számú törvény rendelkezései tiltják, amely a telekommunikációs szektor szabályozásának elsődleges forrása Törökországban. A hatóság jogértelmezése és indokolása alapján a tartós barangolás tiltása és ezzel párhuzamosan a helyi azonosítók használata elősegíti az innovációt és a versenyt az IoT szektorban, valamint megerősíti az adatbiztonság, a személyes adatok védelmének szintjét. [6] Szaúd-Arábiával ellentétben Törökország formális csatlakozási kérelmet nyújtott be az Európai Unióhoz, ezért elviekben szabályozását az Uniós szabályokhoz – beleértve a hírközlési szabályokat is - közelítenie kellene.

A szabályozás 90 napos türelmi időt biztosít a Törökországba érkező IoT eszközök számára. Amennyiben egy barangoló eszköz 90 napnál többet tölt el 120 napon belül egy török mobilhálózaton hanghívás vagy SMS kezdeményezés nélkül, abban az esetben a látogatott hálózat szolgáltatója köteles a tartósan barangoló eszközt a hálózatáról letiltani. A tiltást követően a felhasználók – tehát nem az IoT szolgáltatás nyújtója, hanem az eszköz tényleges tulajdonosai – kötelesek a letiltott eszközöket a hatóság által ebből a célból létrehozott platformján regisztrálni, valamint a regisztrációs díjat megfizetni.

A beágyazott SIM (rövidítve: eSIM) kártyákkal ellátott IoT eszközök esetében a szabályozás előírja, hogy az azok működtetésével összefüggő összes létesítmény, eljárás és rendszer Törökországban kell, hogy létesítésre kerüljön valamely Törökországban bejegyzett és engedéllyel rendelkező hírközlési szolgáltató irányítása alatt. [5]

A tartós barangolást a török szabályozás tiltja, a gyakorlatban tehát az IoT eszközök gyártóinak mindenképpen helyi szolgáltatókkal kell megoldani a cellás IoT eszközök működéséhez szükséges hálózati hozzáférést.

KÖVETKEZTETÉSEK

A tartós barangolás szabályozása kapcsán tehát eltérő megközelítések figyelhetők meg. Az országok egy része, mint például az Európai Unió vagy az Egyesült Államok szabályozása lehetővé teszi a tartós barangolást a szolgáltatók hálózatain a meghatározott feltételek fennállása esetén. Más országok, mint például Szaúd-Arábia, Törökország, Brazília

vagy Kína tiltják a tartós barangolást és szigorú adatlokalizációs szabályokat hoztak, amelyek az IoT szolgáltatókat arra kötelezik, hogy szolgáltatásukat helyi hírközlési szolgáltatók közreműködésével nyújtsák az adott országban. Ez nagyobb kontrollt és betekintést enged a helyi hatóságok számára az IoT szolgáltatásokkal kapcsolatos adatokba, egyúttal azonban a helyi megoldások többletköltséget jelentenek az IoT szolgáltatók számára. Számos esetben a SIM kártya már a gyártási folyamat során behelyezésre kerül az eszközökbe, így azok utólagos cseréje nem feltétlenül megoldható. Az ilyen esetekre is megoldást nyújt a távoli konfiguráció, amely egy olyan technológia, amely lehetővé teszi a SIM kártyán található adatok és profil módosítását anélkül, hogy azt cserélni kellene. Ennek jelentősége az IoT szektor számára jelentős, nem véletlen, hogy az Európai Unió is kötelezi a tagállamokat a távoli konfiguráció előmozdítására amennyiben az technikailag kivitelezhető.[6] [10][11]

Számos olyan állam van, amelynek jogrendszere ma még nem szabályozza a tartós barangolást, így az IoT eszközök probléma nélkül barangolhatnak a helyi hálózatokon időkorlát nélkül. A nemzetközi trendek vizsgálatát követően azonban egyre több állam dönt az IoT szektor szabályozása mellett, beleértve az állandó barangolás kérdését is. Amennyiben jelentős számú állam dönt az állandó barangolás tiltása mellett, az ellehetetlenítheti a globális megoldásokat és így végeredményképp visszavetheti az innovációt az IoT szektorban, továbbá lassíthatja a tartós barangolást tiltó államok digitális átállását és az IoT eszközök széleskörű elterjedését.

Az IoT eszközökre vonatkozó biztonsági előírások, szabványok és ajánlások terén már megfigyelhető hasonló tendencia, amely során egyre több állam teszi közzé saját biztonsági követelményeit, amelyek gyakran eltérnek más államok és nemzetközi szabványok előírásaitól, ezzel megnehezítve az IoT eszközök globális elterjedését és megnövelve a piacra lépés költségeit az IoT szolgáltatók számára.[7]

FELHASZNÁLT FORRÁSOK

[1] BEREC Internet of Things indicators BOR (19) 25 [Online] Elérhető: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/%208464-berec-report-on-internet-of-things-indicators

[2] Nemzeti Média- és Hírközlési Hatóság Azonosítógazdálkodás [Online] Elérhető: https://nmhh.hu/szakmai-erdekeltek/azonositogazdalkodas

[3] CITC Internet of Things (IoT) Regulatory Framework 2019 [Online] Elérhető: https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf

[4] CITC Public Consultation Document on Updating the IoT Regulations 2022 [Online] Elérhető: https://regulations.citc.gov.sa/en/Pages/PublishedPublicConsultations.aspx#/PublishedPublicConsulationDetails/10

[5] ICTA 2019/DK-TED/053 döntés Elérhető: https://www.btk.gov.tr/uploads/boarddecisions/uzaktan-programlanabilir-sim-teknolojileri-esim/053-2019-web.pdf

[6] IAPP Turkey's BTK imposes data localization requirements on e-SIM technologies [Online] Elérthető: https://iapp.org/news/a/turkeys-btk-imposes-data-localization-requirements-on-e-sim-technologies/

[6] Európai Hírközlési Kódex 93. § (6) és Eht. 150. § (3)

[7] Miklós Gellért „Overview of the Internet of Things Security Related Threats and Possible Mitigations” In: Eight International Scientific Web-conference of Scientists and PhD. students or candidates Budapest: Óbuda University, pp 209-217 (2020)

Jogszabályok

[8] Az elektronikus hírközlő hálózatok azonosítóinak nemzeti felosztási tervéről és az azonosítógazdálkodás rendjéről szóló 14/2020. (XII. 15.) NMHH rendelet
[9] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/612 RENDELETE az Unión belüli nyilvános mobilhírközlő hálózatok közötti barangolásról (roaming)
[10] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2018/1972 IRÁNYELVE (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról
[11] Az elektronikus hírközlésről szóló 2003. évi C. törvény